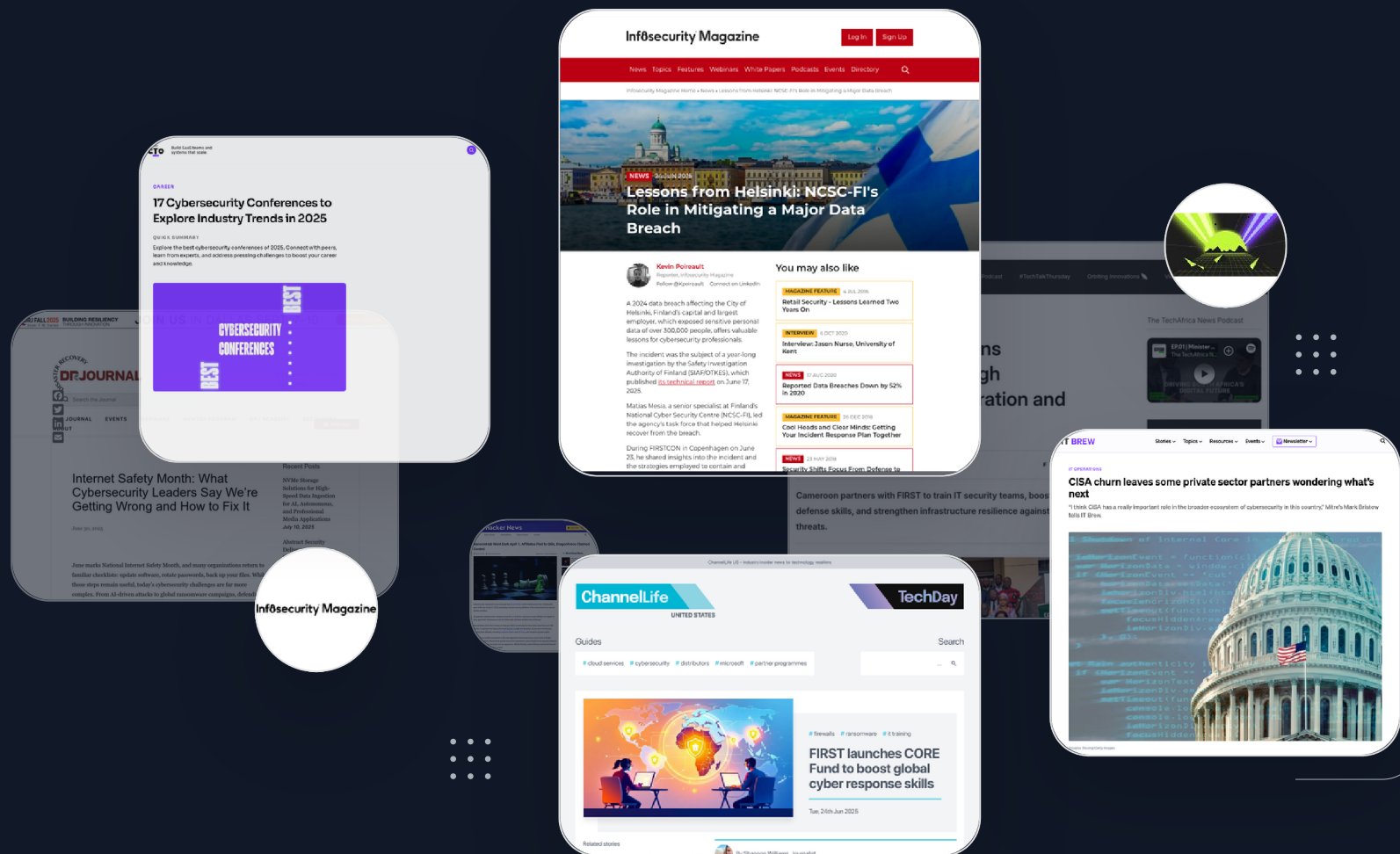




FIRST's Q2FY25 PR Coverage

Presented by Growth Stack Media



Contents

Summary	3
Highlights	6
Coverage	9

Summary



74

Pieces of Coverage

Total number of online, offline and social clips in this book



403K

Estimated Views

Prediction of lifetime views of coverage, based on audience reach & engagement rate on social



29M

Audience

Combined total of publication-wide audience figures for all outlets featuring coverage



1.13K

Engagements

Combined total of likes, comments and shares on social media platforms



44

Avg. Domain Authority

A 0-100 measure of the authority of the site coverage appears on. Provided by Moz



26

Coverage that links

How many items of coverage contain at least 1 backlink to the website(s) you're promoting.



79

Links from Coverage


Total number of backlinks
found across all the coverage.

Highlights

Infosecurity Magazine Log In Sign Up

News Topics Features Webinars White Papers Podcasts Events Directory

Infosecurity Magazine Home » News » Lessons from Helsinki: NCSC-FI's Role in Mitigating a Major Data Breach



Lessons from Helsinki: NCSC-FI's Role in Mitigating a Major Data Breach

Kevin Poireault Reporter, Infosecurity Magazine Follow @kpoireault Connect on LinkedIn

You may also like

Infosecurity Magazine

Lessons from Helsinki: NCSC-FI's Role in Mitigating a Major Data Breac

131K 74 933 27

CTO Build SaaS teams and systems that scale

CAREER

17 Cybersecurity Conferences to Explore Industry Trends in 2025

QUICK SUMMARY
Explore the best cybersecurity conferences of 2025. Connect with peers, learn from experts, and address pressing challenges to boost your career and knowledge.



The CTO Club

17 Cybersecurity Conferences to Explore Industry Trends in 2025


156K 35 32.9K

IT BREW Stories Topics Resources Events Newsletter

IT OPERATIONS

CISA churn leaves some private sector partners wondering what's next

"I think CISA has a really important role in the broader ecosystem of cybersecurity in this country," Mitre's Mark Bristow tells IT Brew.



IT Brew

CISA churn leaves some private sector partners wondering what's next


19.1K 39 3.25K 4

ChannelLife US - Industry insider news for technology readers

ChannelLife UNITED STATES

Guides Search

#cloud services #cybersecurity #distributors #microsoft #partner programmes



FIRST launches CORE Fund to boost global cyber response skills

Tue, 24th Jun 2025

Channellife US

FIRST launches CORE Fund to boost global cyber response skills

248 10 156

DRJ FALL 2025 BUILDING RESILIENCY THROUGH INNOVATION JOIN US IN DALLAS SEPT. 7-10

DR JOURNAL EN ESPAÑOL SIGN IN SUBSCRIBE

Search the Journal

JOURNAL EVENTS WEBINARS MENTOR PROGRAM DRJ ACADEMY RESOURCES

Internet Safety Month: What Cybersecurity Leaders Say We're Getting Wrong and How to Fix It

June 30, 2025

Recent Posts
NVMe Storage Solutions for High-Speed Data Ingestion for AI, Autonomous, and Professional Media Applications July 16, 2025
Abstract Security Delivers 4X Operational Efficiency at Just Labs

June marks National Internet Safety Month, and many organizations return to

Disaster Recovery Journal

Internet Safety Month: What Cybersecurity Leaders Say We're Getting Wrong and How to...

6.04K 50 84 1

Today's Bulletin: July 10, 2025

TechAfrica News News The TechAfrica News Podcast #TechTalkThursday Orbiting Innovations Video Events

#SECURITY

Cameroon Strengthens Cybersecurity Through International Collaboration and Capacity Building

May 23, 2025 1 min read Author: Aayushya Ranjan

Cameroon partners with FIRST to train IT security teams, boost cyber defense skills, and strengthen infrastructure resilience against digital threats.

The TechAfrica News Podcast

EP01 | Minister - The TechAfrica News

Follow us on LinkedIn

NEWSLETTER SIGNUP

Sign up for our weekly newsletter and get the latest industry insights right in your inbox!

TechAfrica News

Cameroon Strengthens Cybersecurity Through International Collaboration and Capacity...

69.4K 32 18.3K 12


BITS, BYTES, AND BREAKING NEWS |
Followed by 5.2M+ million

The Hacker News

[Home](#) [Cyber Attacks](#) [Vulnerabilities](#) [Expert Insights](#) [Contact](#)

RansomHub Went Dark April 1; Affiliates Fled to Qilin, DragonForce Claimed Control






Apr 30, 2025 Rayne Lukahmanan



Cybercrime / Threat Intelligence





Cybersecurity researchers have revealed that RansomHub's online infrastructure has "inexplicably"

— Most Read News

-  DHS Warns Pro-Iranian Hackers Likely to Target U.S. Networks After Iranian Nuclear Strikes
-  Business Case for Agentic AI SOC Analysts
-  Cyber Criminals Exploit Open-Source Tools to Compromise Financial Institutions Across...
-  Weekly Recap: Airline Hacks, Citibank Outage, Outlook Midweek, Banking Trojans and more
-  U.S. House Bans WhatsApp on Official Devices Over Security and Data Protection Issues

The Hacker News

RansomHub Went Dark April 1; Affiliates Fled to Qilin, DragonForce Claimed Control

 687K
 88
 2.32K
 75

A screenshot of the website 'Cybersecurity Conferences 2025 - 2026'. The header features a yellow banner with the text 'Be The First To Know: Cyber Events Alerts in Your State or Country' and a star icon. Below the banner is a navigation bar with links: 'About', 'This Week', 'Sitemap', 'Need Registrations?', 'Our Agency', 'Blog', 'Contact', and a 'Submit' button. The main heading is 'Cybersecurity Conferences 2025 - 2026', followed by the subtitle 'All Security Conference Niches | Upcoming Cybersecurity Events'. A paragraph describes the directory as meticulously updated and manually checked to prevent spam, serving as a premier resource for discovering top cybersecurity conferences, events, meetings, and seminars for 2024, 2025, and beyond. It mentions a curated list of chief information security officers (CISOs), cybersecurity leaders, technology executives, and anyone passionate about the field. Below this is a section titled 'Join Our Community' featuring a row of seven circular profile pictures and a '+479K' badge. Underneath the profiles is the text 'Speaking Opportunities | Ticket Discounts | Geo-Specific / Niche Event Alerts'. The bottom section of the image shows the title 'Cybersecurity Conferences 2025 - 2026 | Over 3.4K Events' with a globe icon, and a footer with social media icons and counts: a person icon with '17.3K', a target icon with '38', an eye icon with '3.23K', and a share icon with '3'.

Coverage

74 pieces



EIN Presswire

Paid and free press release distribution services are in one place. The EIN Presswire offers the best...

70

Domain Authority

Provided by
MOZ

212K

Unique Visits

Provided by
SimilarWeb

April 08, 2025

ONLINE

Phoenix Security Unveils Groundbreaking...

einpresswire.com/article/799896728/pho...

Estimated Views

1.73K

Calculated based on audience size and social engagement

Questions? [+1 \(202\) 335-3939](#) • [Pricing & Comparison Chart](#) • [Contact](#) • [Log In](#)

[Submit Release](#)

[About](#) • [Pricing](#) • [Distribution](#) • [Press Releases](#) • [Newswires](#) • [Knowledge Base](#)

News Search

There were 1,818 press releases posted in the last 24 hours and 405,408 in the last 365 days.

World Media Directory • [RSS](#) • [Email Newsletters](#)

Phoenix Security Unveils Groundbreaking Threat-Centric AI Agent at VulnCon, for a Next-Gen Vulnerability Management

NEWS PROVIDED BY
[Phoenix Security](#)
April 08, 2025, 15:00 GMT

SHARE THIS ARTICLE

Phoenix Security Unveils Revolutionary Threat-Centric AI Agent at VulnCon predicting which vulnerability will become a ransomware or is likely to be exploited

RALEIGH, NC, UNITED STATES, April 8, 2025
[/EINPresswire.com/](#) -- [Phoenix Security](#) is proud to announce the launch of its first AI-powered [Threat-Centric Agent](#) at VulnCon, marking a major leap forward in proactive vulnerability management and remediation. This new agent, built on a 3-step threat-centric approach, is designed to work seamlessly alongside Phoenix's Reachability Analysis AI Agent and Blast Radius Analysis Copilot, enabling organizations to focus on the most dangerous vulnerabilities and apply targeted remediation strategies with unmatched precision.

The new Threat-Centric AI Agent is the result of Phoenix Security's continuous innovation in the cybersecurity space. With Reachability Analysis AI already achieving a 71.5% reduction in vulnerabilities for high-profile clients like Clear Bank, and the Blast Radius Analysis Copilot providing

Available insight into the impact of vulnerabilities within

Phoenix Security Analysis of Ransomware

Phoenix Security ASPM winner of Gartner Peer insight and Get app

Phoenix Security ASPM winner of Gartner Peer insight and Get app

Author Contact

Phil Moroni
Phoenix Security
+1 919-594-8888
[email us here](#)

More From This Source

[Phoenix Security Unveils Groundbreaking Threat-Centric AI Agent at VulnCon for a Next-Gen Vulnerability Management](#)

[Phoenix Security ASPM Kicks Off 2025 with Gartner and Get App Prestigious Client and Industry Recognition](#)

[Press Release: Phoenix Security Expands ASPM Capabilities with Amica Integration and Extended Cloud Security](#)

[View All Stories From This Source](#)



Packet Pushers | IT Podcasts for IT Pros

A podcast network, technical blog, newsletters, videos, and community by & for network engineer...

61

Domain Authority [?]

Provided by
MOZ

29.1K

Unique Visits [?]


Provided by
SimilarWeb

April 08, 2025


🌐 ONLINE

PP057: Behind the Scenes At Cisco: PSIRT, AI, CVEs, and...

packetpushers.net/podcasts/packet-prote...



Podcasts Video Blog Newsletters Resources Sponsor Talk To Us Merch Store





PP057: Behind the Scenes At Cisco: PSIRT, AI, CVEs, and VEX
PACKET PROTECTOR 057


PACKET PROTECTOR > EP. 57 | APRIL 8, 2025

00:00 00:00

PODCAST: [DOWNLOAD](#) (124.1MB) | [EMBED](#)

 Jennifer (JJ) Minella Drew Conry-Murray

LISTEN, SUBSCRIBE & FOLLOW:



Cisco Systems has a sprawling portfolio of home-grown and acquired products. What's it like trying to find and address bugs and vulnerabilities across this portfolio? Omar Santos, a Distinguished Engineer at Cisco, gives us an inside look. We dig into how Cisco identifies security bugs using internal and external sources, the growing role of AI for bug hunting and threat analysis, what it's like to run a Product Security Incident Response Team (PSIRT) across an ever-expanding product line, the CVE process, and industry efforts such as the Vulnerability Exploitability eXchange (VEX) that aim to keep organizations better updated on the status of known vulnerabilities.

Episode Guest: Omar Santos, Distinguished Engineer, Cybersecurity and AI Security Research, Cisco Systems

Omar Santos is a recognized leader in the cybersecurity community. He is the Distinguished Engineer (Sr. Director) at Cisco leading Artificial Intelligence (AI) Security Research, vulnerability research, and disclosure. He works with senior management, executives, engineers, and industry-peers during the investigation and resolution of security vulnerabilities in Cisco products, including cloud services. Omar has designed, implemented, and supported numerous secure networks for Fortune 100 and 500 companies and the U.S. government.

SHARE THIS EPISODE



Explore our podcasts

[Day Two DevOps](#)
[Heavy Networking](#)
[Heavy Strategy](#)
[Heavy Wireless](#)
[IPv6 Buzz](#)
[N Is For Networking](#)
[Network Automation Nerds](#)
[Network Break](#)
[Packet Protector](#)
[Tech Bytes](#)
[Technically Leadership](#)
[Total Network Operations](#)
[The Cloud Gambit](#)

Estimated Views

333 [✓]

Calculated based on audience size and social engagement



Medium

On Medium, anyone can share insightful perspectives, useful knowledge, and life wisdom with the world.

95

Domain
Authority

Provided by
MOZ

April 07, 2025

ONLINE

Happening This Week: “CVE/FIRST VulnCon 2025,” Apr...

medium.com/@cve_program/happening-t...

Links

10

10 links to first.org

Medium

Search

Write

Sign up

Sign in



Happening This Week: “CVE/FIRST VulnCon 2025,” April 7–10, 2025



CVE Program Blog

Follow

1 min read · Apr 7, 2025



2



The [CVE Program](#) and [FIRST](#) are co-hosting [VulnCon 2025](#) this week at the McKimmon Center in Raleigh, North Carolina, USA, April 7–10, 2025.

Agenda

The [full agenda](#) is available now on this [conference web page](#) or view the schedule by day. Virtual attendees should check your email for session links and other details.

Get CVE Program Blog's stories in your inbox

Join Medium for free to get updates from this writer.

Enter your email

Subscribe

Monday, April 7 — [View day 1 schedule](#)

Tuesday, April 8 — [View day 2 schedule](#)

Wednesday, April 9 — [View day 3 schedule](#)

Thursday, April 10 — [View day 4 schedule](#)

Venue

[McKimmon Center](#)

North Carolina State University

1101 Gorman St.

Raleigh, North Carolina 27606

USA



Techmeme

Top news and commentary for technology's leaders, from all around the web.

80

Domain
Authority [?]

Provided by
MOZ

145K

Unique
Visits [?]

Provided by
SimilarWeb

February 10, 2012

🌐 ONLINE

All Tech Events - Techmeme

techmeme.com/events

Estimated Views

3.36K [✓]

Calculated based on
audience size and social
engagement

Engagements

602 [✓]

Total number of social
engagements



All Tech Events

Jul 8-10	RailsConf	Philadelphia
Jul 9-11	WeAreDevelopers World Congress	Berlin
Jul 10	Earnings: TSM	
Jul 13-17	GenAI Week Silicon Valley	Santa Clara, CA
Jul 15-16	Reuters Momentum AI	San Jose
Jul 16	Earnings: ASML	
Jul 17	Earnings: NFLX	
Jul 22-23	Fortune Brainstorm AI Singapore	Singapore
Jul 23	Earnings: GOOG, IBM	
Jul 24	Earnings: INTC, MBLY	
Jul 29	Earnings: PYPL, SPOT, BKN	
Jul 30	Earnings: META, HOOD	
Jul 31	Earnings: AAPL, Samsung Electronics, RDDT, RBLX	
Aug 2-7	Black Hat USA	Las Vegas
Aug 4-6	fintech_devcon	Denver
Aug 6	Earnings: DASH	
Aug 6-10	Rare Evo	Las Vegas
Aug 7-10	DEF CON	Las Vegas
Aug 10-14	SIGGRAPH	Vancouver
Aug 11-13	Ai4	Las Vegas
Aug 13-15	USENIX Security Symposium	Seattle
Aug 14-16	Kansas City Developer Conference	Kansas City
Aug 17-21	HYBRID: Crypto Policy Symposium	Santa Barbara, CA
Aug 19-24	HYBRID: gamescom	Cologne
Aug 21-22	Coinfest Asia	Bali, Indonesia
Aug 24-Sep 1	Burning Man	Black Rock City, Nevada
Aug 25-26	WebX	Tokyo
Aug 25-28	VMware Explore	Las Vegas
Aug 26-28	GopherCon	New York
Aug 27-28	TechBBQ	Copenhagen
Aug 29-Sep 1	PAX West	Seattle
Sep 2-4	Commercial UAV Expo	Las Vegas
Sep 3-4	CONF3RENCE	Dortmund, Germany
Sep 3-5	HubSpot INBOUND	San Francisco
Sep 3-5	HYBRID: DeveloperWeek CloudX + API:World + DataWeek	Santa Clara, CA
Sep 5-7	IFA	Berlin



Socket

Socket fights vulnerabilities and provides visibility, defense-in-depth, and proactive supply chain...

43

Domain
Authority [?]

Provided by
MOZ

75.5K

Unique
Visits [?]

Provided by
SimilarWeb

Big News: Socket Acquires Coana to Bring Reachability Analysis to Every Appsec Team. [Learn more →](#)


Socket Product Learn Company Pricing Love Docs [API](#) [Book a Demo](#) [Install](#) [Sign in](#)


[← Back](#)

SECURITY NEWS

VulnCon 2025: NVD Scraps Industry Consortium Plan, Raising Questions About Reform

At VulnCon 2025, NIST scrapped its NVD consortium plans, admitted it can't keep up with CVEs, and outlined automation efforts amid a mounting backlog.



 **Sarah Gooding**
April 10, 2025

[Twitter](#) [LinkedIn](#) [Facebook](#) [RSS](#)

At VulnCon 2025, NVD program manager Tanya Brewer and NIST division manager Matthew Scholl delivered a long-awaited update on the status and future of the National Vulnerability Database (NVD) today. The talk came just days after [the NVD quietly reclassified tens of thousands of CVEs as "Deferred"](#), signaling its inability to keep up with growing disclosure volume.

Their virtual session — held in a packed ballroom but streamed remotely — outlined recent recovery efforts, upcoming technical improvements, and a shift in strategy after a tumultuous year. But the format and content of the presentation left some attendees underwhelmed.

"The session is virtual? (Weird, since I saw Tanya at the event.) And only 30 minutes long (including Q&A)," security consultant Jeroen Braak [commented](#) on LinkedIn. "For a community that's been raising valid concerns and waiting for answers, this feels like a missed opportunity... it could further reinforce the perception of [NVD's] ongoing decline."

April 11, 2025

 ONLINE

VulnCon 2025: NVD Scraps Industry Consortium Plan,...

socket.dev/blog/vulncon-2025-nvd-scrap...

Estimated Views

9.23K [✓]

Calculated based on
audience size and social
engagement

Engagements

3 [✓]

Total number of social
engagements



Infosecurity Magazine

The award winning online magazine dedicated to the strategy, insight and technology of information...

74

Domain Authority [?]

Provided by
MOZ

131K

Unique Visits [?]

Provided by
SimilarWeb

Inf0security Magazine

Log InSign Up

NewsTopicsFeaturesWebinarsWhite PapersPodcastsEventsDirectory

Infosecurity Magazine Home » News » NVD Revamps Operations as Vulnerability Reporting Surges

NEWS 11 APR 2025

NVD Revamps Operations as Vulnerability Reporting Surges

Kevin Poireault
Reporter, Infosecurity Magazine
Follow @Kpoireault Connect on LinkedIn

After a tumultuous year marked by internal turmoil and a [vulnerability backlog](#), the National Vulnerability Database (NVD) within the US National Institute of Standards and Technology (NIST) has finally stabilized.

However, the NVD is now facing a new challenge: reporting that has sent its backlog soaring, threatening the team's revitalized efforts.

Tanya Brewer, the NVD Program Manager, and Michael Smith, the Computer Security Division at NIST, shared some updates on April 10, the final day of VulnCon, an event focused on vulnerability management in Raleigh, North Carolina.

They announced several improvements in how they handle vulnerabilities and said they were working on new ways to deal with the backlog, including automating more data processing and exploring AI-powered methods to assist them.

NVD Overcomes Staffing

You may also like

NEWS 23 MAY 2024

NVD Leaves Exploited Vulnerabilities Unchecked

NEWS 25 APR 2025

SAP Fixes Critical Vulnerability After Evidence of Exploitation

NEWS FEATURE 23 SEP 2024

Beyond Disclosure: Transforming Vulnerability Data Into Actionable Security

NEWS 28 MAR 2024

NIST Unveils New Consortium to Operate National Vulnerability Database

April 11, 2025

🌐 ONLINE

NVD Revamps Operations as Vulnerability...

infosecurity-magazine.com/news/nvd-rev...

Estimated Views

915 ✓

Calculated based on audience size and social engagement

Engagements

13 ✓

Total number of social engagements



InfoSecMap – Mapping out the best InfoSec events & groups!

17

Domain Authority [?]

Provided by



4.84K

Unique Visits [?]

Provided by



CVE/FIRST VulnCon 2025 & Annual CNA Summit

Details

Group ¹

Visit Website

Share

Report

Description

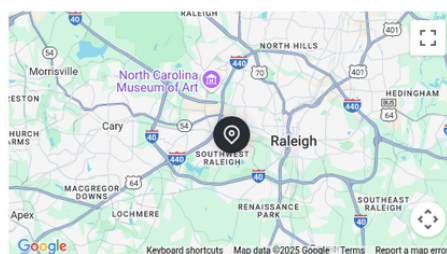
Title: CVE/FIRST VulnCon 2025 & Annual CNA Summit

Connection Details: link will be provided to registered attendees.

Description: The purpose of the conference is to collaborate with various vulnerability management and cybersecurity professionals to develop forward leaning ideas that can be taken back to individual programs for action to benefit the vulnerability management ecosystem. A key goal of the conference is to understand what important stakeholders and programs are doing within the vulnerability management ecosystem and best determine how to benefit the ecosystem broadly.

Event Website: <https://www.first.org/conference/vulncon2025/>

Location



1101 Gorman St, Raleigh, North Carolina 27606, United States

Get Directions

Date and time

April 7, 2025 7:30 am - April 10, 2025 5:30 pm
Timezone: America/New_York

✓ Ended

Categories



Type



Cost



Topics

ONLINE

CVE/FIRST VulnCon 2025 & Annual CNA Summit

infosecmap.com/event/cve-first-vulncon-...

Estimated Views

2.63K [✓]

Calculated based on audience size and social engagement

Links

2 [✓]

2 links to first.org



B2Bdaily.com

Discover the most up-to-date news and current various topics such as business, technology,...

15

Domain Authority

Provided by
MOZ

254K

Unique Visits

Provided by
SimilarWeb

The screenshot shows the B2Bdaily.com website interface. At the top, there's a navigation bar with the B2Bdaily logo and a 'SUBSCRIBE' button. Below the navigation bar, the article title 'NVD Revamps Operations to Tackle Growing Backlog of Vulnerabilities' is prominently displayed. The author is Dwaine Evans, and the date is April 14, 2025. A featured image shows a person working on a laptop with code visible in the background. Below the article title, there's a 'Table of Contents' section with a list of six items: 1. Overcoming Operational Challenges, 2. Embracing Technology, 3. Strategic Adjustments, 4. Community Engagement, 5. Diversifying Data Sources, and 6. Conclusion. To the right of the table of contents, there are tags for 'AI', 'Automation', 'Innovation', 'Linux', and 'Machine Learning'. At the bottom of the screenshot, the first section of the article, 'Overcoming Operational Challenges', is partially visible, starting with the text: 'The National Vulnerability Database (NVD) team at the US National Institute of Standards and Technology (NIST) has faced significant operational challenges over the past year. Periods of internal disruption, coupled with an overwhelming surge in reported vulnerabilities, have created a substantial backlog, stressing NVD's capacity to manage and process vulnerability data efficiently. Although staffing issues have been addressed, the backlog remains a growing concern. NVD leaders Tanya Brewer and Matthew Scholl shared valuable insights into the current state and future direction of the NVD's operations during their presentation at VulnCon, a conference dedicated to vulnerability management.'

April 14, 2025

ONLINE

NVD Revamps Operations to Tackle Growing Backlog of...

b2bdaily.com/it/nvd-revamps-operations-t...

Estimated Views

130K

Calculated based on audience size and social engagement



Energy Central

Energy Central is the go-to platform for utility professionals, providing expert insights, industry...

63

Domain Authority

Provided by MOZ

40.5K

Unique Visits

Provided by SimilarWeb

Welcome to the new Energy Central — same great community, now with a smoother experience. To login, use your Energy Central email and reset your password.

Get the free newsletter

Must-read news in the electric utility industry, in your inbox. Read by 200k+.

Home

Communities

Energy & Grid Management

Energy Business

Intelligent Utility

Customer Engagement & Ex...

Energy Workforce

Fossil Fuels & Generation

Renewables

Nuclear

Resources

Newsletters

Events

Podcasts

Our Partner Network

Job Board

About Us

Guidelines

Advertise With Us

© Copyright 2025

Intelligent Utility

Tom Alrich Expert Member Top Contributor
3 months ago · Posted in Intelligent Utility

Databases, all the way down

I have been attending [VulnCon 2025](#) remotely this week, although not all the sessions. Even though the first conference was last year, VulnCon has clearly found its niche as the premier gathering place for people interested in or involved with vulnerability management. The conference is well designed and well executed.

The sessions I've been attending are those that have to do with software naming in what I call the "CVE ecosystem", but which most people think of as the National Vulnerability Database (NVD). If you have been reading my [recent posts](#), you know that:

1. Learning about a software vulnerability isn't very helpful if you don't know what products are affected by it; ideally, you want to be able to search on a product name in a vulnerability database and immediately be shown all the vulnerabilities that have recently been identified in that product. Moreover, since CVE is by far the most widely cited vulnerability type and there are now over 280,000 CVEs in the official list, affected products need to be referred to using a machine-readable software identifier. The only identifier currently supported by CVE.org (the organization funded by DHS that creates and manages CVE Records) is CPE, which stands for Common Platform Enumeration.
2. When a CVE Numbering Authority (CNA), working for CVE.org, produces a CVE Record to report a new software vulnerability, they do not usually include a CPE name(s) to refer to affected products listed in the text of the record. The reason for this is that the NVD ^[1] has always wanted to be in control of CPE creation. This didn't previously cause a big problem, since until last year, the NVD almost always created a CPE for every affected product described in the text of a CVE Record; they did this within a few days of receiving the record from CVE.org.
3. However, starting on February 12, 2024, the NVD drastically slowed their production of CPE names, for a reason that has never been clearly explained. This has produced an ever-growing backlog of CVE Records without a CPE name. Despite several promises that they would fix the problem by a certain date, the backlog has continued to grow. Today, the backlog stands at well over 40,000 CVE Records (although a well-known vulnerability researcher estimated in the VulnCon chat that the backlog is

ANNOUNCEMENT: The New Energy...
In case you missed it, we'r...

EMBRACING THE TRIPLE BOTTOM...
In today's rapidly evolvin...

Carbon Dioxide Removal...
The high cost of living, primaril...

How BTM Distributed Energy...
U.S. electric utilities are...

Uncovering the Invisible: Closing the...
As the global energy...

April 14, 2025

ONLINE

Databases, all the way down

energycentral.com/intelligent-utility/post/...

Estimated Views

355

Calculated based on audience size and social engagement

Links

1

1 link to first.org

FIRST's Q2FY25 PR Coverage

18



Rivista Cybersecurity Trends

Leggi di più

15

Domain
Authority [?]

Provided by
MOZ

3.73K

Unique
Visits [?]

Provided by
SimilarWeb



NEWS ARTICOLI VIDEO INTERVISTE FOR BEGINNERS FOR EXPERTS RUBRICHE SFOGLIA LA RIVISTA ABOUT US SUPPORTACI

Cyber Security Events 2025: la nostra Guida



Nel contesto globale odierno, dove la tecnologia avanza a passi da gigante, la sicurezza informatica riveste un ruolo sempre più cruciale. La crescente sofisticazione delle minacce informatiche, unita alla necessità di proteggere dati sensibili e infrastrutture vitali, rende la cybersecurity una priorità assoluta per aziende, professionisti e istituzioni.

Il 2025 si preannuncia un anno decisivo per il settore della cybersecurity, con una serie di eventi dedicati a temi di grande attualità, come l'evoluzione delle minacce informatiche, l'uso dell'intelligenza artificiale nella sicurezza, la protezione dei dati personali e il ruolo sempre più centrale della resilienza digitale. Questi appuntamenti rappresentano anche un'importante occasione di incontro e confronto tra professionisti del settore, rappresentanti delle istituzioni, aziende, ricercatori e accademici, accomunati dall'obiettivo di condividere competenze, esperienze e soluzioni innovative.

In questo scenario, in continua evoluzione, restare aggiornati è essenziale, e la partecipazione agli eventi di settore si conferma una delle strategie più efficaci per affrontare le sfide emergenti e rimanere al passo con le ultime novità.

Come ogni anno, siamo lieti di presentare la nostra **Guida agli Eventi Cyber Security 2025**, uno strumento pensato per tutti coloro che desiderano navigare nel vasto panorama degli appuntamenti dedicati alla sicurezza informatica. Questa guida annuale offre un calendario completo di eventi, conferenze, workshop e summit, con informazioni precise su date, luoghi e dettagli utili, facilitando così una pianificazione efficace della partecipazione.

Che tu sia un professionista della cybersecurity, un'azienda o un appassionato, questa guida è il tuo punto di riferimento per orientarti tra le innumerevoli opportunità offerte dal mondo degli

April 14, 2025

ONLINE

Cyber Security Events 2025: la nostra Guida - Rivista...

cybertrends.it/cyber-security-events-2025...

Estimated Views

2.18K [✓]

Calculated based on
audience size and social
engagement

Engagements

4 [✓]

Total number of social
engagements

Links

1 [✓]

1 link to first.org



runZero

runZero delivers the fastest, most complete security visibility possible, giving organizations the ability t...

37

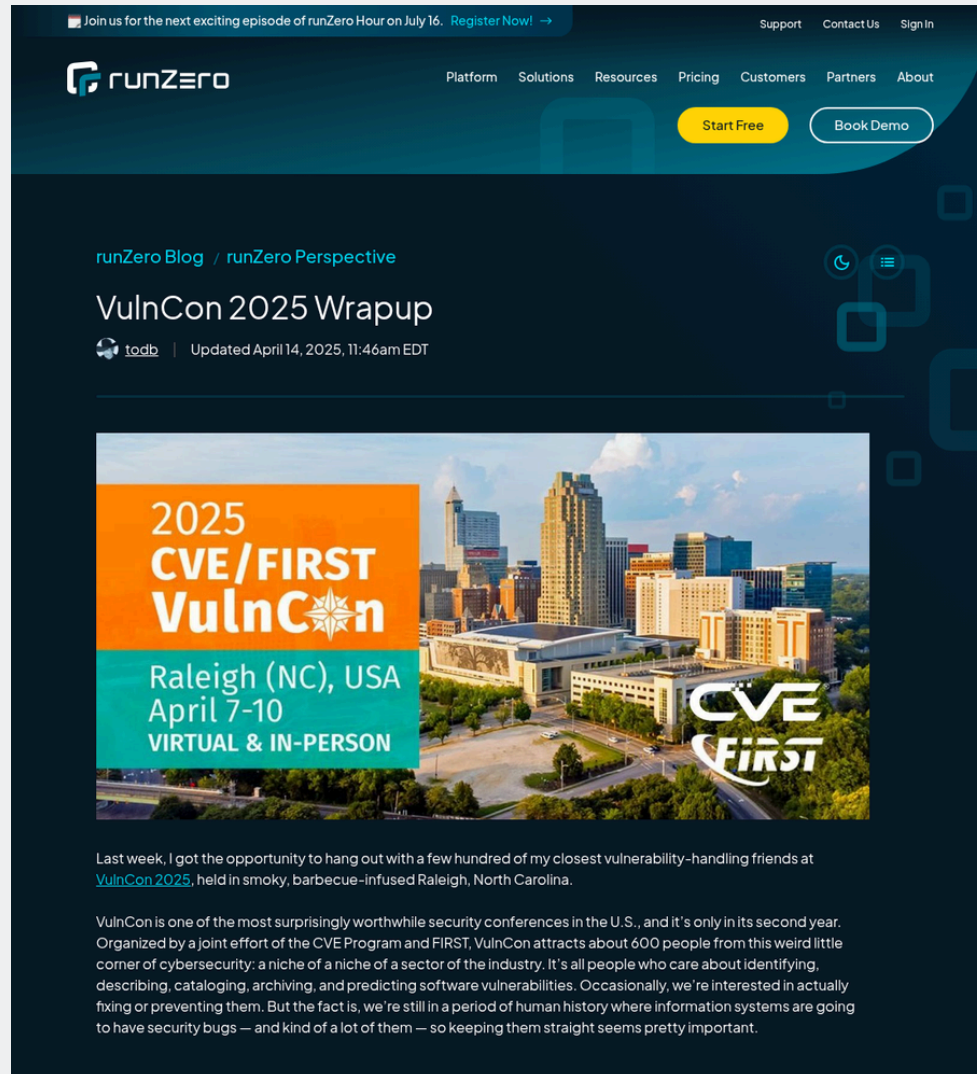
Domain Authority [?]

Provided by
MOZ

18.2K

Unique Visits [?]

Provided by
SimilarWeb



April 14, 2025

ONLINE

VulnCon 2025 Wrapup

runzero.com/blog/vulncon-2025-wrapup/

Estimated Views

5.05K [✓]

Calculated based on audience size and social engagement

Engagements

1 [✓]

Total number of social engagements

Links

2 [✓]

2 links to first.org



Open Source Security Foundation – Linux Foundation Projects

56

Domain
Authority [?]

Provided by
MOZ

30K

Unique
Visits [?]

Provided by
SimilarWeb

Submit your proposal: OpenSSF Community Day Korea


OpenSSF
OPEN SOURCE SECURITY FOUNDATION

About Projects Learning Community Public Policy Blog & News Events [Join](#) ^Q

Key Takeaways from VulnCon 2025: Insights from the OpenSSF Community

April 14, 2025 | Blog

^Q Share



April 14, 2025

🌐 ONLINE

OpenSSF at VulnCon 2025: Key Takeaways on OSS Security and...

openssf.org/blog/2025/04/14/key-takeaw...

Estimated Views

378 [✓]

Calculated based on
audience size and social
engagement

Engagements

1 [✓]

Total number of social
engagements

Links

2 [✓]

2 links to first.org



Open Source Security

31

Domain
Authority [?]

Provided by
MOZ

1.25K

Unique
Visits [?]

Provided by
SimilarWeb

April 19, 2025

🌐 ONLINE

Can we trust CVE?

opensourcesecurity.io/2025/04-can-we-tr...

Open Source Security

[About](#) [Contact](#) [Feeds](#) [Search](#) [Archive](#)

Can we trust CVE?

April 19, 2025 · Josh Bressers



If you are a security nerd, and even if you're not, you probably heard about the epic CVE mess that happened. It's a very long story and was covered in many places, but the TL;DR was the funding for CVE fell through, panic ensued, then CISA found some temporary funds to keep the lights, so everything is fine and we can all go back to normal.

Well, some of us won't go back to normal because the CISA funding is good for 11 months. Will there be more funding in 11 months? Will an asteroid destroy the Earth in 2032? Will society still exist at Christmas? Nobody really knows. Well that asteroid one, we sort of know that. We'll be fine. Yay science!

So anyway, the point of this article isn't to pile on CVE, it's to talk about trust, but not the sort of trust we usually talk about in security. We're usually talking about trust in the context of "can I trust that session isn't a Russian trying to steal my cat memes?". This is human trust, trust with the user story "As a human on Earth, can I ever trust CVE again?". While I could keep you on the edge of your seat during the entirety of this article, I'll ruin the ending. You can't trust CVE ever again, because you are a human, on Earth.

Why can't we trust CVE?

Estimated Views

479 [✓]

Calculated based on
audience size and social
engagement

Engagements

11 [✓]

Total number of social
engagements



Cybersecurity Conferences 2025 - 2026 | Over 3.4K Events

Discover expert insights on cybersecurity trends and best practices. Stay ahead with our...

38

Domain
Authority [?]

Provided by
MOZ

17.3K

Unique
Visits [?]

Provided by
SimilarWeb

🌐 ONLINE

Cybersecurity Conferences 2025 - 2026 | Over 3.4K...

infosec-conferences.com/

Be The First To Know: Cyber Events Alerts in Your State or Country

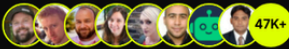
[About](#) [This Week](#) [Sitemap](#) [Need Registrations?](#) [Our Agency](#) [Blog](#) [Contact](#) [Submit Events](#)

Cybersecurity Conferences 2025 - 2026

All Security Conference Niches | Upcoming Cybersecurity Events

Our cybersecurity conference directory is meticulously updated and checked manually to prevent spam, ensuring it remains the community's premier resource for discovering top cybersecurity conferences, events, meetings, and seminars for 2024, 2025, and beyond. This carefully curated list caters to chief information security officers (CISOs), cybersecurity leaders, technology executives, and anyone passionate about the field.

Join Our Community

 47K+

[Speaking Opportunities](#) | [Ticket Discounts](#) | [Geo-Specific / Niche Event Alerts](#)

Show **50** entries

Event Name	Event Date	Event Type	Country	Region
SecretCon 4 2026	2026-06-04	Conference	United States	North America
SWISS GRC DAY 2026	2026-05-20	Conference	Switzerland	EMEA
Women In Technology 2026	2026-04-09	Conference	United States	North America
Cyber Leaders' Summit 2026	2026-04-07	Conference	United Kingdom	EMEA
CypherCon 9 2026	2026-04-01	Conference	United States	North America
Gen AI Conference NYC 2026	2026-03-23	Conference	United States	North America
International Conference on Cy...	2026-03-05	Conference	United States	North America

Estimated Views

3.23K [✓]

Calculated based on
audience size and social
engagement

Engagements

3 [✓]

Total number of social
engagements



Security Unscripted

"Security Unscripted" is a new podcast for insightful, no-nonsense discussions on the ever-evolving world of cybersecurity. In each shor...

87

Subscribers ?



April 16, 2025

YOUTUBE

Security Unscripted E08: CVE is dead... long live CVE!

youtube.com/watch?v=WfWp1i5Vroo

Views

211 ✓

Number of views

Engagements

14 ✓

Total number of social
engagements



Medium

On Medium, anyone can share insightful perspectives, useful knowledge, and life wisdom with the world.

95

Domain Authority ?

Provided by MOZ

April 16, 2025

ONLINE

We Name Hurricanes. We Track Diseases. But Now We're...

medium.com/@gabrielreissantos/we-nam...

Medium

Search

Write

Sign up

Sign in



We Name Hurricanes. We Track Diseases. But Now We're Ignoring Cyber Threats?



Gabriel Santos

Follow

4 min read · Apr 16, 2025



Today morning I came across this news and started wondering...

What happens when something invisible but absolutely essential just... stops?

Scrolling through LinkedIn, I saw a post claiming that MITRE would no longer issue CVEs, the globally recognized system for tracking cybersecurity vulnerabilities, because U.S. government funding had been cut. At first, I thought it was one of those overblown hot takes. But then I checked the source: The Hacker News, and sure enough, it's real. As of April 16, 2025, MITRE has lost federal support to continue running the CVE Program.

And honestly, I'm stunned. Not because I didn't think something like this *could* happen. But because it happened *without* any visible urgency, backup plan, or coordinated public response. For something as central to digital safety as CVEs? That's insane.

What Are CVEs and Why Do They Matter?

Imagine if every disease in the world had to be tracked manually by each hospital, in their own way, without any central database or naming system. One hospital calls it "New Flu," another says "Strain A2025," and a third just says "Some weird virus." Chaos, right?

That's basically what CVEs prevent, but for software vulnerabilities.



Medium

Read writing from Stephen Shaffer on Medium. Engineer focused on the intersection of cybersecurity and data science. Passionate about...

3

Domain
Authority [?]

Provided by
MOZ

April 16, 2025

🌐 ONLINE

Vulnerability Information Cones

[stephenshaffer.io/vulnerability-information...](https://stephenshaffer.io/vulnerability-information-cones)

Medium

🔍 Search

✍ Write

Sign up

Sign in



Vulnerability Information Cones

Applying Light Cones as a Mental Model for Navigating Uncertainty



Stephen Shaffer

Follow

7 min read · Apr 16, 2025



8



Inspiration

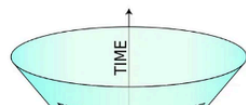
Note: I wrote this before the MITRE announcement regarding the CVE program funding. That is an evolving situation, but the mental model outlined here holds true regardless of the existence of the CVE program — our past light cone may be collectively degraded moving forward, but we will recover.

I spent the last week bouncing between my two favorite security conferences — FIRST's VulnCon in Raleigh (where I spoke) and BSidesCharm in Baltimore — and I was inspired to articulate my mental model of vulnerabilities, risk, and the decisions we make with imperfect information.

In order to do that, I need to be blunt. I'm kind of an astrophysics nerd in my spare time. So if any of this goes way over your head, I apologize in advance. It took me time to understand the concepts in the theory of relativity and on which my mental model is based.

Light Cones

Hearing folks talk about the data quality, what pieces of information mean to varying operators, and how we forecast risk made me think of a favorite physics concept of mine: light cones.



Links

3 [✓]

3 links to first.org

Rants of a deranged squirrel.

Rants of a Deranged Squirrel

13



Domain
Authority [?]

Provided by
MOZ

351

Unique
Visits [?]

Provided by
SimilarWeb

Enjoy this site?  Gift the author a WordPress.com plan. 

Gift



Rants of a Deranged Squirrel

[Home](#)

[About](#)

[Contact](#)



VulnCon Day 2 Errata & Taking Ben Edwards to Task



[4/13/2025 Update: See very end, below last image, for an amusing update.]

Today was the second day of [VulnCon 2025](#), a conference whose stated purpose is “to collaborate with various vulnerability management and cybersecurity professionals to develop forward leaning ideas that can be taken back to individual programs for action to benefit the vulnerability

April 09, 2025

 ONLINE

VulnCon Day 2 Errata & Taking Ben Edwards to Task

jericho.blog/2025/04/08/vulncon-day-2-e...

Estimated Views

275 [✓]

Calculated based on
audience size and social
engagement

Engagements

14 [✓]

Total number of social
engagements

Links

6 [✓]

6 links to first.org



Open Source Security

31

Domain
Authority [?]

Provided by
MOZ

1.25K

Unique
Visits [?]

Provided by
SimilarWeb

Open Source Security

[About](#) [Contact](#) [Feeds](#) [Search](#) [Archive](#)

Why I didn't go to VulnCon

April 11, 2025 · Josh Bressers



VulnCon 2025 is over. I didn't go. A bunch of people have asked me why, and rather than keep my answer to a small group, I thought it would make sense to write something public about it all.

The TL;DR is I went to a different conference that I thought was a better use of my time.

The conference I went to was [Cyphercon](#) and [BSides Milwaukee](#). They are regional conferences in Wisconsin. Good people, great shows, a lot of fun and learning. Yeah, it was technically the week before VulnCon, but I lack the fortitude to do two conferences back to back. Some people can, I tip my hat to those folks. I'm not one of them. I should be clear though, this isn't the only reason. I also don't think VulnCon should exist (more on that at the end).

Why do we go to conferences?

It would be easy to construct a gigantic list of why we go to conferences. But I think the two biggest are to meet people (the human connection is extremely valuable and important), and the second is to learn about the future of your industry.

April 11, 2025

ONLINE

Why I didn't go to VulnCon

opensourcsecurity.io/2025/04-why-i-did...

Estimated Views

466 [✓]

Calculated based on
audience size and social
engagement

Engagements

2 [✓]

Total number of social
engagements

Links

2 [✓]

2 links to first.org



DevCentral - an F5 Community

A community of F5 experts collaborating to solve challenges, share ideas, and discuss industry...

81

Domain Authority

Provided by
MOZ

26.6K

Unique Visits

Provided by
SimilarWeb

F5 Sites

Contact

DevCentral Community

Forums CrowdSRC Articles Groups Events Suggestions More Register Sign In

DevCentral > Articles > Security Insights

VulnCon 2025, EU CRA, CVE funding, Smishing Kit

Notable security news for the week of April 13th through April 20th. Your editor this week is Chris from the F5 Security Incident Response Team. A bit of a different format this week as I was in Raleigh for VulnCon 2025 the previous week. I will discuss highlights from that as well as notable events from the past week.

VulnCon 2025

The 2025 Vulnerability Management Ecosystem Collaboration, Ideation, and Action Conference (aka "VulnCon"), which was sponsored by FIRST and the CVE Program, was held from April 7th through April 10th this year. The aim of this conference is to promote collaboration between various vulnerability management and cybersecurity professionals to better help the whole cybersecurity ecosystem. Key topics that were highlighted this year were the EU's Cyber Resilience Act (CRA), Vulnerability Exploitability eXchange (VEX), Cybersecurity Assurance Framework (CSAF), and publishing more complete CVE records or Vulnrichment. I will discuss the CRA in the next paragraph. VEX facilitates the exchange of vulnerability information, fostering collaboration to swiftly address emerging threats. Concurrently, CSAF ensures a standardized approach to cybersecurity practices. One of the pushes that was discussed was to get security scanners to start ingesting VEX to help decrease the amount of false positives and focus more on vulnerabilities that are exploitable. As for Vulnrichment, it is alarming that a large number of CVEs that are disclosed every year do not include Common Weakness Enumerations (CWE) or Common Vulnerability Scoring System (CVSS) scores. I agree that adding this information at a minimum would be very beneficial to both the consumers as well as the vendor. The vendor is in the best position to assign these in a more accurate manner since they are most familiar with the products.

<https://www.first.org/conference/vulncon2025/>

<https://openssf.org/blog/2023/09/07/vdr-vex-openvex-and-csaf/>

EU Cyber Resilience Act (CRA)

The Cyber Resilience Act introduces mandatory cybersecurity requirements for hardware and software products, throughout their whole lifecycle. The main goals of

Related Content

VulnCon, NVD, XZ, and More - March 25-31, 2024 - F5 SIRT - Thi...
MegaZone · Apr 09, 2024
• Security Insights · 3 unread
F5 SIRT SECURITY TWIS
301 3 3

VulnCon, Big Brother, School Daze, and More - Jan 22nd-28th,...
MegaZone · Feb 05, 2024
• Security Insights
F5 SIRT RANSOMWARE SECURITY TWIS
185 1 0

Juice jacking attack and State-funded attacks - April 15th - 21st ...
Lior_Rotkovitch · Apr 27, 2023
• Security Insights
SECURITY TWIS
913 2 0

Show More

April 22, 2025

ONLINE

VulnCon 2025, EU CRA, CVE funding, Smishing Kit l...

[community.f5.com/kb/security-insights/vuln...](https://community.f5.com/kb/security-insights/vulncon-2025-eu-cra-cve-funding-smishing-kit-l...)

Estimated Views

147

Calculated based on audience size and social engagement

Links

1

1 link to first.org



Linux Security

Stay ahead with top Linux news, security advisories, expert how-to guides, and cutting-edge feature...

51


Domain
Authority [?]

Provided by
MOZ

27K


Unique
Visits [?]


Provided by
SimilarWeb




News ▾ Advisories ▾ HOWTOs ▾ Features ▾ Newsletters ▾ Polls ▾ About ▾f X in Login 🔍 [Sign Up](#)

Security Dictionary

Key Trends & Takeaways from VulnCon 2025

**Brittany Day** ⌚ 3 - 5 min read ⌚ Apr 28, 2025





[VulnCon 2025](#), recently held in Raleigh, NC, created a dynamic stage for security professionals and open-source advocates to connect, share, and collaborate on tackling some of today's most pressing challenges in vulnerability management and open-source software security. The conference buzzed with energy as industry experts, developers, and Linux admins unpacked the latest advancements, explored emerging trends, and exchanged actionable strategies to strengthen their security practices.

From groundbreaking solutions to practical methodologies, VulnCon 2025 provided attendees with the tools and insights needed to better protect the ecosystems they oversee. Let's dive into the key moments and powerful takeaways from this year's event.

Get the Latest News & Insights

Sign up to get the latest security news affecting Linux and open source delivered straight to your inbox

☒ Linux Advisory Watch

☒ Linux Security Week

[Subscribe](#)

LinuxSecurity Poll

How often do you reboot your Linux server?

☐ Only after a kernel update

☐ Once a month, just in case

☐ Never, uptime is king

☐ Wait... I was supposed to reboot?

[🗳️ Result](#) [🗳️ Vote](#)

April 28, 2025

🌐 ONLINE

Key Trends & Takeaways from VulnCon 2025

linuxsecurity.com/news/organizations-eve...

Estimated Views

384 [✓]

Calculated based on audience size and social engagement

Engagements

16 [✓]

Total number of social engagements

Links

1 [✓]

1 link to first.org



The Hacker News

The Hacker News is the top cybersecurity news platform, delivering real-time updates, threat...

88

Domain Authority

Provided by
MOZ

687K

Unique Visits

Provided by
SimilarWeb

Bits, Bytes, and Breaking News | Followed by 5.20+ million

The Hacker News

Subscribe - Get Latest News

Home Cyber Attacks Vulnerabilities Expert Insights Contact

RansomHub Went Dark April 1; Affiliates Fled to Qilin, DragonForce Claimed Control

Apr 30, 2025 Ravie Lakshmanan Cybercrime / Threat Intelligence



Cybersecurity researchers have revealed that [RansomHub's](#) online infrastructure has "inexplicably" gone offline as of April 1, 2025, prompting concerns among affiliates of the ransomware-as-a-service (RaaS) operation.

Singaporean cybersecurity company Group-IB [said](#) that this may have caused affiliates to migrate to Qilin, given that "disclosures on its DLS [data leak site] have doubled since February."

RansomHub, which first emerged in February 2024, is estimated to have stolen data from over 200 victims. It replaced two high-profile RaaS groups, LockBit and BlackCat, to become a frontrunner, courting their affiliates, including [Scattered Spider](#) and [Evil Corp](#), with lucrative payment splits.

"Following a possible acquisition of the web application and ransomware source code of Knight (formerly Cyclops), RansomHub quickly rose in the ransomware scene, thanks to the dynamic features of its multi-platform encryptor and an aggressive, affiliate-friendly model offering substantial financial incentives," Group-IB said in a report.

RansomHub's ransomware is designed to work on Windows, Linux, FreeBSD, and ESXi as well as on x86, x64, and ARM architectures, while avoiding attacking companies located in the Commonwealth of Independent States (CIS), Cuba, North Korea, and China. It can also encrypt local and remote file

Most Read News

- DHS Warns Pro-Iranian Hackers Likely to Target U.S. Networks After Iranian Nuclear Strikes
- Business Case for Agentic AI SOC Analysts
- Cyber Criminals Exploit Open-Source Tools to Compromise Financial Institutions Across...
- Weekly Recap: Airline Hacks, Citrix 0-Day, Outlook Malware, Banking Trojans and more
- U.S. House Bans WhatsApp on Official Devices Over Security and Data Protection Issues
- Beware the Hidden Risk in Your Extra Environment

View -> Trending Stories

Popular Resources

- Still Wasting Hours on SOC Alerts? Here's the AI Tool That Does It in Seconds
- A Lamented Truth: Modern SOC Data Resilience
- Guide: How to Find and Close Privilege Pathways Before Hackers Walk Right In

April 30, 2025

ONLINE

RansomHub Went Dark April 1; Affiliates Fled to Qilin,...

thehackernews.com/2025/04/ransomhub...

Estimated Views

2.32K

Calculated based on audience size and social engagement

Engagements

75

Total number of social engagements

Links

1

1 link to first.org

May 01, 2025

 ONLINE

Predictive analytics and legacy risk: Rajesh Kumar C G's...

techbullion.com/predictive-analytics-and-l...

Estimated Views

1.22K 

Calculated based on audience size and social engagement

HOME
TECH NEWS +
FINTECH +
BLOCKCHAIN +
BIG DATA
FINANCE
INTERVIEWS
PI

LATEST NEWS

Predictive analytics and legacy risk: Rajesh Kumar C G's blueprint for modern cybersecurity

By Anamta Shehzadi

Posted on May 1, 2025

Cybercriminals are leveraging increasingly advanced and sophisticated tools, but there is a way out.

According to the recent report, published by the [Forum of Incident Response and Security Teams](#), the number of detected vulnerabilities is expected to grow 11% in comparison with the year 2024, which also indicates a whopping 470% increase compared to 2023. The vulnerabilities can vary greatly in their scope, from code logic errors that need to be fixed to zero-day exploits that present a direct threat to the security of users' data or software stability.

Being an IEEE Member, a cybersecurity expert with vast experience, and a founder and CEO of INOVITSI consulting firm, Rajesh Kumar C G has a first-hand understanding of overcoming the challenges of modern cybersecurity. For over 18 years, he's helped government agencies and private enterprises in Australia reimagine how security frameworks should operate in the face of increasingly sophisticated attacks.

"Many companies still depend heavily on perimeter protection and static rules," Rajesh observes.

TRENDING STORIES

ARTIFICIAL INTELLIGENCE
What Are AI Co-Pilots in Social Media Management—and How Do They Work? Insights by Amplysphere OU

LATEST NEWS
Pakistani Passport: How to Apply, Types, and Travel with Your Passport to the World

CRYPTOCURRENCY
Top 4 Low-Cap Cryptos to Buy in 2025: BlockchainFX Joins Ethena, Ondo and Stellar

PRESS RELEASE
Status Unveils First Gasless L2 on Linea With 100% Community Yield Allocation Mechanism

PRESS RELEASE
MultiBank Group Announces Early Access Waitlist for Pioneering \$MBG Token

TECHNOLOGY
Vital Translate Buds Complaints Explained (2025 Consumer Reports) Here's What You Should Know Before Buying

TECHNOLOGY
How to Rank on LLMs: A Complete Guide to Boost Visibility on ChatGPT, Perplexity & Other AI Platforms

BUSINESS NEWS
Top Legitimate Crypto Recovery Companies: A Guide

BUSINESS NEWS
Best Solution for Asset Protection in 2025: Myne Global Explained



The Cyber Post

Cybersecurity news daily. Enjoy the latest hacker news. Cyber security reports on cybercrime,...

13

Domain
Authority [?]

Provided by
MOZ

80

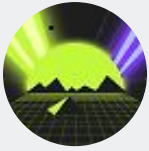
Unique
Visits [?]

Provided by
SimilarWeb

🌐 ONLINE

Database Error

thecyberpost.com/news/hackers/ransom...



The CTO Club

35

Domain
Authority [?]

Provided by
MOZ

156K

Unique
Visits [?]

Provided by
SimilarWeb

March 21, 2024

🌐 ONLINE

17 Cybersecurity Conferences to Explore Industry...

thectoclub.com/career/best-cybersecurity...

THE CTO CLUB
Build SaaS teams and
systems that scale.



CAREER

17 Cybersecurity Conferences to Explore Industry Trends in 2025

QUICK SUMMARY

Explore the best cybersecurity conferences of 2025. Connect with peers, learn from experts, and address pressing challenges to boost your career and knowledge.



Estimated Views

32.9K [✓]

Calculated based on
audience size and social
engagement

Links

4 [✓]

4 links to first.org



Disaster Recovery Journal

DRJ is the largest resource for business continuity, disaster recovery, crisis communication, and risk...

50

Domain Authority [?]

Provided by
MOZ

6.04K

Unique Visits [?]

Provided by
SimilarWeb

May 07, 2025

🌐 ONLINE

Fortifying Your Defenses: Ransomware...

drj.com/journal_main/fortifying-your-defe...

Estimated Views

104 [✓]

Calculated based on audience size and social engagement

Engagements

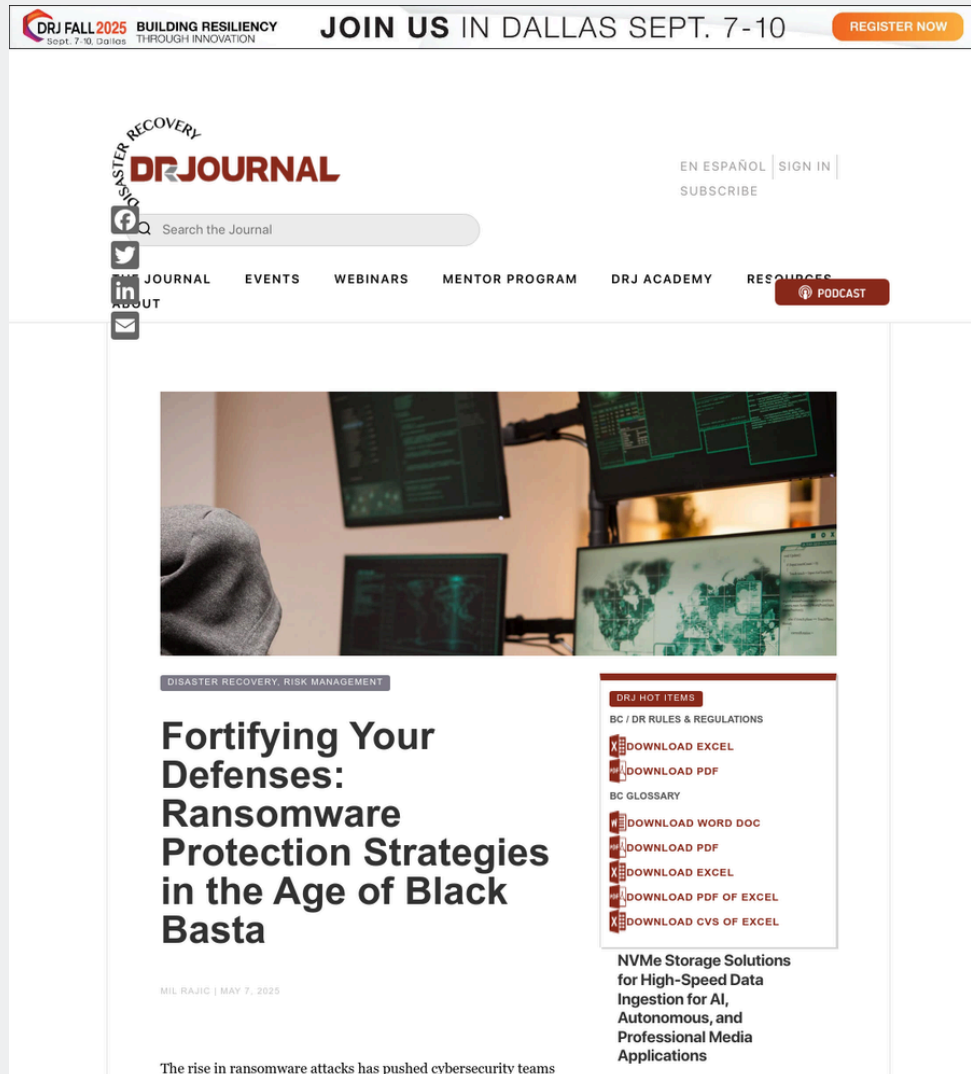
14 [✓]

Total number of social engagements

Links

1 [✓]

1 link to first.org





The Hacker News

The Hacker News is the top cybersecurity news platform, delivering real-time updates, threat...

88

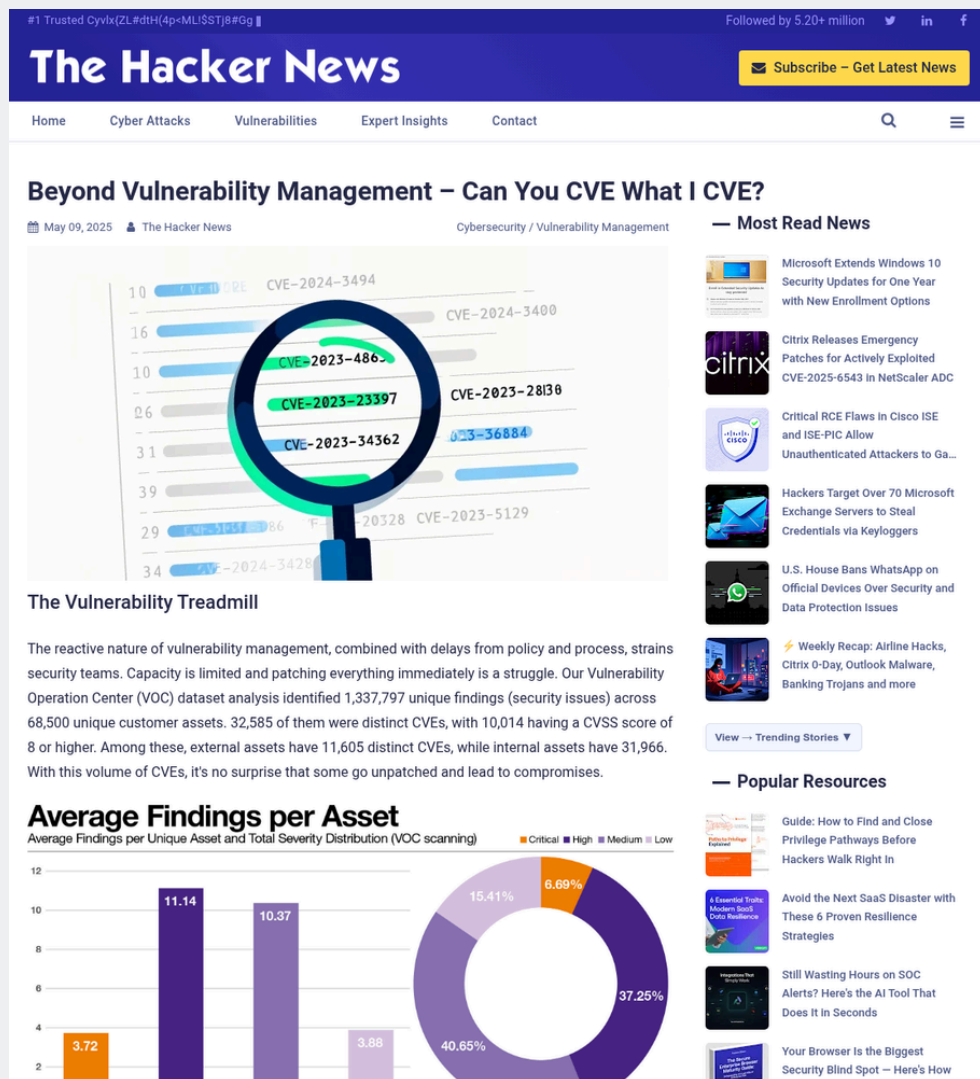
Domain
Authority [?]

Provided by
MOZ

687K

Unique
Visits [?]

Provided by
SimilarWeb



May 09, 2025

ONLINE

Beyond Vulnerability Management – Can You CVE What I CVE?

thehackernews.com/2025/05/beyond-vul...

Estimated Views

2.31K [✓]

Calculated based on audience size and social engagement

Engagements

73 [✓]

Total number of social engagements

Links

3 [✓]

3 links to first.org



DevCentral - an F5 Community

A community of F5 experts collaborating to solve challenges, share ideas, and discuss industry...

81

Domain Authority

Provided by
MOZ

26.6K

Unique Visits

Provided by
SimilarWeb

May 08, 2025

ONLINE

The Future Soon I DevCentral

community.f5.com/kb/security-insights/th...

F5 Sites

Contact

DevCentral Community

Forums CrowdsRC Articles Groups Events Suggestions More Register Sign In

DevCentral > Articles > Security Insights

The Future Soon

It's the first May, first of May, outdoor... Oh, hi, didn't see you there. Welcome back, once again, to This Week In Security, the weekly (mostly weekly) newsletter where we take the random security news of the week and run it down. I'm your host this week, @MegaZone, and these are the items that happened to catch my eye for the week of April 27th to May 3rd, as I once again drank from the firehose of doom, or security news, same thing.

But before I jump in, I just need to say... Signalgate. What? Or any of its sequels so far — the latest news is just insane. Just when you think the cybersecurity clown show can't get any worse, or more ridiculous, it does. I suspect that if anyone reading this right now did anything half as inept as some of our most trusted government officials, it would mean instant termination. It's really frustrating working to try to improve security only to see those who should take it the most seriously utterly trashing it. It's disheartening, really. But her emails.

Anyway, let's jump into it...

Good Morning Tucson

It was a few weeks ago, but as this is my first TWIS since, I'm going to talk about VulnCon a bit. VulnCon 2025 was held April 7–10 in Raleigh, NC, for the second year in a row—but it will *not* be back next year. As revealed at the end of the event, and on the [FIRST Events](#) page for 2026 and 2027, VulnCon is moving to Arizona - but actually Scottsdale, not Tucson. It is relocating to the [DoubleTree Resort by Hilton, Paradise Valley](#), held April 13–16, 2026. This is a resort with an attached convention facility, so we'll be able to stay on-site. We'll also have more space, allowing for more content and more attendees. We don't want to grow too quickly, and this facility should be good for at least the next couple of years.

I'll miss Raleigh. The last few years have been fun because I've been able to explore the area, find interesting places, and go back to some of my favorite places. The McKimmon Center at NC State has been a decent facility for us, but we've outgrown it and needed to find a new place. I've never been to Scottsdale, so that'll be a new experience.

Back to this year — VulnCon was bigger and better in its second year. I may be biased, as a member of the program committee, but I was impressed by [the presentations](#) I personally attended and I've talked to a number of others who felt the same. This year we had four days, up from three, and more simultaneous rooms on most days, meaning

Related Content

Securing Generative AI: Defending the Future of Innovation and...
Jordan_Zebor · Jul 19, 2023
• Technical Articles · 2 unread
AI F5 SIRT SECURITY
2.1K 7 2

Exploring Agentic AI: Ethics, Quantum Computing, and the...
AubreyKingF5 · Dec 20, 2024
• Technical Articles · 2 unread
AI
115 1 2

Hack to the Future: The Results
ltwagnon · Sep 04, 2018
• Technical Articles · 3 unread
APPLICATION DELIVERY BIG-IP
433 0 3

[Show More](#)

Estimated Views

147

Calculated based on audience size and social engagement

Links

5

5 links to first.org



Foresight

Foresight provides in depth insights into the business of innovation to help you figure out the...

19

Domain Authority [?]

Provided by
MOZ

650

Unique Visits [?]

Provided by
SimilarWeb

fore/sight

The Business of Innovation

Long ReadsTopicsNewsletterEventsAboutinXSubscribeQ

Artificial IntelligenceCyberFuture TelecomsMaterialsNet zeroQuantumRobotics



Events & Conferences:
Cybersecurity

Cyber

Essential cybersecurity conferences

Cybersecurity events and conferences to watch

 **By David Maher Roberts** / 16 May 25 / Reading time: 4 mins

With the pace of cybersecurity innovation continuing to accelerate, the 2025 calendar is packed with high-profile events that cater to academics, businesses, and governmental organisations alike. As global cyber threats evolve, these conferences offer the chance to dive deep into topics such as AI-driven cybersecurity, [quantum computing's impact on cryptography](#), processor security and more. Whether you are an industry professional, researcher, or just keen to keep up with emerging trends, these events will give you the insights and connections you need to stay at the forefront of the field.

Many of these conferences are hybrid, allowing for both in-person and online participation, making them accessible from wherever you are in the world.

Get your Foresight Digest every two weeks, straight to your inbox.

Subscribe

Most popular

[Quantum,](#)
Quantum computing in 2025: risk and reward
Reading time: 10 mins

[Quantum,](#)
"The utility and the..."

May 16, 2025

🌐 ONLINE

Essential cybersecurity conferences -...

biforesight.com/cyber/essential-cybersec...

Estimated Views

335 [✓]

Calculated based on audience size and social engagement

Engagements

2 [✓]

Total number of social engagements

Links

1 [✓]

1 link to first.org



TechAfrica News

The leading independant B2B news platform in Africa and the Middle East

32
Domain
Authority

Provided by
MOZ

69.4K
Unique
Visits

Provided by
SimilarWeb

Today's Bulletin: July 10, 2025

TechAfrica News News The TechAfrica News Podcast #TechTalkThursday Orbiting Innovations Video Events

#SECURITY

Cameroon Strengthens Cybersecurity Through International Collaboration and Capacity Building

May 23, 2025 1 min read Author: Aayushya Ranjan

Cameroon partners with FIRST to train IT security teams, boost cyber defense skills, and strengthen infrastructure resilience against digital threats.

The TechAfrica News Podcast

EP01 | Minister... The TechAfrica N...
DRIVING SOUTH AFRICA'S DIGITAL FUTURE

Follow us on LinkedIn
Go to Our Page

NEWSLETTER SIGNUP
Sign up for our weekly newsletter and get the latest industry insights right in your inbox!

Name
Your Email
Company
Position
Sign Up

TechAfrica News
YOUR COMPETITORS FOLLOW US. WHY DON'T YOU?

May 23, 2025 ONLINE

Cameroon Strengthens Cybersecurity...

techafricanews.com/2025/05/23/camero...

Estimated Views **18.3K**

Calculated based on audience size and social engagement

Engagements **12**

Total number of social engagements



The Register: Enterprise Technology News and Analysis

Enterprise technology news for IT decision-makers and professionals

90

Domain Authority

Provided by MOZ

1.74M

Unique Visits

Provided by SimilarWeb

May 26, 2025

ONLINE

TeleMessage security SNAFU worsens

theregister.com/2025/05/26/security_in_...

SIGN IN / UP

The Register

SECURITY

11

TeleMessage security SNAFU worsens as 60 government staffers exposed

PLUS: Interpol kills more malware; GoDaddy settles in awful infosec case; Giant stolen creds DB exposed

iain.thomson

Mon 26 May 2025 04:28 UTC

INFOSEC IN BRIEF

Secrets of the Trump administration may have been exposed after a successful attack on messaging service TeleMessage, which has been used by some officials.

Evidence of an attack on administration officials appeared last week on [leak site](#) Distributed Denial of Secrets, hosted an archive of messages that included details of over 60 government workers, a White House staffer, and members of the Secret Service.

The leak, [first reported](#) by Reuters, isn't as serious as [Signalgate](#) - no one was discussing air strikes and possible war crimes - but it's still suboptimal.

The White House said that it was "aware of the cyber security incident" but didn't comment further.

TeleMessage servers are reportedly closed while an investigation is carried out.

Operation Endgame II takes out malware

Europol had already detailed attempts to take down the [Qakbot](#) and [Danabot](#) malware groups, and last Friday it announced the disruption of the following five malware crews:

- Bumblebee
- Lactroductus
- Hijackloader
- Trickbot
- Warmcookie

Operation Endgame II, a combined operation involving police from the EU, UK, US, and Canada, has now led to 20 arrests and 18 suspects have been added to the EU's [most wanted list](#). In addition a total of €21.2 million has been seized.

"This new phase demonstrates law enforcement's ability to adapt and strike again, even as cybercriminals retool and reorganise," [said](#) Catherine De Bolle, Europol executive director. "By disrupting the services criminals rely on to deploy ransomware, we are breaking the kill chain at its source."

Estimated Views

4.93K

Calculated based on audience size and social engagement

Engagements

46

Total number of social engagements

FIRST's Q2FY25 PR Coverage

40



Infosecrity Magazine

The award winning online magazine dedicated to the strategy, insight and technology of information...

74

Domain Authority

Provided by
MOZ

131K

Unique Visits

Provided by
SimilarWeb

Infosecrity Magazine

Log InSign Up

NewsTopicsFeaturesWebinarsWhite PapersPodcastsEventsDirectory

Infosecrity Magazine Home » News » NIST Introduces New Metric to Measure Likelihood of Vulnerability Exploits

NEWS 26 MAY 2025
NIST Introduces New Metric to Measure Likelihood of Vulnerability Exploits

Kevin Poireault
Reporter, Infosecrity Magazine
Follow @Kpoireault Connect on LinkedIn

The US National Institute of Standards and Technology (NIST) has launched a new metric to assess the likelihood that a vulnerability is being exploited.

In [a technical white paper](#), published on May 19, NIST introduced a new metric called Likely Exploited Vulnerabilities (LEV) to help organizations determine if a product vulnerability has been exploited.

The LEV calculation guides prioritization efforts and builds upon the existing Exploit Prediction Scoring System (EPSS).

EPSS is a data-driven scoring system introduced in 2018 by a team within the Forum of Incident Response and Security Teams (FIRST).

EPSS predicts the likelihood of a vulnerability

You may also like

NEWS 23 MAY 2024
NVD Leaves Exploited Vulnerabilities Unchecked

NEWS 25 APR 2025
SAP Fixes Critical Vulnerability After Evidence of Exploitation

NEWS 14 MAY 2024
NIST Confusion Continues as Cyber Pros Complain CVE Uploads Stalled

NEWS 16 APR 2024
Cybersecurity Pros Urge US Congress to Help NIST Restore NVD Operation

NEWS 30 MAY 2025
CISA Urged to Enrich KEV Catalog with

May 26, 2025

ONLINE

NIST Launches Metric to Measure Likelihood of Vulnerability...

infosecrity-magazine.com/news/nist-met...

Estimated Views

987

Calculated based on audience size and social engagement

Engagements

60

Total number of social engagements



IT Brew

From cybersecurity and big data to cloud computing, IT Brew covers the latest trends shapin...

39

Domain
Authority [?]

Provided by
MOZ

19.1K

Unique
Visits [?]

Provided by
SimilarWeb

June 05, 2025

🌐 ONLINE

CISA churn leaves some private sector partners wondering...

itbrew.com/stories/2025/06/05/cisa-churn...

IT BREW

Stories ▾

Topics ▾

Resources ▾

Events ▾

Newsletter ▾

Q

IT OPERATIONS

CISA churn leaves some private sector partners wondering what's next

"I think CISA has a really important role in the broader ecosystem of cybersecurity in this country," Mitre's Mark Bristow tells IT Brew.



Douglas Rissing/Getty Images

By Eoin Higgins

JUNE 5, 2025 • 3 MIN READ

IT teams are familiar with tight budgets, but the federal government should be

Estimated Views

3.25K [✓]

Calculated based on
audience size and social
engagement

Engagements

4 [✓]


Total number of social
engagements



IT Brew

From cybersecurity and big data to cloud computing, IT Brew covers the latest trends shapin...

39

Domain Authority 

Provided by
MOZ

19.1K

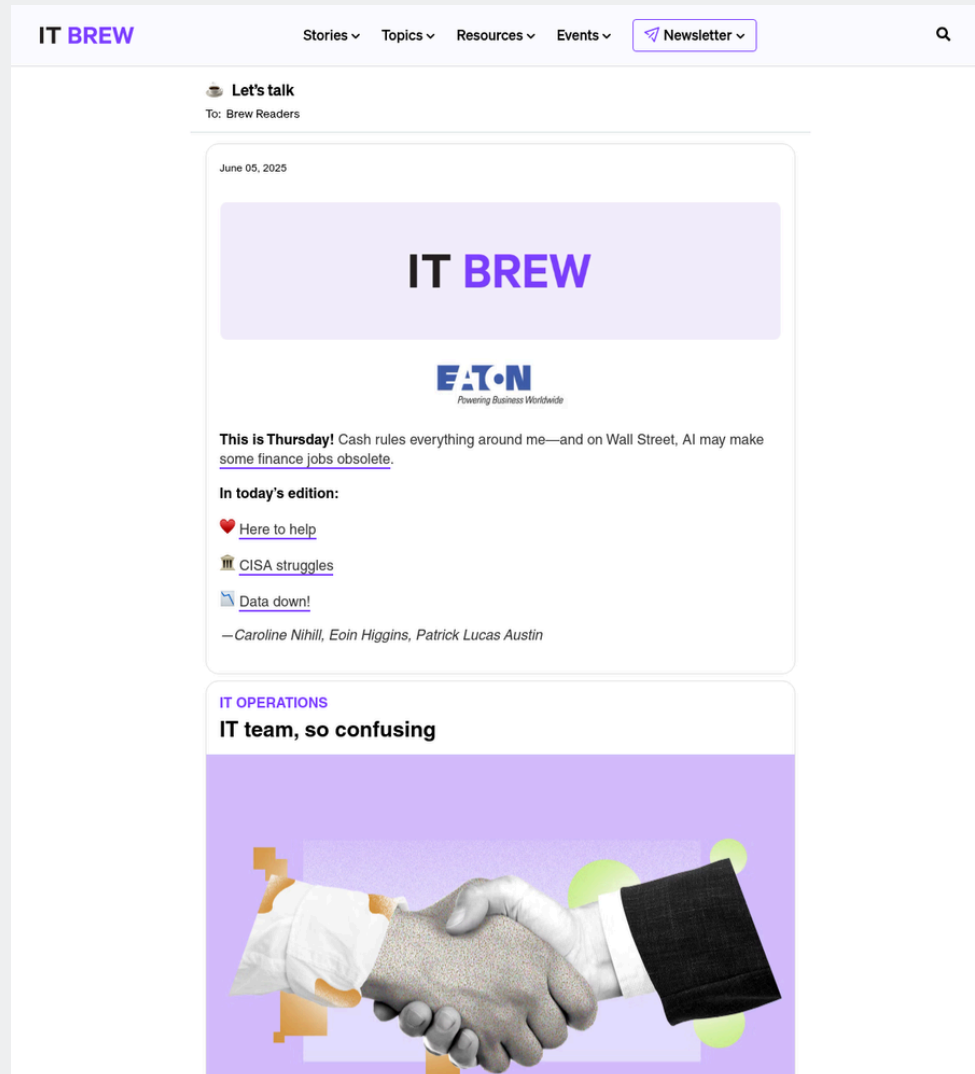
Unique Visits 

Provided by
SimilarWeb

 ONLINE

IT Brew

itbrew.com/issues/let-s-talk?mbcid=40174...



Estimated Views

3.24K 

Calculated based on
audience size and social
engagement



Built In | Tech Jobs Personalized

Built In is the online community for National startups and tech companies. Find startup jobs, tech news...

70

Domain
Authority [?]

Provided by
MOZ

1.61M

Unique
Visits [?]

Provided by
SimilarWeb

How Cybersecurity Teams Can Stay Ahead in 2025 and Beyond

Chat logs from cyber threat group Black Basta reveal that a company's greatest vulnerability is its overlooked infrastructure. Here's what that means for cybersecurity defense.

Written by [Éireann Leverett](#)
Published on Jun. 05, 2025

Summary: Ransomware tactics are growing stealthier, exploiting overlooked infrastructure and old vulnerabilities. Defenders must shift from reactive patching to proactive planning and collaboration to stay ahead.

This year is shaping up to be a turning point in defense tactics.

We've already seen major disruptions across the [ransomware](#) ecosystem. Groups like LockBit and RansomHub have gone dark or been disrupted, prompting a flurry of speculation. But if

June 05, 2025

🌐 ONLINE

How Cybersecurity Teams Can Stay Ahead in 2025 and...

builtin.com/articles/cybersecurity-ransom...

Estimated Views

12K [✓]

Calculated based on audience size and social engagement

Engagements

25 [✓]

Total number of social engagements

Links

2 [✓]

2 links to first.org



IT Brew

From cybersecurity and big data to cloud computing, IT Brew covers the latest trends shapin...

39

Domain
Authority [?]

Provided by
MOZ

19.1K

Unique
Visits [?]

Provided by
SimilarWeb

June 10, 2025

🌐 ONLINE

Vendor contract negotiations offer opportunity,...

itbrew.com/stories/2025/06/10/vendor-co...

IT **BREW**

Stories ▾

Topics ▾

Resources ▾

Events ▾

Subscribe ▾

Q

IT STRATEGY

Vendor contract negotiations offer opportunity, frustration for buyers

"Vendors are not vendors, they're partners," West Monroe Partner Nate Buniva tells IT Brew.



Ljubaphoto/Getty Images

By **Eoin Higgins**

JUNE 10, 2025 • 4 MIN READ

Contracting out work to third-party IT vendors is often challenging.

From licensing issues, regulations forcing companies to submit multiple bids, and

Estimated Views

3.24K ✓

Calculated based on
audience size and social
engagement

Engagements

1 ✓

Total number of social
engagements



Turning Servers Against the Cloud – Communications of...

cacm.acm.org/news/turning-servers-agai...

COMMUNICATIONS
ACM

Explore Topics ▾ Latest Issue ▾ 🔍 Sign In Join ACM →


NEWS

Architecture and Hardware

Turning Servers Against the Cloud

Server-Side Request Forgery attacks targeted vulnerabilities in applications and platforms running on cloud servers.

By David Geer
Posted Jun 12 2025



[Share](#) [Print](#) [Join the Discussion](#)

You expect the guardians at the gate of any system to keep attacks out; you don't expect them to turn against internal systems and networks and ravage those on behalf of threat actors. Yet that's what happened with cloud servers: they turned against internal systems.

In March 2025, Server-Side Request Forgery (SSRF) attacks targeting cloud servers allowed attackers to send

Related Reading

[Practice](#)
A View of Cloud Computing
Architecture and Hardware

Estimated Views

285 [✓]

Calculated based on
audience size and social
engagement

Engagements

1 [✓]

Total number of social
engagements

Links

1 [✓]

1 link to first.org



CSO Online

CSO delivers the critical information about trends, practices, and products enterprise security leaders...

85

Domain Authority

Provided by
MOZ

211K

Unique Visits

Provided by
SimilarWeb

July 07, 2025

ONLINE

How to conduct an effective post-incident review

csoonline.com/article/4009438/how-to-c...

Estimated Views

854

Calculated based on audience size and social engagement

Engagements

47

Total number of social engagements

The new CSOonline.com hybrid search: Explore CSO content smarter, faster and AI powered. Try it!

Home • Security • How to conduct an effective post-incident review

by Bob Violino
Contributing writer

in

How to conduct an effective post-incident review

Feature
Jun 20, 2025 • 9 mins

Incident Response Security Practices

Mitigation and remediation aren't the endpoints of incident response. Having a structured process to analyze and learn from a cybersecurity incident once it has been resolved is paramount to improving security operations.

Credit: PeopleImages.com - Yuri A / Shutterstock

Let's say your organization has experienced a cybersecurity incident that had no material impact on the business but nevertheless rattled the security team and got the attention of senior management. Somehow the



DEV Community

A space to discuss and keep up software development and manage your software career

83

Domain Authority

Provided by
MOZ

3.29M

Unique Visits

Provided by
SimilarWeb

June 25, 2025

ONLINE

A New Era of Code Quality: Beyond bugs to supply chain...

dev.to/lizzzzz/a-new-era-of-code-qualityb...

DEV

Find related posts...

Powered by Algolia

Log in

Create account

3

2

0

...

Liz Acosta
Posted on Jun 25 • Originally published at Medium

3

A New Era of Code Quality: Beyond bugs to supply chain security and dependency health

codequality #sbom #dependencymanagement

Code quality (4 Part Series)

- Code That Won't Cost You: Coding best practices for any l...
- Passing the Vibe Check: Navigating the changing develop...
- A New Era of Code Quality: Beyond bugs to supply cha...**
- A New Era of Code Quality: Beyond bugs and into legal lice...

In today's interconnected software landscape, most applications don't just spring up from thin air. Developers are constantly pulling in countless open-source libraries, frameworks, and other third-party components to speed things up and reuse existing solutions. And why not? If a specialized solution already exists for a particular problem, why reinvent the wheel? However, while efficient, this reliance opens up a massive new vulnerability: the software supply chain.

This article is designed to accommodate different learning and reading styles, so feel free to jump ahead:

- [Weak links: Anatomy of a supply chain attack and the new](#)

Liz Acosta
Follow

Film student -> Marketer -> Engineer
-> Developer Advocate -> Developer
Content Manager ... just your typical
DevRel journey! Lover of plants,
pizza, pugs, and Python.

LOCATION
San Francisco, CA

PRONOUNS
she/her/hers

WORK
Developer Advocate

JOINED
Nov 24, 2020

More from Liz Acosta

A New Era of Code Quality: Beyond bugs and into legal license compliance and risk management
#codequality #sbom #sonar #dependencymanagement

Code That Won't Cost You: Coding best practices for any language to increase code quality and reduce developer toil
#codequality #bestpractices #sonarqube

Comparing CodiumAI PR-Agent to Copilot for Pull Request
#ai #pullrequest #productivity #codequality

AWS PROMOTED

Estimated Views

14.4K

Calculated based on audience size and social engagement

Links

4

4 links to first.org



Disaster Recovery Journal

DRJ is the largest resource for business continuity, disaster recovery, crisis communication, and risk...

50

Domain
Authority [?]

Provided by
MOZ

6.04K

Unique
Visits [?]

Provided by
SimilarWeb

June 30, 2025

🌐 ONLINE

Internet Safety Month: What Cybersecurity...

drj.com/industry_news/internet-safety-mo...

DRJ FALL 2025
Sept. 7-10, Dallas

BUILDING RESILIENCY
THROUGH INNOVATION

JOIN US IN DALLAS SEPT. 7-10

REGISTER NOW

DRJ JOURNAL

EN ESPAÑOL | SIGN IN |
SUBSCRIBE

Search the Journal

JOURNAL

EVENTS

WEBINARS

MENTOR PROGRAM

DRJ ACADEMY

RESOURCES

ABOUT

PODCAST

Internet Safety Month: What Cybersecurity Leaders Say We're Getting Wrong and How to Fix It

June 30, 2025

June marks National Internet Safety Month, and many organizations return to familiar checklists: update software, rotate passwords, back up your files. While those steps remain useful, today's cybersecurity challenges are far more complex. From AI-driven attacks to global ransomware campaigns, defending digital infrastructure now requires a broader, more strategic approach.

To understand how cybersecurity must evolve in 2025 and beyond, we asked industry leaders to weigh in. Their insights point to a common theme: building smarter systems, improving collaboration, and treating cybersecurity as an organization-wide priority. This isn't just about technology anymore. It's about culture, coordination, and staying a step ahead in a constantly shifting threat landscape.

Resilience Is the New Cybersecurity Imperative

"In a world where everything runs on digital infrastructure, strong passwords and data backups aren't enough to keep you safe," said Rob Gutierrez, Senior Cybersecurity and Compliance Manager at [Secureframe](#). "It's about building

Recent Posts

NVMe Storage Solutions for High-Speed Data Ingestion for AI, Autonomous, and Professional Media Applications
July 10, 2025

Abstract Security Delivers 4X Operational Efficiency at Juul Labs
July 9, 2025

Fortinet Report: OT Cybersecurity Risk Elevates within Executive Leadership Ranks
July 9, 2025

EGGER Group Achieves 99.99% Uptime Across Global Operations with SIOS LifeKeeper for Linux
July 9, 2025

Aligned's Phoenix Data Center Earns Three Green Globes Certification
July 9, 2025

Estimated Views

84 [✓]

Calculated based on audience size and social engagement

Engagements

1 [✓]

Total number of social engagements

Links

1 [✓]

1 link to first.org



FIRST Announces New CORE Initiative with Fortinet as a...

cyberdefensewire.com/first-announces-n...

Call us Toll Free (USA): 1-833-844-9468 International: +1-603-280-4451 M-F 8am to 6pm EST

Cyber Defense Magazine Cyber Defense Awards Cyber Defense Webinars Cyber Defense Conferences Cyber Defense TV Cyber Defense Radio Subscribe

CYBERDEFENSE Wire Home Press Releases Contact [Submit a Press Release](#)

FIRST Announces New CORE Initiative with Fortinet as a Founding Partner

in [Twitter](#) [Facebook](#) [Email](#) [+](#)

New initiative empowers cybersecurity and incident response teams worldwide through capacity building and community development

June 23, 2025 – The Forum of Incident Response and Security Teams (FIRST), a leading global cybersecurity non-profit, today introduced its **CORE** (Community, Operational capacity, Resilience, and Empowerment) initiative with **Fortinet** as its founding partner.

FIRST CORE is a strategic program designed to enhance incident response capabilities around the world, sharing the expertise and insights of the global incident response community through tailored initiatives to help improve cybersecurity. This new effort will build on FIRST's long history of education, training, and knowledge sharing within the international cybersecurity community.

"Fortinet's leadership as our founding partner demonstrates their commitment to strengthening cybersecurity knowledge across industries and borders. Together, we're building communities grounded in internationally recognized best practices that will enhance incident response capabilities across the globe," said Chris Gibson, CEO, FIRST.

FIRST CORE will provide critical funding to expand the organization's Community and Capacity Building Program (CCB), which focuses on developing incident response capabilities in regions where resources are limited. This program builds on FIRST's long history of education, training, and knowledge sharing within the international security community.

The CORE program will support capacity building priorities, such as:

- Developing new and updated incident response training content

Download Cyber Defense Magazine July Edition for 2025

[Download eMag](#)

Published monthly by Cyber Defense Magazine, this resource shares a wealth of information to help you stay one step ahead of the next cyber threat.

Estimated Views

602 ✓

Calculated based on audience size and social engagement

Links

4 ✓

4 links to first.org



Fortinet

Fortinet delivers cybersecurity everywhere you need it. We secure the entire digital attack surface...

83

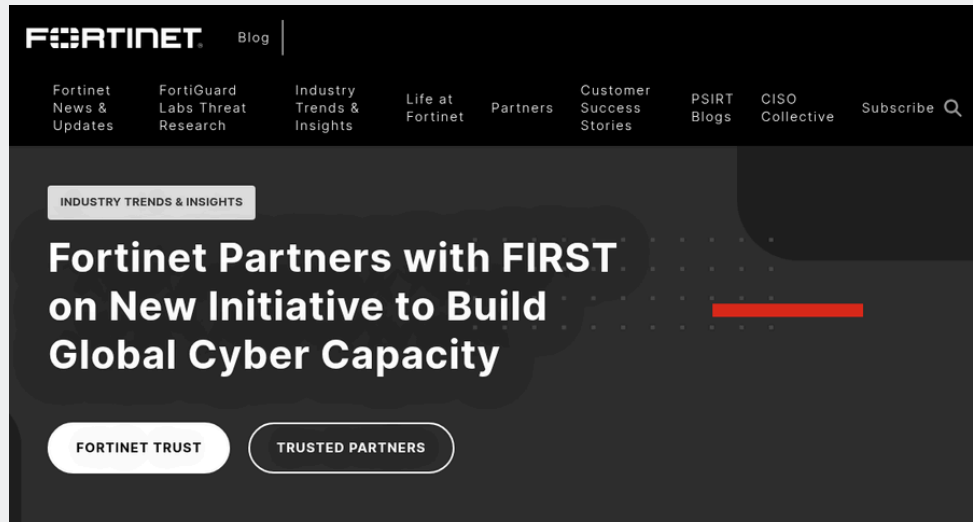
Domain Authority

Provided by
MOZ

1.54M

Unique Visits

Provided by
SimilarWeb



By **Derek Manky** | June 23, 2025

Under-resourced regions around the globe face a growing list of challenges that significantly impact cyber resilience, including rapidly expanding digital adoption efforts, limited cybersecurity expertise, and increasingly sophisticated threat actors targeting global networks. The recent wave of ransomware attacks targeting critical infrastructure in developing nations, combined with the growing use of these geographic areas as launching pads for new cybercrime groups, underscores a sobering truth: Investing in building cyber capacity isn't only about helping individual countries protect themselves; it's about strengthening the security of our entire interconnected digital ecosystem.

Given this reality, cultivating public-private partnerships is vital to enhancing cyber resilience everywhere. That's why I'm excited to share that Fortinet is a founding partner of the all-new Forum of Incident Response and Security Teams (**FIRST**) initiative, Community, Operational capacity, Resilience, and Empowerment (CORE), an effort designed to empower cybersecurity and incident response teams worldwide through capacity building and community development.

Fortinet: Trust Is Our Business

Learn about Fortinet innovation, collaboration partners, product security processes, and about our enterprise-grade products.

[Learn More](#)

June 23, 2025

ONLINE

Fortinet Partners with FIRST on New Initiative to Build...

fortinet.com/blog/industry-trends/fortinet-...

Estimated Views

10.1K

Calculated based on audience size and social engagement

Links

4

4 links to first.org



Disaster Recovery Journal

DRJ is the largest resource for business continuity, disaster recovery, crisis communication, and risk...

50

Domain
Authority [?]

Provided by



6.04K

Unique
Visits [?]

Provided by



June 23, 2025

🌐 ONLINE

FIRST Announces New CORE Initiative with Fortinet as a...

drj.com/industry_news/first-announces-n...

DRJ FALL 2025
Sept. 7-10, Dallas

BUILDING RESILIENCY
THROUGH INNOVATION

JOIN US IN DALLAS SEPT. 7-10

REGISTER NOW

DRJ JOURNAL

EN ESPAÑOL | SIGN IN |
SUBSCRIBE

Search the Journal

JOURNAL | EVENTS | WEBINARS | MENTOR PROGRAM | DRJ ACADEMY | RESOURCES | ABOUT |

PODCAST

FIRST Announces New CORE Initiative with Fortinet as a Founding Partner

June 23, 2025

New initiative empowers cybersecurity and incident response teams worldwide through capacity building and community development

The Forum of Incident Response and Security Teams (FIRST), a leading global cybersecurity non-profit, today introduced its CORE (Community, Operational capacity, Resilience, and Empowerment) initiative with Fortinet as its founding partner.

FIRST CORE is a strategic program designed to enhance incident response capabilities around the world, sharing the expertise and insights of the global incident response community through tailored initiatives to help improve cybersecurity. This new effort will build on FIRST's long history of education, training, and knowledge sharing within the international cybersecurity community.

"Fortinet's leadership as our founding partner demonstrates their commitment to strengthening cybersecurity knowledge across industries and borders.

Recent Posts

Abstract Security Delivers 4X Operational Efficiency at Juul Labs
July 9, 2025

Fortinet Report: OT Cybersecurity Risk Elevates within Executive Leadership Ranks
July 9, 2025

EGGER Group Achieves 99.99% Uptime Across Global Operations with SIOS LifeKeeper for Linux
July 9, 2025

Aligned's Phoenix Data Center Earns Three Green Globes Certification
July 9, 2025

Portnox Unleashes Fast, Frictionless, Cloud-Native ZTNA
July 8, 2025

Blue Mantis to Empower Massachusetts

Estimated Views

84 [✓]

Calculated based on audience size and social engagement

Engagements

1 [✓]

Total number of social engagements

Links

3 [✓]

3 links to first.org



Infosecurity Magazine

The award winning online magazine dedicated to the strategy, insight and technology of information...

74

Domain Authority [?]

Provided by
MOZ

131K

Unique Visits [?]

Provided by
SimilarWeb

June 24, 2025

🌐 ONLINE

Cyber Intel Pros and Hobbyists Can Now Report Threats...

infosecurity-magazine.com/news/cyber-in-...

Infösecurity Magazine Log In Sign Up

News Topics Features Webinars White Papers Podcasts Events Directory

Infosecurity Magazine Home » News » Cyber Intel Pros and Hobbyists Can Now Report Threats Anonymously

NEWS 24 JUN 2025

Cyber Intel Pros and Hobbyists Can Now Report Threats Anonymously

Kevin Poireault
Reporter, Infosecurity Magazine
Follow @Kpoireault Connect on LinkedIn

You may also like

- INTERVIEW** 20 NOV 2020
Interview: Richard Betts and Eward Driehuis, Cybersprint
- NEWS FEATURE** 4 NOV 2020
Top Ten: Things Learned from the NCSC Annual Report
- OPINION** 12 OCT 2020
#HowTo Launch a Remote SOC
- NEWS** 7 NOV 2019
SecureData CTO Names Three Pillars of Active Defense
- NEWS** 4 OCT 2019
#VB2019: Cyber Threat Alliance Cites Vendor Collaboration Benefits

Estimated Views

919 ✓

Calculated based on audience size and social engagement

Engagements

15 ✓

Total number of social engagements

ChannelLife US

ChannelLife US is a live news website with regular email newsletters dedicated to the US's technology channel, in...

10

Domain
Authority [?]

Provided by
MOZ

248

Unique
Visits [?]

Provided by
SimilarWeb

June 24, 2025

🌐 ONLINE

FIRST launches CORE Fund to boost global cyber response skills

channellife.news/story/first-launches-core...

Estimated Views

156 [✓]

Calculated based on
audience size and social
engagement

ChannelLife US - Industry insider news for technology resellers


ChannelLife
UNITED STATES

TechDay

Guides

cloud services # cybersecurity # distributors # microsoft # partner programmes

Search



firewalls # ransomware # it training

FIRST launches CORE Fund to boost global cyber response skills

Tue, 24th Jun 2025

Related stories

- Cynomi adds impact analysis & continuity to vCISO platform
- AppOmni secures FedRAMP Moderate ATO for SaaS security platform
- Platform9 & Commvault partner to boost private cloud security
- Bitdefender & Creators Guild unite to protect digital creators
- Aryaka wins global SASE award & G2 leader for customer focus

By Shannon Williams, Journalist

FIRST has launched the CORE Fund, a global initiative to strengthen cybersecurity incident response capabilities in under-resourced regions, with Fortinet as the founding partner.

The Forum of Incident Response and Security Teams (FIRST), an international non-profit organisation, has announced the formation of the CORE (Community, Operational capacity, Resilience, and Empowerment) initiative to expand the operational capacities of cybersecurity teams around the world. The programme is set to focus especially on regions that currently have limited resources to defend against growing cyber threats such as ransomware.

Programme objectives

FIRST CORE is designed as a strategic programme to enhance incident response capabilities by leveraging guidance and experience from the global incident response community. Recent efforts have begun in Africa and the Caribbean, and there are plans to expand activities into the Asia-Pacific and Latin America regions.

The initiative includes several targeted measures such as the development of updated incident response training content, subsidising local training costs for partners from lower-income

IT Brief US

Dedicated to IT decision-makers at enterprise, corporate, and government organisations throughout the US. These are...

14

Domain
Authority [?]

Provided by
MOZ

1.74K

Unique
Visits [?]

Provided by
SimilarWeb

June 24, 2025

🌐 ONLINE

FIRST launches CORE Fund to boost global cyber response skills

itbrief.news/story/first-launches-core-fund...

Estimated Views

1.1K [✓]

Calculated based on
audience size and social
engagement

IT Brief US - Technology news for CIOs & IT decision-makers

ITBrief
UNITED STATES


TechDay

Guides

artificial intelligence # digital transformation # disaster recovery # hybrid & remote work # internet of things

Search

... 🔍



firewalls # ransomware # it training

FIRST launches CORE Fund to boost global cyber response skills

Tue, 24th Jun 2025

Related stories

- Cynomi adds impact analysis & continuity to vCISO platform
- AppOmni secures FedRAMP Moderate ATO for SaaS security platform
- Platform9 & Commvault partner to boost private cloud security
- Zyxel advances Secure by Design for global SMB networking security

By Shannon Williams, Journalist

FIRST has launched the CORE Fund, a global initiative to strengthen cybersecurity incident response capabilities in under-resourced regions, with Fortinet as the founding partner.

The Forum of Incident Response and Security Teams (FIRST), an international non-profit organisation, has announced the formation of the CORE (Community, Operational capacity, Resilience, and Empowerment) initiative to expand the operational capacities of cybersecurity teams around the world. The programme is set to focus especially on regions that currently have limited resources to defend against growing cyber threats such as ransomware.

Programme objectives



SecurityBrief US

SecurityBrief US is focused on cybersecurity and cyberattack news. Its readers include business an...

13

Domain
Authority [?]

Provided by
MOZ

735

Unique
Visits [?]

Provided by
SimilarWeb

SecurityBrief US - Technology news for CISOs & cybersecurity decision-makers

SecurityBrief

UNITED STATES

TechDay

Guides

cloud security # cybersecurity # endpoint protection # firewalls # ransomware

Search

... 🔍



firewalls # ransomware # it training

FIRST launches CORE Fund to boost global cyber response skills

Tue, 24th Jun 2025

Related stories

Red Hat unveils no-cost Linux platform for business developers

Bitdefender & Creators Guild unite to protect digital creators

Organisations urged to boost data resilience as AI adoption rises

Huntress & Microsoft partner to boost business cybersecurity

Over half of global companies leave email systems exposed to phishing



By Shannon Williams, Journalist

FIRST has launched the CORE Fund, a global initiative to strengthen cybersecurity incident response capabilities in under-resourced regions, with Fortinet as the founding partner.

The Forum of Incident Response and Security Teams (FIRST), an international non-profit organisation, has announced the formation of the CORE (Community, Operational capacity, Resilience, and Empowerment) initiative to expand the operational capacities of cybersecurity teams around the world. The programme is set to focus especially on regions that currently have limited resources to defend against growing cyber threats such as ransomware.

Programme objectives

FIRST CORE is designed as a strategic programme to enhance incident response capabilities by leveraging guidance and experience from the global incident response community. Recent efforts have begun in Africa and the Caribbean, and there are plans to expand activities into the Asia-Pacific and Latin America regions.

The initiative includes several targeted measures such as the development of updated incident response training content, subsidising local training costs for partners from lower-income

June 24, 2025

🌐 ONLINE

FIRST launches CORE Fund to boost global cyber response skills

securitybrief.news/story/first-launches-cor...

Estimated Views

477 [✓]

Calculated based on
audience size and social
engagement



IT Brief Asia

Dedicated to IT decision-makers at enterprise, corporate, and government organisations...

33

Domain Authority

Provided by
MOZ

8.36K

Unique Visits

Provided by
SimilarWeb

June 24, 2025

ONLINE

FIRST launches CORE Fund to boost global cyber response skills

itbrief.asia/story/first-launches-core-fund-t...

Estimated Views

2.36K

Calculated based on audience size and social engagement

IT Brief Asia - Technology news for CIOs & IT decision-makers

ITBrief

ASIA

TechDay

Guides

artificial intelligence # digital transformation # disaster recovery # hybrid & remote work # internet of things

Search

...

firewalls # ransomware # it training

FIRST launches CORE Fund to boost global cyber response skills

Tue, 24th Jun 2025

Related stories

Zyxel advances Secure by Design for global SMB networking security

Red Hat unveils no-cost Linux platform for business developers

NCS launches SGD \$130 million programme to boost AI in Asia Pacific

Organisations urged to boost data resilience as AI adoption rises

By Shannon Williams, Journalist

FIRST has launched the CORE Fund, a global initiative to strengthen cybersecurity incident response capabilities in under-resourced regions, with Fortinet as the founding partner.

The Forum of Incident Response and Security Teams (FIRST), an international non-profit organisation, has announced the formation of the CORE (Community, Operational capacity, Resilience, and Empowerment) initiative to expand the operational capacities of cybersecurity teams around the world. The programme is set to focus especially on regions that currently have limited resources to defend against growing cyber threats such as ransomware.

Programme objectives



SecurityBrief Asia

SecurityBrief Asia is focused on cybersecurity and cyberattack news. Its readers include business an...

42

Domain
Authority [?]

Provided by
MOZ

4.55K

Unique
Visits [?]

Provided by
SimilarWeb

SecurityBrief Asia - Technology news for CISOs & cybersecurity decision-makers

SecurityBrief

ASIA

TechDay

Guides

cloud security # cybersecurity # endpoint protection # firewalls # ransomware

Search

...



firewalls # ransomware # it training

FIRST launches CORE Fund to boost global cyber response skills

Tue, 24th Jun 2025

Related stories

Huntress & Microsoft partner to boost business cybersecurity

Over half of global companies leave email systems exposed to phishing

Keymou+ blurs hacktivism & commerce amid 700 DDoS attacks

July Patch Tuesday reveals 137 vulnerabilities

Ben Dawson named new Cisco APJC President as Dave West shifts role



By Shannon Williams, Journalist

FIRST has launched the CORE Fund, a global initiative to strengthen cybersecurity incident response capabilities in under-resourced regions, with Fortinet as the founding partner.

The Forum of Incident Response and Security Teams (FIRST), an international non-profit organisation, has announced the formation of the CORE (Community, Operational capacity, Resilience, and Empowerment) initiative to expand the operational capacities of cybersecurity teams around the world. The programme is set to focus especially on regions that currently have limited resources to defend against growing cyber threats such as ransomware.

Programme objectives

FIRST CORE is designed as a strategic programme to enhance incident response capabilities by leveraging guidance and experience from the global incident response community. Recent efforts have begun in Africa and the Caribbean, and there are plans to expand activities into the Asia-Pacific and Latin America regions.

The initiative includes several targeted measures such as the development of updated incident response training content, subsidising local training costs for partners from lower-income

June 24, 2025

🌐 ONLINE

FIRST launches CORE Fund to boost global cyber response skills

securitybrief.asia/story/first-launches-core...

Estimated Views

659 [✓]

Calculated based on audience size and social engagement



ChannelLife Australia

ChannelLife Australia is a live news website with regular email newsletters dedicated to Australia's...

44

Domain
Authority [?]

Provided by
MOZ

11K

Unique
Visits [?]

Provided by
SimilarWeb

June 24, 2025

🌐 ONLINE

FIRST launches CORE Fund to boost global cyber response skills

channellife.com.au/story/first-launches-co...

Estimated Views

1.31K [✓]

Calculated based on
audience size and social
engagement

ChannelLife

AUSTRALIA

TechDay

Guides

cloud services # cybersecurity # distributors # microsoft # partner programmes

Search

...

firewalls # ransomware # it training

FIRST launches CORE Fund to boost global cyber response skills

Tue, 24th Jun 2025

Related stories

Deepfake & AI crime surge poses major threat to business trust

Fraud, friction, and the future: Prioritising trust in a high-stakes market

Manual certificate management costs Australian firms over USD \$250,000

Aryaka wins global SASE award & G2 leader for customer focus

Huntress & Microsoft partner to boost business cybersecurity

By Shannon Williams, Journalist

FIRST has launched the CORE Fund, a global initiative to strengthen cybersecurity incident response capabilities in under-resourced regions, with Fortinet as the founding partner.

The Forum of Incident Response and Security Teams (FIRST), an international non-profit organisation, has announced the formation of the CORE (Community, Operational capacity, Resilience, and Empowerment) initiative to expand the operational capacities of cybersecurity teams around the world. The programme is set to focus especially on regions that currently have limited resources to defend against growing cyber threats such as ransomware.

Programme objectives

FIRST CORE is designed as a strategic programme to enhance incident response capabilities by leveraging guidance and experience from the global incident response community. Recent efforts have begun in Africa and the Caribbean, and there are plans to expand activities into the Asia-Pacific and Latin America regions.

The initiative includes several targeted measures such as the development of updated incident response training content, subsidising local training costs for partners from lower-income

FIRST's Q2FY25 PR Coverage

59



IT Brief Australia

IT Brief is a live news website and weekly email newsletter dedicated to IT Managers & CIO's at...

47

Domain
Authority [?]

Provided by
MOZ

27.5K

Unique
Visits [?]

Provided by
SimilarWeb

June 24, 2025

🌐 ONLINE

FIRST launches CORE Fund to boost global cyber response skills

itbrief.com.au/story/first-launches-core-fu...

Estimated Views

1.55K [✓]

Calculated based on
audience size and social
engagement

IT Brief Australia - Technology news for CIOs & IT decision-makers

ITBrief
AUSTRALIA


TechDay

Guides

artificial intelligence # digital transformation # disaster recovery # hybrid & remote work # internet of things

Search

... 🔍



firewalls # ransomware # it training

FIRST launches CORE Fund to boost global cyber response skills

Tue, 24th Jun 2025


Related stories

Deepfake & AI crime surge poses major threat to business trust

Zyxel advances Secure by Design for global SMB networking security

Red Hat unveils no-cost Linux platform for business developers

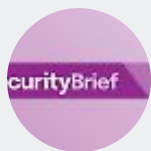
NCS launches SGD \$130 million programme to boost AI in Asia Pacific

 By Shannon Williams, Journalist

FIRST has launched the CORE Fund, a global initiative to strengthen cybersecurity incident response capabilities in under-resourced regions, with Fortinet as the founding partner.

The Forum of Incident Response and Security Teams (FIRST), an international non-profit organisation, has announced the formation of the CORE (Community, Operational capacity, Resilience, and Empowerment) initiative to expand the operational capacities of cybersecurity teams around the world. The programme is set to focus especially on regions that currently have limited resources to defend against growing cyber threats such as ransomware.

Programme objectives



SecurityBrief Australia

SecurityBrief Australia is focused on cybersecurity and cyberattack news. Its readers include busines...

45

Domain
Authority [?]

Provided by
MOZ

10.7K

Unique
Visits [?]

Provided by
SimilarWeb

June 24, 2025

🌐 ONLINE

FIRST launches CORE Fund to boost global cyber response skills

securitybrief.com.au/story/first-launches-c...

Estimated Views

964 [✓]

Calculated based on
audience size and social
engagement

SecurityBrief Australia - Technology news for CISOs & cybersecurity decision-makers

SecurityBrief
AUSTRALIA


TechDay

Guides

cloud security # cybersecurity # endpoint protection # firewalls # ransomware

Search

...



firewalls # ransomware # it training

FIRST launches CORE Fund to boost global cyber response skills

Tue, 24th Jun 2025

Related stories


Five use cases that justify ditching VPNs for good

Fraud, friction, and the future: Prioritising trust in a high-stakes market

Manual certificate management costs Australian firms over USD \$250,000

Huntress & Microsoft partner to boost business cybersecurity

Over half of global companies leave email systems exposed to phishing

 By Shannon Williams, Journalist

FIRST has launched the CORE Fund, a global initiative to strengthen cybersecurity incident response capabilities in under-resourced regions, with Fortinet as the founding partner.

The Forum of Incident Response and Security Teams (FIRST), an international non-profit organisation, has announced the formation of the CORE (Community, Operational capacity, Resilience, and Empowerment) initiative to expand the operational capacities of cybersecurity teams around the world. The programme is set to focus especially on regions that currently have limited resources to defend against growing cyber threats such as ransomware.

Programme objectives

FIRST CORE is designed as a strategic programme to enhance incident response capabilities by leveraging guidance and experience from the global incident response community. Recent efforts have begun in Africa and the Caribbean, and there are plans to expand activities into the Asia-Pacific and Latin America regions.

The initiative includes several targeted measures such as the development of updated incident response training content, subsidising local training costs for partners from lower-income



ChannelLife New Zealand

ChannelLife NZ is a live news website with regular email newsletters dedicated to New Zealand's...

42

Domain
Authority [?]

Provided by
MOZ

2.64K

Unique
Visits [?]

Provided by
SimilarWeb

June 24, 2025

🌐 ONLINE

FIRST launches CORE Fund to boost global cyber response skills

channellife.co.nz/story/first-launches-core...

Estimated Views

383 [✓]

Calculated based on
audience size and social
engagement

ChannelLife New Zealand - Industry insider news for technology resellers

ChannelLife
NEW ZEALAND

TechDay

Guides

cloud services # cybersecurity # distributors # microsoft # partner programmes

Search

... 🔍



firewalls # ransomware # it training

FIRST launches CORE Fund to boost global cyber response skills

Tue, 24th Jun 2025

Related stories

- HCLTech signs 10-year deal to modernise Dunedin IT services
- Aryaka wins global SASE award & G2 leader for customer focus
- Huntress & Microsoft partner to boost business cybersecurity
- Over half of global companies leave email systems exposed to phishing
- Juniper named Leader in Gartner's Magic Quadrant for fifth year

By Shannon Williams, Journalist

FIRST has launched the CORE Fund, a global initiative to strengthen cybersecurity incident response capabilities in under-resourced regions, with Fortinet as the founding partner.

The Forum of Incident Response and Security Teams (FIRST), an international non-profit organisation, has announced the formation of the CORE (Community, Operational capacity, Resilience, and Empowerment) initiative to expand the operational capacities of cybersecurity teams around the world. The programme is set to focus especially on regions that currently have limited resources to defend against growing cyber threats such as ransomware.

Programme objectives

FIRST CORE is designed as a strategic programme to enhance incident response capabilities by leveraging guidance and experience from the global incident response community. Recent efforts have begun in Africa and the Caribbean, and there are plans to expand activities into the Asia-Pacific and Latin America regions.

The initiative includes several targeted measures such as the development of updated incident response training content, subsidising local training costs for partners from lower-income



IT Brief New Zealand

Dedicated to IT decision-makers at enterprise, corporate, and government organisations...

46

Domain Authority

Provided by
MOZ

6.44K

Unique Visits

Provided by
SimilarWeb

June 24, 2025

ONLINE

FIRST launches CORE Fund to boost global cyber response skills

itbrief.co.nz/story/first-launches-core-fund...

Estimated Views

556

Calculated based on audience size and social engagement

IT Brief New Zealand - Technology news for CIOs & IT decision-makers

ITBrief
NEW ZEALAND

Guides

artificial intelligence # digital transformation # disaster recovery # hybrid & remote work # internet of things

Search

...

firewalls # ransomware # it training

FIRST launches CORE Fund to boost global cyber response skills

Tue, 24th Jun 2025

Related stories

- Deepfake & AI crime surge poses major threat to business trust
- Zyxel advances Secure by Design for global SMB networking security
- Red Hat unveils no-cost Linux platform for business developers
- NCS launches SGD \$130 million programme to boost AI in Asia Pacific

By Shannon Williams, Journalist

FIRST has launched the CORE Fund, a global initiative to strengthen cybersecurity incident response capabilities in under-resourced regions, with Fortinet as the founding partner.

The Forum of Incident Response and Security Teams (FIRST), an international non-profit organisation, has announced the formation of the CORE (Community, Operational capacity, Resilience, and Empowerment) initiative to expand the operational capacities of cybersecurity teams around the world. The programme is set to focus especially on regions that currently have limited resources to defend against growing cyber threats such as ransomware.

Programme objectives



SecurityBrief New Zealand

SecurityBrief New Zealand is focused on cybersecurity and cyberattack news. Its readers...

44

Domain
Authority [?]

Provided by
MOZ

3.36K

Unique
Visits [?]

Provided by
SimilarWeb

June 24, 2025

🌐 ONLINE

FIRST launches CORE Fund to boost global cyber response skills

securitybrief.co.nz/story/first-launches-cor...

Estimated Views

369 [✓]

Calculated based on
audience size and social
engagement

SecurityBrief New Zealand - Technology news for CISOs & cybersecurity decision-makers


SecurityBrief
NEW ZEALAND

TechDay

Guides

cloud security # cybersecurity # endpoint protection # firewalls # ransomware

Search



firewalls # ransomware # it training

FIRST launches CORE Fund to boost global cyber response skills

Tue, 24th Jun 2025

Related stories

- Organisations urged to boost data resilience as AI adoption rises
- Five use cases that justify ditching VPNs for good
- Huntress & Microsoft partner to boost business cybersecurity
- Over half of global companies leave email systems exposed to phishing
- Trend Micro invests in Pacific as regional cybersecurity surges

By Shannon Williams, Journalist

FIRST has launched the CORE Fund, a global initiative to strengthen cybersecurity incident response capabilities in under-resourced regions, with Fortinet as the founding partner.

The Forum of Incident Response and Security Teams (FIRST), an international non-profit organisation, has announced the formation of the CORE (Community, Operational capacity, Resilience, and Empowerment) initiative to expand the operational capacities of cybersecurity teams around the world. The programme is set to focus especially on regions that currently have limited resources to defend against growing cyber threats such as ransomware.

Programme objectives

FIRST CORE is designed as a strategic programme to enhance incident response capabilities by leveraging guidance and experience from the global incident response community. Recent efforts have begun in Africa and the Caribbean, and there are plans to expand activities into the Asia-Pacific and Latin America regions.

The initiative includes several targeted measures such as the development of updated incident response training content, subsidising local training costs for partners from lower-income



ChannelLife UK

ChannelLife UK is a live news website with regular email newsletters dedicated to the United...

29

Domain
Authority [?]

Provided by
MOZ

2.49K

Unique
Visits [?]

Provided by
SimilarWeb

June 24, 2025

🌐 ONLINE

FIRST launches CORE Fund to boost global cyber response skills

channellife.co.uk/story/first-launches-core...

Estimated Views

942 [✓]

Calculated based on
audience size and social
engagement

ChannelLife

UNITED KINGDOM

TechDay

Guides

cloud services # cybersecurity # distributors # microsoft # partner programmes

Search

... 🔍



firewalls # ransomware # it training

FIRST launches CORE Fund to boost global cyber response skills

Tue, 24th Jun 2025

Related stories


SUSE launches EU-based support to meet digital sovereignty needs

DE-CIX welcomes GRASS-MERKUR & IP-Max as premium partners

e2e-assure & Validato partner to bolster public sector cyber defences

Cynomi adds impact analysis & continuity to vCISO platform

Aryaka wins global SASE award & G2 leader for customer focus



By Shannon Williams, Journalist

FIRST has launched the CORE Fund, a global initiative to strengthen cybersecurity incident response capabilities in under-resourced regions, with Fortinet as the founding partner.

The Forum of Incident Response and Security Teams (FIRST), an international non-profit organisation, has announced the formation of the CORE (Community, Operational capacity, Resilience, and Empowerment) initiative to expand the operational capacities of cybersecurity teams around the world. The programme is set to focus especially on regions that currently have limited resources to defend against growing cyber threats such as ransomware.

Programme objectives

FIRST CORE is designed as a strategic programme to enhance incident response capabilities by leveraging guidance and experience from the global incident response community. Recent efforts have begun in Africa and the Caribbean, and there are plans to expand activities into the Asia-Pacific and Latin America regions.

The initiative includes several targeted measures such as the development of updated incident response training content, subsidising local training costs for partners from lower-income



IT Brief UK

Dedicated to IT decision-makers at enterprise, corporate, and government organisations...

32

Domain Authority [?]

Provided by
MOZ

4.28K

Unique Visits [?]

Provided by
SimilarWeb

June 24, 2025

🌐 ONLINE

FIRST launches CORE Fund to boost global cyber response skills

itbrief.co.uk/story/first-launches-core-fund...

Estimated Views

1.41K [✓]

Calculated based on audience size and social engagement

IT Brief UK - Technology news for CIOs & IT decision-makers

ITBrief
UNITED KINGDOM


TechDay

Guides

artificial intelligence # digital transformation # disaster recovery # hybrid & remote work # internet of things

Search

... 🔍



firewalls # ransomware # it training

FIRST launches CORE Fund to boost global cyber response skills

Tue, 24th Jun 2025

Related stories

- SUSE launches EU-based support to meet digital sovereignty needs
- DE-CIX welcomes GRASS-MERKUR & IP-Max as premium partners
- e2e-assure & Validato partner to bolster public sector cyber defences
- Cynomi adds impact analysis & continuity to vCISO platform

By Shannon Williams, Journalist

FIRST has launched the CORE Fund, a global initiative to strengthen cybersecurity incident response capabilities in under-resourced regions, with Fortinet as the founding partner.

The Forum of Incident Response and Security Teams (FIRST), an international non-profit organisation, has announced the formation of the CORE (Community, Operational capacity, Resilience, and Empowerment) initiative to expand the operational capacities of cybersecurity teams around the world. The programme is set to focus especially on regions that currently have limited resources to defend against growing cyber threats such as ransomware.

Programme objectives



SecurityBrief UK

SecurityBrief UK is focused on cybersecurity and cyberattack news. Its readers include business an...

34

Domain
Authority [?]

Provided by
MOZ

7.62K

Unique
Visits [?]

Provided by
SimilarWeb

SecurityBrief UK - Technology news for CISOs & cybersecurity decision-makers

SecurityBrief

UNITED KINGDOM

TechDay

Guides

cloud security # cybersecurity # endpoint protection # firewalls # ransomware

Search

... 🔍



firewalls # ransomware # it training

FIRST launches CORE Fund to boost global cyber response skills

Tue, 24th Jun 2025

Related stories

Red Hat unveils no-cost Linux platform for business developers

Organisations urged to boost data resilience as AI adoption rises

Huntress & Microsoft partner to boost business cybersecurity

IDnow bolsters global leadership to boost digital trust vision

Younger Brits help safeguard elders as online scams surge



By Shannon Williams, Journalist

FIRST has launched the CORE Fund, a global initiative to strengthen cybersecurity incident response capabilities in under-resourced regions, with Fortinet as the founding partner.

The Forum of Incident Response and Security Teams (FIRST), an international non-profit organisation, has announced the formation of the CORE (Community, Operational capacity, Resilience, and Empowerment) initiative to expand the operational capacities of cybersecurity teams around the world. The programme is set to focus especially on regions that currently have limited resources to defend against growing cyber threats such as ransomware.

Programme objectives

FIRST CORE is designed as a strategic programme to enhance incident response capabilities by leveraging guidance and experience from the global incident response community. Recent efforts have begun in Africa and the Caribbean, and there are plans to expand activities into the Asia-Pacific and Latin America regions.

The initiative includes several targeted measures such as the development of updated incident response training content, subsidising local training costs for partners from lower-income

June 24, 2025

🌐 ONLINE

FIRST launches CORE Fund to boost global cyber response skills

securitybrief.co.uk/story/first-launches-cor...

Estimated Views

1.93K [✓]

Calculated based on
audience size and social
engagement



ChannelLife India

ChannelLife India is a live news website with regular email newsletters dedicated to India's technology...

15

Domain
Authority [?]

Provided by
MOZ

1.29K

Unique
Visits [?]

Provided by
SimilarWeb

June 24, 2025

🌐 ONLINE

FIRST launches CORE Fund to boost global cyber response skills

channellife.in/story/first-launches-core-fu...

Estimated Views

794 [✓]

Calculated based on
audience size and social
engagement

ChannelLife

INDIA

TechDay

Guides

cloud services # cybersecurity # distributors # microsoft # partner programmes

Search

...

firewalls # ransomware # it training

FIRST launches CORE Fund to boost global cyber response skills

Tue, 24th Jun 2025

Related stories

Aryaka wins global SASE award & G2 leader for customer focus

Huntress & Microsoft partner to boost business cybersecurity

Over half of global companies leave email systems exposed to phishing

Juniper named Leader in Gartner's Magic Quadrant for fifth year

Ben Dawson named new Cisco APJC President as Dave West shifts role

By Shannon Williams, Journalist

FIRST has launched the CORE Fund, a global initiative to strengthen cybersecurity incident response capabilities in under-resourced regions, with Fortinet as the founding partner.

The Forum of Incident Response and Security Teams (FIRST), an international non-profit organisation, has announced the formation of the CORE (Community, Operational capacity, Resilience, and Empowerment) initiative to expand the operational capacities of cybersecurity teams around the world. The programme is set to focus especially on regions that currently have limited resources to defend against growing cyber threats such as ransomware.

Programme objectives

FIRST CORE is designed as a strategic programme to enhance incident response capabilities by leveraging guidance and experience from the global incident response community. Recent efforts have begun in Africa and the Caribbean, and there are plans to expand activities into the Asia-Pacific and Latin America regions.

The initiative includes several targeted measures such as the development of updated incident response training content, subsidising local training costs for partners from lower-income



IT Brief India

IT Brief is a live news website and weekly email newsletter dedicated to IT Managers & CIO's at...

15

Domain Authority

Provided by
MOZ

1.74K

Unique Visits

Provided by
SimilarWeb

June 24, 2025

ONLINE

FIRST launches CORE Fund to boost global cyber response skills

itbrief.in/story/first-launches-core-fund-to-...

Estimated Views

1.02K

Calculated based on audience size and social engagement

IT Brief India - Technology news for CIOs & IT decision-makers

ITBrief INDIA

TechDay

Guides

artificial intelligence # digital transformation # disaster recovery # hybrid & remote work # internet of things

Search

...

firewalls # ransomware # it training

FIRST launches CORE Fund to boost global cyber response skills

Tue, 24th Jun 2025

Related stories

- Zyxel advances Secure by Design for global SMB networking security
- Red Hat unveils no-cost Linux platform for business developers
- Organisations urged to boost data resilience as AI adoption rises
- Aryaka wins global SASE award & G2 leader for customer focus

By Shannon Williams, Journalist

FIRST has launched the CORE Fund, a global initiative to strengthen cybersecurity incident response capabilities in under-resourced regions, with Fortinet as the founding partner.

The Forum of Incident Response and Security Teams (FIRST), an international non-profit organisation, has announced the formation of the CORE (Community, Operational capacity, Resilience, and Empowerment) initiative to expand the operational capacities of cybersecurity teams around the world. The programme is set to focus especially on regions that currently have limited resources to defend against growing cyber threats such as ransomware.

Programme objectives



SecurityBrief India

SecurityBrief India is focused on cybersecurity and cyberattack news. Its readers include business an...

20

Domain
Authority [?]

Provided by
MOZ

1.27K

Unique
Visits [?]

Provided by
SimilarWeb

SecurityBrief India - Technology news for CISOs & cybersecurity decision-makers

SecurityBrief

INDIA

TechDay

Guides

cloud security # cybersecurity # endpoint protection # firewalls # ransomware

Search

...



firewalls # ransomware # it training

FIRST launches CORE Fund to boost global cyber response skills

Tue, 24th Jun 2025

Related stories

Over half of global companies leave email systems exposed to phishing

Keymous+ blurs hacktivism & commerce amid 700 DDoS attacks

July Patch Tuesday reveals 137 vulnerabilities

Ben Dawson named new Cisco APJC President as Dave West shifts role

Bugcrowd names Umesh Shankar to board, bolstering AI security



By Shannon Williams, Journalist

FIRST has launched the CORE Fund, a global initiative to strengthen cybersecurity incident response capabilities in under-resourced regions, with Fortinet as the founding partner.

The Forum of Incident Response and Security Teams (FIRST), an international non-profit organisation, has announced the formation of the CORE (Community, Operational capacity, Resilience, and Empowerment) initiative to expand the operational capacities of cybersecurity teams around the world. The programme is set to focus especially on regions that currently have limited resources to defend against growing cyber threats such as ransomware.

Programme objectives

FIRST CORE is designed as a strategic programme to enhance incident response capabilities by leveraging guidance and experience from the global incident response community. Recent efforts have begun in Africa and the Caribbean, and there are plans to expand activities into the Asia-Pacific and Latin America regions.

The initiative includes several targeted measures such as the development of updated incident response training content, subsidising local training costs for partners from lower-income

June 24, 2025

🌐 ONLINE

FIRST launches CORE Fund to boost global cyber response skills

securitybrief.in/story/first-launches-core-f...

Estimated Views

652 [✓]

Calculated based on audience size and social engagement

Engagements

2 [✓]

Total number of social engagements

ChannelLife Canada

ChannelLife Canada is a live news website with regular email newsletters dedicated to Canada's technology channel, in...

2

Domain
Authority [?]

Provided by
MOZ

589

Unique
Visits [?]

Provided by
SimilarWeb

June 24, 2025

🌐 ONLINE

FIRST launches CORE Fund to boost global cyber response skills

channellife.ca/story/first-launches-core-fu...

Estimated Views

480 [✓]

Calculated based on
audience size and social
engagement

ChannelLife

CANADA

TechDay

Guides

cloud services # cybersecurity # distributors # microsoft # partner programmes

Search



firewalls # ransomware # it training

FIRST launches CORE Fund to boost global cyber response skills

Tue, 24th Jun 2025

Related stories

Fortinet finds Canadian OT cyber maturity rising, C-suite leads

Aryaka wins global SASE award & G2 leader for customer focus

Huntress & Microsoft partner to boost business cybersecurity

Over half of global companies leave email systems exposed to phishing

Juniper named Leader in Gartner's Magic Quadrant for fifth year

 By Shannon Williams, Journalist

FIRST has launched the CORE Fund, a global initiative to strengthen cybersecurity incident response capabilities in under-resourced regions, with Fortinet as the founding partner.

The Forum of Incident Response and Security Teams (FIRST), an international non-profit organisation, has announced the formation of the CORE (Community, Operational capacity, Resilience, and Empowerment) initiative to expand the operational capacities of cybersecurity teams around the world. The programme is set to focus especially on regions that currently have limited resources to defend against growing cyber threats such as ransomware.

Programme objectives

FIRST CORE is designed as a strategic programme to enhance incident response capabilities by leveraging guidance and experience from the global incident response community. Recent efforts have begun in Africa and the Caribbean, and there are plans to expand activities into the Asia-Pacific and Latin America regions.

The initiative includes several targeted measures such as the development of updated incident response training content, subsidising local training costs for partners from lower-income

IT Brief Canada

Dedicated to IT decision-makers at enterprise, corporate, and government organisations throughout Canada. These are...

8

Domain
Authority [?]

Provided by
MOZ

494

Unique
Visits [?]

Provided by
SimilarWeb

June 24, 2025

🌐 ONLINE

FIRST launches CORE Fund to boost global cyber response skills

itbrief.ca/story/first-launches-core-fund-to...

Estimated Views

341 [✓]

Calculated based on
audience size and social
engagement

IT Brief Canada - Technology news for CIOs & IT decision-makers

ITBrief
CANADA


TechDay

Guides

artificial intelligence # digital transformation # disaster recovery # hybrid & remote work # internet of things

Search

... 🔍



firewalls # ransomware # it training

FIRST launches CORE Fund to boost global cyber response skills

Tue, 24th Jun 2025


Related stories

Zyxel advances Secure by Design for global SMB networking security

Red Hat unveils no-cost Linux platform for business developers

Organisations urged to boost data resilience as AI adoption rises

Fortinet finds Canadian OT cyber maturity rising, C-suite leads



By Shannon Williams, Journalist

FIRST has launched the CORE Fund, a global initiative to strengthen cybersecurity incident response capabilities in under-resourced regions, with Fortinet as the founding partner.

The Forum of Incident Response and Security Teams (FIRST), an international non-profit organisation, has announced the formation of the CORE (Community, Operational capacity, Resilience, and Empowerment) initiative to expand the operational capacities of cybersecurity teams around the world. The programme is set to focus especially on regions that currently have limited resources to defend against growing cyber threats such as ransomware.

Programme objectives

SecurityBrief Canada

SecurityBrief Canada is focused on cybersecurity and cyberattack news. Its readers include business and enterprise...

8

Domain
Authority [?]

Provided by
MOZ

337

Unique
Visits [?]

Provided by
SimilarWeb

June 24, 2025

🌐 ONLINE

FIRST launches CORE Fund to boost global cyber response skills

securitybrief.ca/story/first-launches-core-f...

Estimated Views

266 [✓]

Calculated based on
audience size and social
engagement

SecurityBrief Canada - Technology news for CISOs & cybersecurity decision-makers

SecurityBrief
CANADA


TechDay

Guides

cloud security # cybersecurity # endpoint protection # firewalls # ransomware

Search

... 🔍



firewalls # ransomware # it training

FIRST launches CORE Fund to boost global cyber response skills

Tue, 24th Jun 2025

Related stories

- Huntress & Microsoft partner to boost business cybersecurity
- Over half of global companies leave email systems exposed to phishing
- Keymou+ blurs hacktivism & commerce amid 700 DDoS attacks
- July Patch Tuesday reveals 137 vulnerabilities
- Bugcrowd names Umesh Shankar to board, bolstering AI security

By Shannon Williams, Journalist

FIRST has launched the CORE Fund, a global initiative to strengthen cybersecurity incident response capabilities in under-resourced regions, with Fortinet as the founding partner.

The Forum of Incident Response and Security Teams (FIRST), an international non-profit organisation, has announced the formation of the CORE (Community, Operational capacity, Resilience, and Empowerment) initiative to expand the operational capacities of cybersecurity teams around the world. The programme is set to focus especially on regions that currently have limited resources to defend against growing cyber threats such as ransomware.

Programme objectives

FIRST CORE is designed as a strategic programme to enhance incident response capabilities by leveraging guidance and experience from the global incident response community. Recent efforts have begun in Africa and the Caribbean, and there are plans to expand activities into the Asia-Pacific and Latin America regions.

The initiative includes several targeted measures such as the development of updated incident response training content, subsidising local training costs for partners from lower-income



Infosecurity Magazine

The award winning online magazine dedicated to the strategy, insight and technology of information...

74

Domain Authority [?]

Provided by
MOZ

131K

Unique Visits [?]

Provided by
SimilarWeb

June 24, 2025

🌐 ONLINE

Lessons from Helsinki: NCSC-FI's Role in Mitigating a...

infosecurity-magazine.com/news/helsinki-...

Estimated Views

933 [✓]

Calculated based on audience size and social engagement

Engagements

27 [✓]


Total number of social engagements

Infösecurity Magazine

Log InSign Up


NewsTopicsFeaturesWebinarsWhite PapersPodcastsEventsDirectory🔍

Infosecurity Magazine Home » News » Lessons from Helsinki: NCSC-FI's Role in Mitigating a Major Data Breach



NEWS24 JUN 2025

Lessons from Helsinki: NCSC-FI's Role in Mitigating a Major Data Breach

**Kevin Poireault**
Reporter, Infosecurity Magazine
Follow @KpoireaultConnect on LinkedIn

A 2024 data breach affecting the City of Helsinki, Finland's capital and largest employer, which exposed sensitive personal data of over 300,000 people, offers valuable lessons for cybersecurity professionals.

The incident was the subject of a year-long investigation by the Safety Investigation Authority of Finland (SIAF/OTKES), which published [its technical report](#) on June 17, 2025.

Matias Mesia, a senior specialist at Finland's National Cyber Security Centre (NCSC-FI), led the agency's task force that helped Helsinki recover from the breach.

During FIRSTCON in Copenhagen on June 23, he shared insights into the incident and the strategies employed to contain and

You may also like

MAGAZINE FEATURE4 JUL 2016

Retail Security - Lessons Learned Two Years On

INTERVIEW6 OCT 2020

Interview: Jason Nurse, University of Kent

NEWS17 AUG 2020

Reported Data Breaches Down by 52% in 2020

MAGAZINE FEATURE26 DEC 2018

Cool Heads and Clear Minds: Getting Your Incident Response Plan Together

NEWS23 MAY 2018

Security Shifts Focus From Defense to



Home - SDxCentral

76

Domain
Authority [?]

Provided by
MOZ

45.2K

Unique
Visits [?]

Provided by
SimilarWeb

June 24, 2025

🌐 ONLINE

Fortinet partners with FIRST to enhance global cybersecurity...

sdxcentral.com/news/fortinet-partners-wit...

sdxcentral

Channels Media Live Events [Login / Create Account](#) 🔍

[HOME](#) > [NEWS](#) > [SECURITY](#)

Fortinet partners with FIRST to enhance global cybersecurity skills

Plans are underway to develop training tools and provide fellowship support

June 24, 2025 By: Ben Wodecki [Comment](#)



Nonprofit cybersecurity group The Forum of Incident Response and Security Teams (FIRST) has teamed up with Fortinet on an initiative aimed at enhancing incident response capabilities.

The FIRST CORE program will facilitate the sharing of expertise and insights from across the global incident response community to develop response capabilities for cybersecurity teams.

Fortinet will fund FIRST CORE program efforts, including plans to develop incident response training content and subsidize local training costs for lower-income partners.

The cybersecurity firm will also help establish a network of regional liaisons and mentors to support incident response teams and support the [Suguru Yamaguchi Fellowship Program](#) to provide opportunities for the next generation of cybersecurity talent from underrepresented regions.

"Fortinet's leadership as our founding partner demonstrates their commitment to strengthening cybersecurity knowledge across industries and borders," FIRST CEO Chris Gibson noted in a statement.

The FIRST CORE program ultimately builds on FIRST's nearly three decades of education, training, and knowledge sharing within the international security community.

"FIRST CORE represents a unique opportunity to provide boots-on-the-ground support to security teams around the world, particularly in under-resourced regions, and we're proud to be the founding partner of this important initiative," Derek Manky, chief security strategist and global VP of threat intelligence at Fortinet, said. "Creating new avenues for defenders everywhere to share knowledge and best practices ultimately give[s] us more opportunities to collectively disrupt global cybercrime."

Resources

[More](#)



5 reasons to transform your web and network security
10 Jul 2025

Successfully moving enterprise GenAI from proof of concept to production
02 Jul 2025

Data center networks for the AI era
27 Jun 2025

Networking for AI workloads
24 Jun 2025



Episode Software and hardware co-design: Optimizing next-gen compute

Estimated Views

273 [✓]

Calculated based on audience size and social engagement

Links

2 [✓]

2 links to first.org



CISO2CISO.COM & CYBER SECURITY GROUP

LATEST NEWS 05 / 20 : 1:01 pm : What American Enterprises Can Learn From Europe's GDPR Mistake

15

Domain Authority

Provided by
MOZ

977

Unique Visits

Provided by
SimilarWeb

June 24, 2025

ONLINE

Cyber Intel Pros and Hobbyists Can Now Report Threats...

ciso2ciso.com/cyber-intel-pros-and-hobb...

Estimated Views

588

Calculated based on audience size and social engagement

Home

About Us

Contact Us

Register to apply for a free CISO2CISO Membership

CISO2CISO Network

CISO2CISO Services

Sitemap

Submit News

CISO2CISO.COM

THE MOST COMPLETE REFERENCE SITE IN CYBER

CISO2CISO Notepad Series

CISO Strategies

Incidents & Attacks Notepad

Cybersecurity Latest News

User Private Area

Search Site...

Cyber Intel Pros and Hobbyists Can Now Report Threats Anonymously – Source: www.infosecurity-magazine.com

JUNE 24, 2025 POST AUTHOR / PUBLISHER: [INFOSECURITY MAGAZINE](https://www.infosecurity-magazine.com)

CISO2CISO post categories: [cyber](#), [Cyber Security News](#), [Info Security Magazine](#), [rss-feed-post-generator-echo](#)



INFOSECURITY MAGAZINE

☆☆☆☆☆ Rate this post

Source: www.infosecurity-magazine.com – Author:

Imagine a world in which any cybersecurity professional, or even a cyber hobbyist or whistleblower, could report a new cluster of malicious cyber activity anonymously, without having to go through lengthy and formal cyber reporting disclosure processes.

This is the mission that a group of European-based cybersecurity practitioners is trying to achieve with Draugnet, a new anonymous threat reporting platform built on Malware Information Sharing Platform (MISP), an open-source cyber threat intelligence (CTI) sharing platform.

Trey Darley, a security researcher based in Belgium, and Alexandre Dulaunoy, the head of the Computer Incident Response Center Luxembourg (CIRCL), will launch and demonstrate Draugnet during FIRSTCON in Copenhagen on June 24.

Initially called 'Abracadabra,' to convey how simple it is to use, Draugnet allows anyone to report a piece of threat

ADVISOR PICK'S POST

LASTEST PUBLISHED POSTS

CISO2CISO NOTEPAD SERIES

Agile Security

WEBSITE CISO2CISO

How Can We Structure Cybersecurity...

OCCUPYTHEM

LINUX BASICS FOR HACKERS

Linux Basics For Hackers By...

NSA

Digital Forensics and Incident Response (DFIR) Framework for Operational Technology (OT)

Digital Forensics And Incident Response...

THINK BIG BLOG

Top 10 TED Talks To Learn about Cybersecurity

Top 10 TED Talks To...

Cyber Security Small Business Guide

NCSC Cyber Security For Small...

PRACTICAL DEVOPS

API Security Fundamentals

API Security

MARCO JAVIER

NEW FIREWALL PARA IA

THE 2024 CISO BURNOUT REPORT

THE 2024 CISO BURNOUT REPORT...

MOHAMMAD ALKHODADI

CYBERSECURITY STRONG STRATEGY

CYBERINT

Retail Threat Landscape Report Q1-Q3...

PROTECTING CRITICAL SUPPLY CHAINS

Protecting Critical Supply Chains...

CULTURE AI

Time To Adapt - The State of Human Risk Management in 2024

NATIONAL CYBER SECURITY CENTRE

Engaging With AI: America's Role in Improving the Management of Cybersecurity Risk

Engaging With Boards To Improve...

2024 State of Multicloud Security Report

2024 State of Multicloud Security...

INSIDE THE MIND OF A CISO 2024

CYBERSECURITY STRONG STRATEGY

Cybersecurity Strong Strategy Step By...

CISO's Playbook to Cloud Security

CISO's Playbook to Cloud Security By...

ENTREPRENEUR

Cybersecurity Operational Center



SC Media

The essential resource for cybersecurity professionals, delivering in-depth, unbiased news,...

73

Domain Authority

Provided by
MOZ

99K

Unique Visits

Provided by
SimilarWeb

June 25, 2025

ONLINE

Draugnet launches for anonymous cyber threat tharing

scworld.com/brief/draugnet-launches-for-...

Estimated Views

681

Calculated based on audience size and social engagement

Media
A Click & Reserve

CyberRisk
ALLIANCE

LOG IN REGISTER

Threat Intelligence

Draugnet launches for anonymous cyber threat tharing

June 25, 2025

Share

By SC Staff

Aiming to simplify and democratize the way cyber threats are reported, European cybersecurity professionals are launching Draugnet, an anonymous reporting platform built on the open-source MISP framework, according to [Infosecurity Magazine](#).

Set to debut at FIRSTCON in Copenhagen on June 24, Draugnet enables users, including professionals, hobbyists, and whistleblowers, to submit [threat intelligence](#) without creating accounts or undergoing formal disclosure processes. Its for quiet defenders and anyone caught between responsible stewardship and unmanageable risk, said co-creator Trey Darley. Users receive a browser-stored follow-up token to continue or update submissions. While the platform emphasizes anonymity, Darley concedes that total online anonymity is impossible and acknowledges the risk of false submissions. Nonetheless, Draugnet is designed as a modular tool that organizations can adopt in controlled environments, such as ISACs or national agencies, possibly using confidential computing methods like Intel SGX. The initiative reflects growing frustration with bureaucratic barriers to sharing cyber intelligence and seeks to foster broader, lightweight collaboration.

SC Staff

Related

THREAT INTELLIGENCE
Toll of GMX crypto heist exceeds \$40M
SC Staff July 10, 2025

Related Events

CYBERCAST
Bridging the Gap: Turning Threat Intelligence into Operational Security Outcomes
On-Demand Event

CYBERCAST
Threat Intelligence Unleashed: Staying Ahead of Evolving Cyber Threats
On-Demand Event

VIRTUAL CONFERENCE
Nationwide Cybersecurity Summit 2025: Safeguarding America's Digital Future
WED NOV 19

GET DAILY EMAIL UPDATES

SC Media's daily must-read of the most current and pressing daily news

Business Email*

By clicking the Subscribe button below, you agree to SC Media [Terms of Use](#) and [Privacy Policy](#).

SUBSCRIBE



Metacuriosity

One-stop destination to end infosec news overload, scanned from thousands of sources

17

Domain Authority

Provided by
MOZ

338

Unique Visits

Provided by
SimilarWeb

[Home](#) [About](#) [RSS](#)

<Meta>curity®



[Sign in](#)

[Subscribe](#)

CYBERSECURITY

French cops busted BreachForum, IntelBroker operators

Qilin gang ransomware attack killed an NHS patient, Glasgow City Council hit by ransomware attack, Western Sydney University student arrested for school database hacking, Liberal Party hacked after pro-women messaging, Columbia University probes security incident, much more



Cynthia B Brumfield
26 Jun 2025 — 18 min read

This post is for paying subscribers only

[Subscribe now](#)

Already have an account? [Sign in](#)

READ MORE



UK's NCA arrested four people for M&S, Co-Op cyberattacks

Russian hoops player Kasatkin busted in France in connection...

By Cynthia B Brumfield — 10 Jul



M&S and Qantas leaders remain mum on ransomware payments

M&S chairman says two other British companies' ransomwar...

By Cynthia B Brumfield — 09 Jul



Italian cops arrest FBI-wanted Chinese hacker who tried to steal the COVID-19 vaccine

Brazilian cops bust IT worker connected to \$100m banking...



IT giant Ingram Micro's systems shut down after SafePay ransomware attack

Qantas is talking with threat actor after attack, Android...

June 26, 2025

ONLINE

French cops busted BreachForum, IntelBroker operators

[metacuriosity.com/french-cops-busted-breach...](https://metacuriosity.com/french-cops-busted-breachforum-intelbroker-operators)

Estimated Views

185

Calculated based on audience size and social engagement



Infosecurity Magazine

The award winning online magazine dedicated to the strategy, insight and technology of information...

74

Domain Authority [?]

Provided by
MOZ

131K


Unique Visits [?]

Provided by
SimilarWeb

Inf0security Magazine [Log In](#) [Sign Up](#)


[News](#) [Topics](#) [Features](#) [Webinars](#) [White Papers](#) [Podcasts](#) [Events](#) [Directory](#) [Q](#)


Infosecurity Magazine Home » News » Common Good Cyber Fund Launched to Support Non-Profit Security Efforts



NEWS 25 JUN 2025

Common Good Cyber Fund Launched to Support Non-Profit Security Efforts

**James Coker**
Deputy Editor, Infosecurity Magazine
[Follow @ReporterCoker](#)

**Kevin Poirault**
Reporter, Infosecurity Magazine
[Follow @Kpoireault](#) [Connect on LinkedIn](#)

A Common Good Cyber Fund has been launched, designed to support the work of non-profits organizations that deliver core cybersecurity services for the wider public good.

The fund has been established by Common Good Cyber, a global initiative set up to implement models for sustaining groups, organizations and individuals involved in critical cybersecurity functions for the broader Internet community.

The governments of the UK and Canada have announced that they will both invest the joint Canada-UK Common Good Cyber Fund. Additionally, during the recent G7

You may also like

NEWS 17 JUN 2025

Microsoft Promises to Keep European Cloud Data in Europe

NEWS 26 MAR 2025

ENISA Probes Space Threat Landscape in New Report

NEWS 25 FEB 2025

61% of Hackers Use New Exploit Code Within 48 Hours of Attack

NEWS 13 FEB 2025

Russian Seashell Blizzard Enlists Specialist Initial Access Subgroup to Expand Ops

NEWS 3 FEB 2025

June 25, 2025

 ONLINE

Common Good Cyber Fund Launched to Support Non-Profit...

infosecurity-magazine.com/news/commo...

Estimated Views

1.14K [✓]

Calculated based on audience size and social engagement

Engagements

8 [✓]

Total number of social engagements



Call us Toll Free (USA): 1-833-844-9468 International: +1-603-280-4451 M-F 8am to 6pm EST

Cyber Defense Magazine Cyber Defense Awards Cyber Defense Webinars Cyber Defense Conferences Cyber Defense TV Cyber Defense Radio Subscribe



CYBERDEFENSE^{Wire}

Home

Press Releases

Contact



Submit a Press Release

FIRSTCON25 Delivers Global Collaboration and Groundbreaking Cybersecurity Initiatives

in

Annual conference unveils new funding initiatives, platforms and tools, leadership appointments, and expanded global capacity building programs

COPENHAGEN, DENMARK – June 27, 2025 – The **Forum of Incident Response and Security Teams (FIRST)** has successfully concluded **FIRSTCON25**, its 37th Annual Conference. The five-day event brought together more than 1,000 registered attendees from 100+ countries, establishing new benchmarks for international cooperation in cybersecurity and incident response.

"The record-breaking attendance and depth of collaboration at FIRSTCON25 demonstrates the critical importance of international partnership in addressing today's complex threat landscape," said **Chris Gibson**, CEO of FIRST. "The initiatives launched this week will have a lasting impact on global cybersecurity resilience, particularly for underrepresented regions where capacity building is most needed."

Major Initiatives Launched to Strengthen Global Cybersecurity

FIRSTCON25 witnessed the introduction of several new programs designed to strengthen cybersecurity capabilities worldwide:

FIRST CORE with Fortinet: FIRST announced its **CORE (Community, Operational capacity,**



Press Release by Forum of Incident Response and Security Teams (FIRST)

Media Contact

Summer Mitchell

summer@growthstackmedia.com

Download Cyber Defense Magazine July Edition for 2025

Download eMag

Published monthly by Cyber Defense Magazine, this resource shares a wealth of information to help you stay one step ahead of the next cyber threat.

June 30, 2025

ONLINE

FIRSTCON25 Delivers Global Collaboration and Groundbreakin...

cyberdefensewire.com/firstcon25-deliver...

Estimated Views

602 ✓

Calculated based on audience size and social engagement

Links

12 ✓

12 links to first.org



NewsBreak

NewsBreak is the best local source for news, videos, and information on weather, traffic, safety,...

78

Domain Authority

Provided by
MOZ

16.1M

Unique Visits

Provided by
SimilarWeb

ONLINE

FIRSTCON25 Delivers Global Collaboration and Groundbreakin...

newsbreak.com/news/4083990132582-fi...

Estimated Views

94K

Calculated based on audience size and social engagement

NEWSBREAK Sign in

FIRSTCON25 Delivers Global Collaboration and Groundbreaking Cybersecurity Initiatives

By Gary, 10 days ago

Annual conference unveils new funding initiatives, platforms and tools, leadership appointments, and expanded global...

[Read full article](#)

- Q Kate Ditches Royal Reunion Battle
- Q Pirates Release Pitching Talent
- Q Girl Discovers Parents' Death, Sister...
- Q Idaho Search Ends in Mistake
- Q Epstein's Secret Suicide Note Unveiled

[See all trends >](#)

COMMENTS

Be the first to comment here.

Post

[Community Policy](#)

YOU MAY ALSO LIKE

Jim DeLillo · Follow
user · 3.2K followers

Deadly Bacteria Found in 45,000 Pounds of Frozen Shrimp— Nationwide Recall Issued

AI was utilized for research, writing, citation management, and editing. Seafood lovers, beware: nearly 45,000 pounds...

21d

383 183 Share

Bucks County Beacon · Follow
user · 14.0K followers



Fortinet

Fortinet delivers cybersecurity everywhere you need it. We secure the entire digital attack surface...

83

Domain Authority

Provided by
MOZ

1.54M

Unique Visits

Provided by
SimilarWeb

June 30, 2025

ONLINE

Fortinet Collaborates with Global Governments to Drive...

fortinet.com/blog/industry-trends/fortinet-...

Estimated Views

10.1K

Calculated based on audience size and social engagement

The screenshot shows the Fortinet website header with the logo and a navigation menu. The main content area features a large title 'Fortinet Collaborates with Global Governments to Drive Cyber Resiliency Across Five Eyes and Beyond' with a red horizontal bar. Below the title are two buttons: 'FORTINET TRUST' and 'TRUSTED PARTNERS'. The article text begins with 'By Fortinet | June 30, 2025' and discusses the need for global cooperation against cybercrime. It mentions Fortinet's role as a founding member of the World Economic Forum's Centre for Cybersecurity (C4C), a regular contributor to the Partnership Against Cybercrime (PAC), and a founding member of the Cybercrime Atlas initiative. It also mentions Fortinet's role as a long-standing member of INTERPOL Gateway, a partner of NIST's National Cybersecurity Excellence Partnership (NCEP), an active collaborator with Forum of Incident Response and Security Teams (FIRST) and founding partner of its Community, Operational capacity, Resilience, and Empowerment (CORE) initiative, and a founding member of the Cyber Threat Alliance, among others. At the bottom, there is a dark blue banner with the text 'Fortinet: Trust Is Our Business' and a 'Learn More' button.

FORTINET Blog

Fortinet News & Updates FortiGuard Labs Threat Research Industry Trends & Insights Life at Fortinet Partners Customer Success Stories PSIRT Blogs CISO Collective Subscribe

INDUSTRY TRENDS & INSIGHTS

Fortinet Collaborates with Global Governments to Drive Cyber Resiliency Across Five Eyes and Beyond

FORTINET TRUST TRUSTED PARTNERS

By **Fortinet** | June 30, 2025

In today's connected and complex digital landscape, the fight against global cybercrime requires unprecedented cooperation across the public and private sectors. No user, organization, or government agency can meaningfully disrupt cybercrime alone. To accomplish this, it's crucial to collectively develop opportunities for sharing information and threat intelligence across industries and borders, breaking down barriers to strengthen every organization's defense capabilities.

Since Fortinet's inception nearly 25 years ago, the company has invested time and resources in **building trusted** public and private partnerships to fight global cybercrime. Fortinet is a **founding member of the World Economic Forum's Centre for Cybersecurity (C4C)**, a regular contributor to its Partnership Against Cybercrime (PAC), and a founding member of the **Cybercrime Atlas initiative**, an effort designed to create an action-oriented, global knowledge base on cybercrime to mitigate and disrupt cybercrime at scale. Fortinet is also a long-standing member of INTERPOL Gateway, a partner of NIST's **National Cybersecurity Excellence Partnership (NCEP)** program, an active collaborator with Forum of Incident Response and Security Teams (FIRST) and founding partner of its **Community, Operational capacity, Resilience, and Empowerment (CORE) initiative**, and a founding member of the **Cyber Threat Alliance**, among others.

Fortinet: Trust Is Our Business

Learn about Fortinet innovation, collaboration partners **Learn More**



TechTarget - Global Network of Information Technology Websites and Contributors

91
Domain
Authority [?]
Provided by
MOZ

2.04M
Unique
Visits [?]
Provided by
SimilarWeb

The screenshot shows the TechTarget website interface. At the top, there's a navigation bar with 'informa' and a dropdown menu. Below it, a search bar and navigation links for various IT topics are visible. The main content area features a featured article titled 'Enterprise cybersecurity: A strategic guide for CISOs' with a 'Download this guide' button. Below this, the article 'What is vulnerability management? Definition, process and strategy' is displayed. The article is authored by Alexander S. Gillis and Sean Michael Kerner, published on June 30, 2025. The article text defines vulnerability management as the process of identifying, assessing, remediating, and mitigating security vulnerabilities in software and computer systems. It also discusses a typical vulnerability management process involving scanning IT assets, evaluating risks, and addressing vulnerabilities in a prioritized order. The article concludes with a comparison of vulnerability management vs. patch management.

What is vulnerability management? Definition, process and strategy

By Alexander S. Gillis, Technical Writer and Editor | Sean Michael Kerner | Published: Jun 30, 2025

Vulnerability management is the process of identifying, assessing, remediating and mitigating security vulnerabilities in software and computer systems. It's a critical part of managing cybersecurity risk in IT environments, as vulnerabilities that are not found and fixed can expose an organization to damaging [cyberattacks](#) and data breaches.

A typical vulnerability management process involves continuously [scanning IT assets for vulnerabilities](#), evaluating the risks of those that are found, and addressing the vulnerabilities in a prioritized order based on risk severity. The goals of vulnerability management include reducing [attack surface](#), improving an organization's overall [security posture](#) management, meeting regulatory compliance requirements and minimizing business risks.

Vulnerability management vs. patch management

Patch management is a subset of systems management. It involves identifying, acquiring, testing and installing patches or code changes that are intended to fix bugs, close security holes or add features.

Vulnerability management is not the same as patch management. Although they overlap, there are [differences between the two processes](#). Vulnerability management takes a big picture view to identify vulnerabilities and then resolve them across IT systems. Patch

June 30, 2025

🌐 ONLINE

What is Vulnerability Management? Definition, Process...

techtarget.com/searchsecurity/definition/...

Estimated Views

3.83K [✓]

Calculated based on audience size and social engagement

Engagements

28 [✓]

Total number of social engagements