Collective Defense Intelligence

A Model for Empowering the Open Cybersecurity Ecosystem

Jason Keirstead
CTO & Distinguished Engineer, IBM Security
Co-Chair, Open Cybersecurity Alliance
Steering Committee, OCSF
Board Member, OASIS Open
Traditional cybersecurity is broken – 66% of security teams do NOT share their data, far worse for their analytics.

- 45% of security teams require security engineers to hand wire integrations.
- Still, 21% of security decision-makers cite understaffing as a top challenge.

Industry and technology cooperation is needed – 84% believe that a product’s integration capabilities are important – 83% believe future interoperability depends upon established standards – 77% want more support for open standards

Source: ESG Research Report, July 2022 “Technology Perspectives from Cybersecurity Professionals”
"Detection As Code" – What!?

- Do SOC Engineers have to write code now?
- What about intelligence?
- What about response plans?
- What about automations?

- **Test-Driven Detection Development (TDD)**

- **Composability & Reuse**

- **Version-controlled, automated deployment workflow**

John Lambert, "The githubification of infosec" - https://medium.com/@johnlatwc/the-githubification-of-infosec-afbdbfaad1d1
Florian Roth, "Creating leverage" - https://cyb3rops.medium.com/leverage-is-key-b2abd3c323e2
Anton Chuvakin, “Can we have ‘Detection as Code’" - https://medium.com/anton-on-security/can-we-have-detection-as-code-96f869cfdc79
Shifting Left and Right

- We need to encourage detections that are *less specific* and *more modular*, to be able to scale and support collaboration.
- The more specific a detection is, the less useful it is in practice and shorter its shelf-life.
- Environments have realistic upper-limit to detections that can be deployed, we can’t write atomic detections for everything.
From “Detection as Code” to “Collective Defense Intelligence”

- **Threat intelligence** is **evidence-based knowledge** (e.g., context, mechanisms, indicators, implications and action-oriented advice) about **existing or emerging** menaces or hazards to assets. – *Gartner*

- **Defense intelligence** is **curated tactical knowledge** (e.g. hunt scenarios, alerting rules, detection analytics, manual and automated remediations, and playbooks) that will detect, mitigate, or prevent **validated and quantified** menaces or hazards to assets. – *Me*

- **Collective Defense intelligence** is enabled via an open security ecosystem that aids collaborating together on common Defense intelligence.
How can we enable collective defense?

- There is a serious tradeoff between secrecy and action in intelligence and counterintelligence activities.
- For various reasons, in cybersecurity organizations we skew much too far into the secrecy side of this trade.
- A number of fallacies contribute to this issue – we need to fight these.

https://www.youtube.com/watch?v=a4CS2tCjAgk
Resolving Perceived Challenges

- Can’t be “jack of all trades, master of none”
- We want to collaborate, but don’t know how to do it
- We want to collaborate, but have no tools to enable it
- How can I trust someone else’s defense?
Resolving Perceived Challenges

You are not special. You are not a beautiful or unique snowflake.

You are the same decaying organic matter as everything else.
Open Security leads to Collective Defense

**Foundational Standards**
- Foundational security elements
- Encryption, identity, data interchange
- Enable development of secure applications and services

**Operational Standards and Compliance**
- Best practice consumption from regulators and industry bodies
- Continuous policy monitoring and enforcement
- Vulnerability normalization and prioritization

**Threat Intelligence Sharing**
- Commercial and OSINT feeds
- ISAC / ISAO sharing
- Intelligence operationalization
- Creation of organization-specific intelligence

**Collaborative Detection**
- Common frameworks to understand attackers
- Common data models to enable analytics
- Shared cross-platform detections

**Collective Defense**
- Shared cross-platform hunting
- Shared cross-platform response runbooks
- Linkage from intelligence to detection to response to policy enforcement
- End-to-end collaboration
Security Standards
Enabling Collective Defense Intelligence

Standards

DefenseOps

Collaboration in the open
Nonprofit Cyber is a coalition of implementation-focused cybersecurity nonprofits to collaborate, work together on projects, voluntarily align activities to minimize duplication and increase mutual support, and link the community to key stakeholders with a shared communication channel.
How To Help

Learn more about open security initiatives to understand how to aid collective defense

Become part of the security ecosystem that embraces open source and collective defense

Contribute to the open security community with code, tooling, detections

Contribute and collaborate on detections as well as response plans

Open Cybersecurity Alliance

opencybersecurityalliance.org

Open Cybersecurity Schema Framework

ocsf.io

“Cybersecurity Meets Privacy”
11-12 September 2023
Royal Holloway*, University of London
CFP Closes June 9!

https://borderlesscyber2023.oasis-open.org

* Royal Holloway is located 15 minutes from Heathrow Airport & 35 minutes from downtown London.
Ways to consider participating…

• Attend: Registration is open. Fee to attend is £120-180+, includes daily breakfast, lunch and day one dinner.

• Sponsor: A variety of options available. Packages include podium time, tabletop exhibits and more.

• Submit a Proposal: There's still time to submit a proposal. Submission details can be found on the conference website.

* Royal Holloway is located 15 minutes from Heathrow Airport & 35 minutes from downtown London.

• ** A limited amount of reasonability priced university accommodations are available. Reserve now.
Questions ???

Jason Keirstead
CTO & Distinguished Engineer, IBM Security
Co-Chair, Open Cybersecurity Alliance
Steering Committee, OCSF
Board Member, OASIS Open

jason AT Keirstead DOT org
https://twitter.com/BlueTeamJK/
https://www.linkedin.com/in/jasonkeirståed/