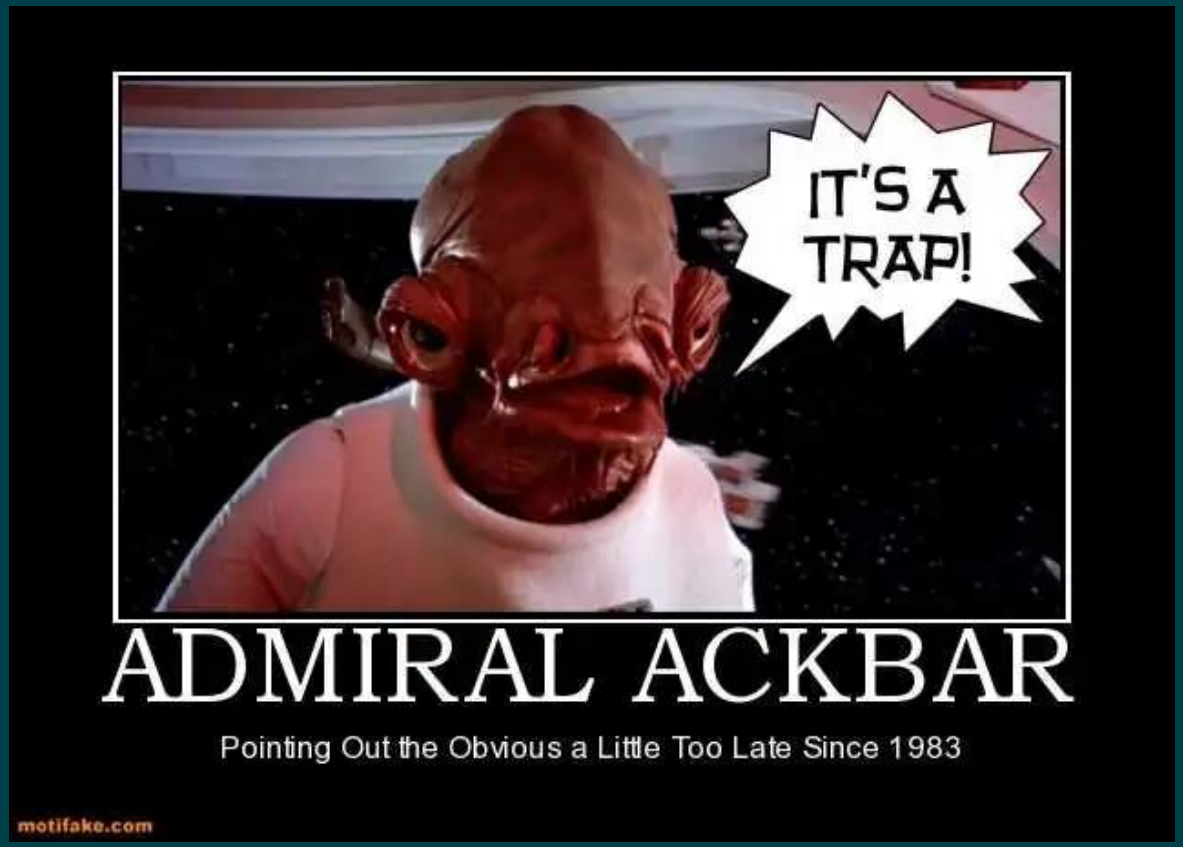
From your gut to a gold standard – Introducing the Admiralty System in CTI

Freddy Murstad, Senior Threat Intelligence Advisor, NFCERT

Nordic Financial CERT

Agenda

- About Me
- Problem with Existing CTI and OSINT
- Why we need the Admiralty Scale
- Introduction to the Admiralty System
- Case Study: Ticketmaster
- Conclusion
- QnA



- Senior Advisor Threat Intelligence @ NFCERT
- PhD Student @ NTNU

- Background
  - BA in Marketing
  - MA in Counter Terrorism
  - MA in Intelligence & Cyber
  - Intelligence in the Norwegian Army

FREDDY MURSTAD


It came to me in a dream
Trust me bro
CITING A SOURCE IN MY CTI REPORT
imgflip.com
JAKE-CLARK.TUMBLR

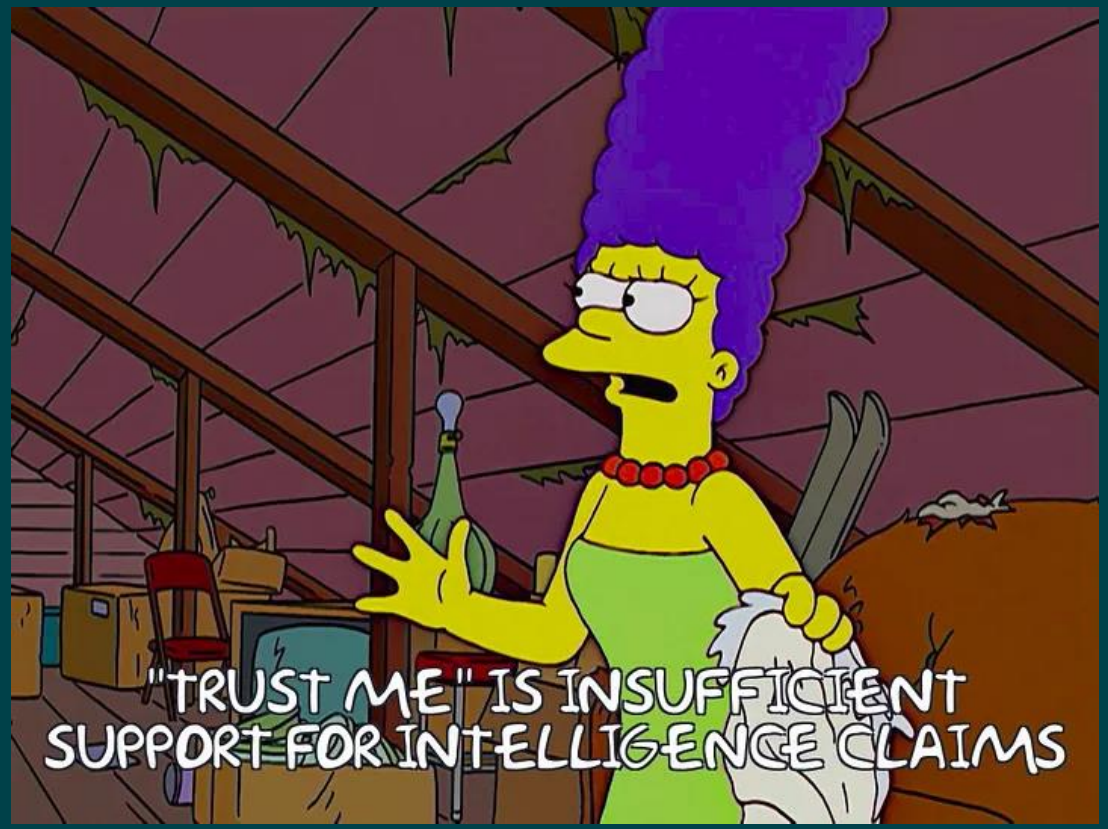
Problem with existing CTI and OSINT

- The bread and butter of CTI and OSINT Reporting
  - Blogs and Social Media posts
  - A ton of screenshots
  - Dissecting how a malware, dropper, or campaign worked
  - “Hey, look at all the cool things I can do. I am awesome, right?”

Problem with existing CTI and OSINT

- There's a huge lack of transparency, argumentation, and logic!
  - Just.... "Trust us!"

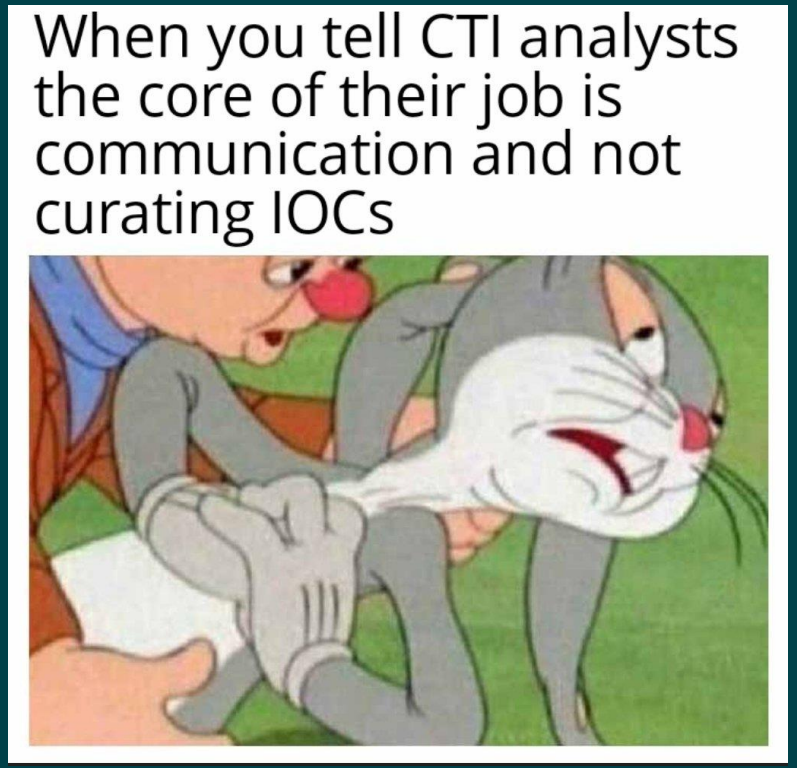
I need your source & information evaluation so I can assess whether to trust your reporting!



Source: Ramon Martinez, FOR578 Cybercrime student

Problem with existing CTI and OSINT

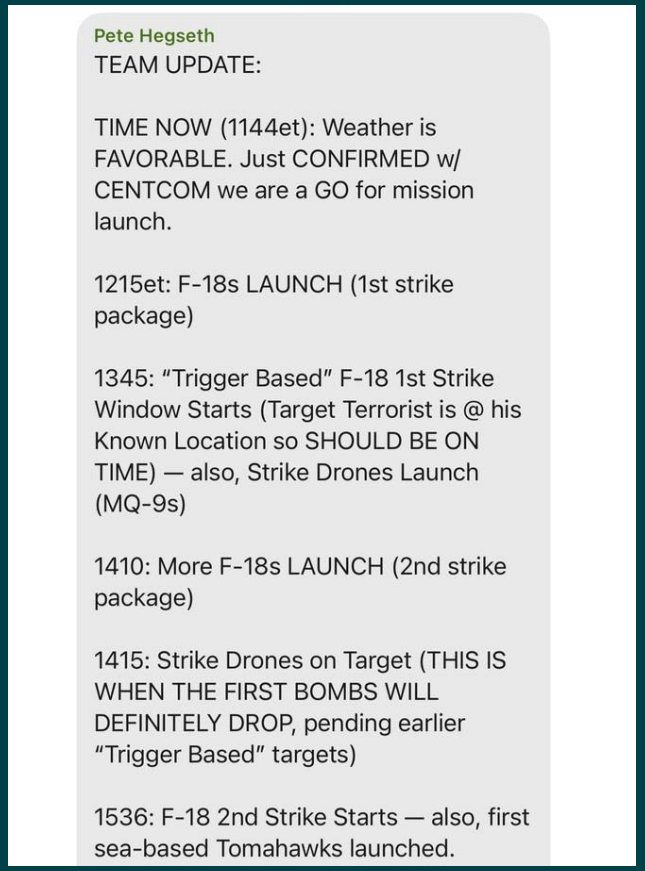
- Demonstrate to the reader WHAT you are basing your assessments on
- Assessments are built on data, information AND source & information evaluation
- Show us the trust you put in the sources you used and the data and information the sources provide
- More importantly, this is how we decide to trust your reporting, or not



Why we need the Admiralty System

Source: The Clarion Ledger, Cartoonist Marshall Ramsey

Why we need the Admiralty System



Pete Hegseth

TEAM UPDATE:

TIME NOW (1144et): Weather is FAVORABLE. Just CONFIRMED w/ CENTCOM we are a GO for mission launch.

1215et: F-18s LAUNCH (1st strike package)

1345: "Trigger Based" F-18 1st Strike Window Starts (Target Terrorist is @ his Known Location so SHOULD BE ON TIME) — also, Strike Drones Launch (MQ-9s)

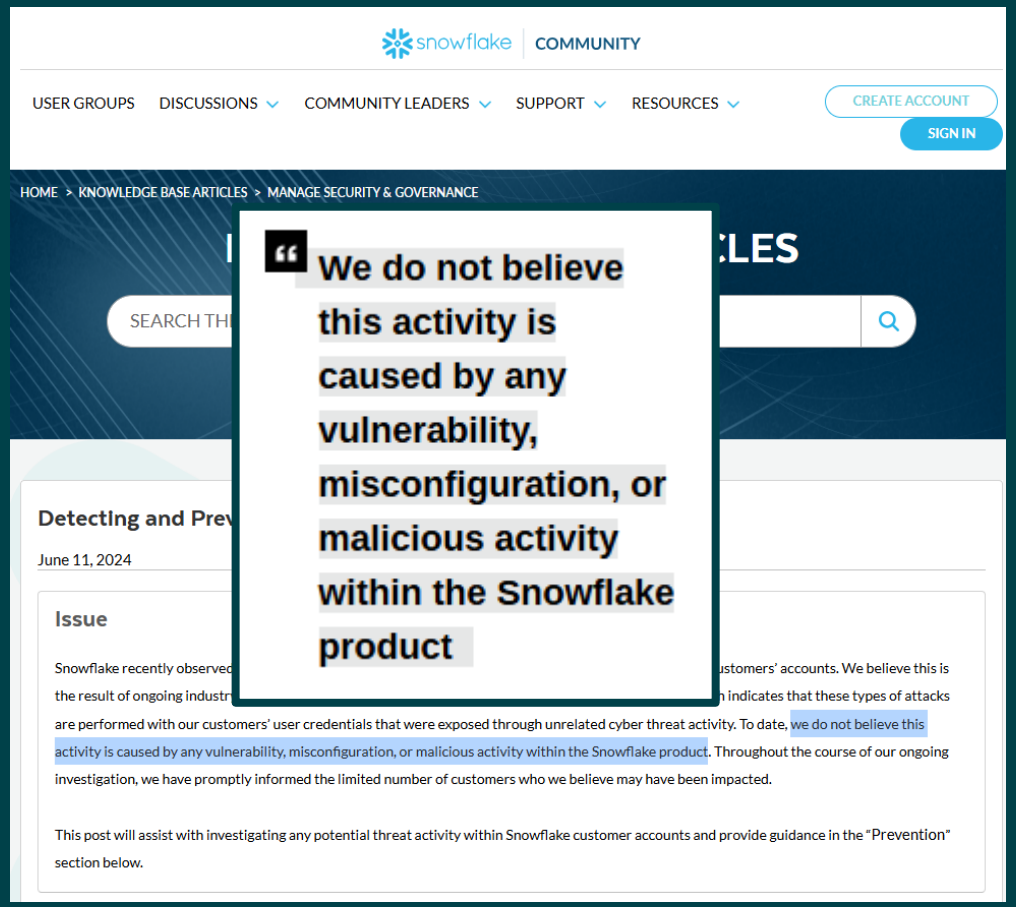
1410: More F-18s LAUNCH (2nd strike package)

1415: Strike Drones on Target (THIS IS WHEN THE FIRST BOMBS WILL DEFINITELY DROP, pending earlier "Trigger Based" targets)

1536: F-18 2nd Strike Starts — also, first sea-based Tomahawks launched.

Source: Screenshot, The Atlantic

Why we need the Admiralty System



Why we need the Admiralty System

Adversary Intelligence • 3 mins read

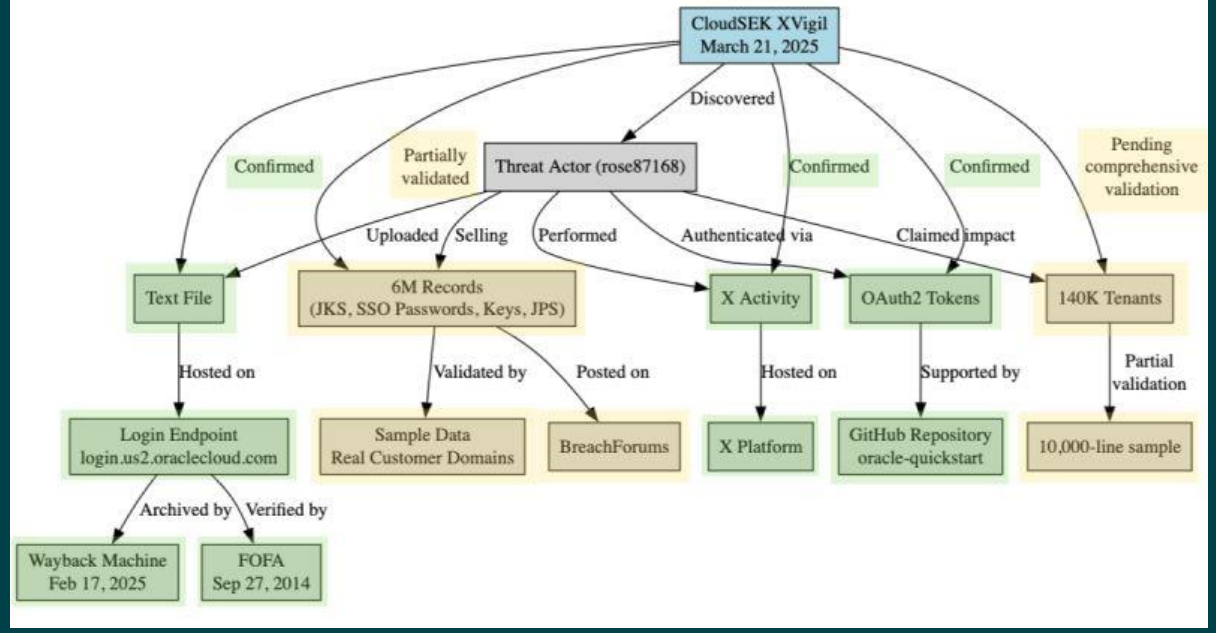
The Biggest Supply Chain Hack Of 2025: 6M Records Exfiltrated from Oracle Cloud affecting over 140k Tenants

CloudSEK uncovers a major breach targeting Oracle Cloud, with 6 million records exfiltrated via a suspected undisclosed vulnerability. Over 140,000 tenants are impacted, as the attacker demands ransom and markets sensitive data online. Learn the full scope, risks, and how to respond. Are you worried your organization might be affected? Check your exposure here - https://exposure.cloudsek.com/oracle

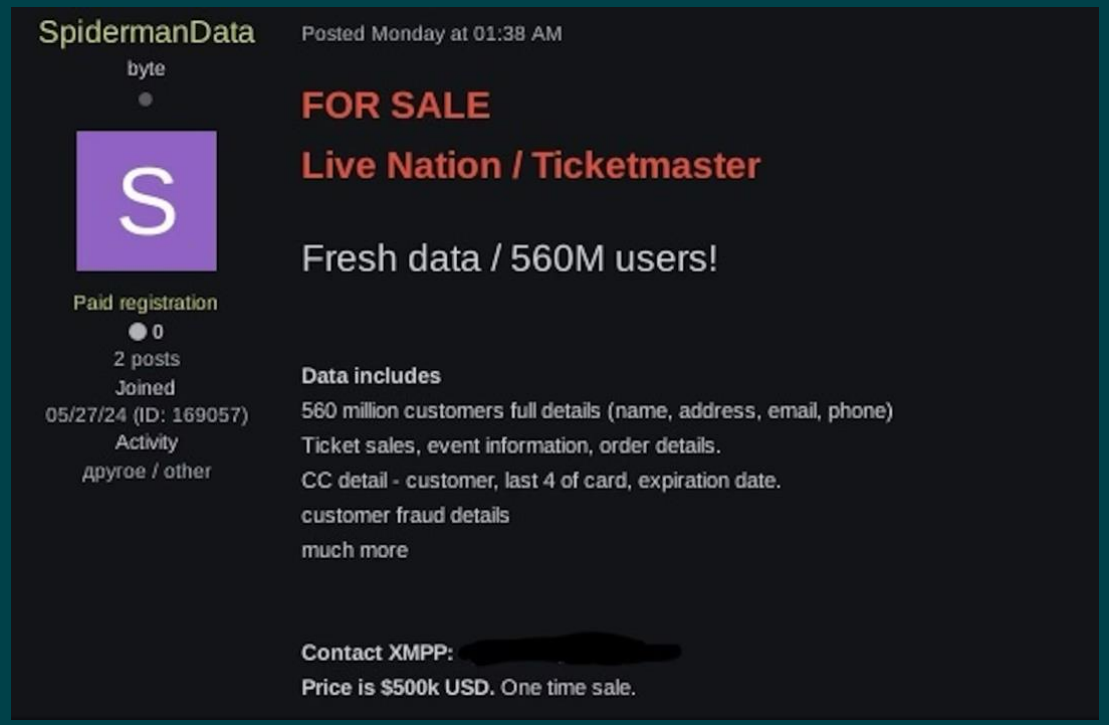
CloudSEK TRIAD
March 21, 2025

Link Analysis: Mapping the Alleged Oracle Cloud Breach

Link Analysis



Why we need the Admiralty System



- First to make a claim ➔dictates narrative
  - Regardless of truth
- Tactic to
  - Bolster their reputation
  - Gain credibility within underground communities
  - Simply drive attention to their services.

Why we need the Admiralty System

SpidermanData
byte

S

Paid registration
0
2 posts
Joined
05/27/24 (ID: 169057)
Activity
другое / other

Posted Monday at 01:38 AM

FOR SALE

Live Nation / Ticketmaster

Fresh data / 560M users!

Data includes
560 million customers full details (name, address, email, phone)
Ticket sales, event information, order details.
CC detail - customer, last 4 of card, expiration date.
customer fraud details
much more

Contact XMPP: [redacted]
Price is $500k USD. One time sale.

The Cyber Express
https://thecyberexpress.com › ... › Firewall Daily

Snowflake Breach Victims: 165 Organizations Identified So ...

May 28, 2024 — Some of the high-profile organizations hit in the attack have included **Ticketmaster**, Advance Auto Parts, Santander, and more. ... The Snowballing of the Snowflake ...

Hackread
https://hackread.com › Security

Hackers Claim Ticketmaster Breach: 560 Million Users' Info ...

May 28, 2024 — **ShinyHunters has claimed to have breached Ticketmaster**, stealing the data of 560m users. The 1.3 TB of stolen data also inlcudes payment details.
Missing: ~~Snowflake~~ | Show results with: Snowflake

ThreatDown by Malwarebytes
https://www.threatdown.com › blog › category › breac...

Breaches

Apr 11, 2024 — **Snowflake "breach" looks like 165 individual incidents**. After an investigation, Snowflake has concluded that recent data leaks were not caused by a ...

Concord USA
https://www.concordusa.com › blog › intruder-alert-ho...

Intruder Alert! How to Protect Yourself After the Recent ...

May 23, 2024 — It describes a **Snowflake** sales engineer's credentials being stolen, affecting over 150 customer environments such as **TicketMaster** and Santander bank.

Findings.co
https://findings.co › may-2024-data-breach-round-up

May 2024 Data Breach Round Up

May 19, 2024 — **Ticketmaster experienced a significant data breach**, confirmed by Live Nation, following the compromise of a third-party cloud database, likely Snowflake.

ClassAction.org
https://www.classaction.org › ticketmaster-may-2024

Ticketmaster Data Breach Lawsuit Investigation

May 20, 2024 — Were you affected by the **Ticketmaster** data **breach**? A class action could help you recover money for exposure of your info. Learn more.

bigt.net
http://bigt.net › Blog

Snowflake Data Breach: What Really Happened - Insights

Houlihan Lokey
https://www2.hl.com › pdf › cybersecurity-market... PDF

Cybersecurity Quarterly Update Q2 2024

May 19, 2024 — At least 165 customers were affected due to compromised credentials; customers affected include **Ticketmaster**, Santander Bank, and Pure. Storage. Outcome of ...

Fraud Intelligence
https://www.counter-fraud.com › skills-and-tools › info...

Information & Systems Security

May 15, 2024 — **Snowflake claims Santander and Ticketmaster breaches** not its fault. Data cloud platform Snowflake denies that vulnerabilities in its system allowed the ...

StrongDM
https://www.strongdm.com › what-is › behavior-based-a...

What is Behavior-Based Access Control (BBAC)?

Apr 8, 2024 — Behavior-Based Access Control (BBAC) is a security model that grants or denies access to resources based on the observed behavior of users or entities.

Nimbus Intelligence
https://nimbusintelligence.com › Blogposts

A Guide for obtaining the Snowflake Data Engineer ...

May 3, 2024 — Resources to pass the **Snowflake** Data Engineer Certification Exam: · Previous Post**Snowflake's** involvement in the **Ticketmaster** data **breach**. What happened and how ...

santander.com
https://www.santander.com › stories › statement

Statement - Banco Santander

May 14, 2024 — We recently became aware of an unauthorized access to a Santander database hosted by a third-party provider. We immediately implemented measures to contain ...
Missing: ~~Ticketmaster~~ ~~Snowflake~~

The Cyber Express
https://thecyberexpress.com › ... › Hacker Claims

Hacker Claims QuoteWizard Data Breach

May 28, 2024 — Dark web hacker, Sp1d3r, allegedly pilfered 2TB of data from QuoteWizard data breach, compromising 190M records.

Facebook · Cybersecurity

Findings.co
https://findings.co › may-2024-data-breach-round-up

May 2024 Data Breach Round Up

May 19, 2024 — **Ticketmaster experienced a significant data breach**, confirmed by Live Nation, following the compromise of a third-party cloud database, likely Snowflake.

ClassAction.org
https://www.classaction.org › ticketmaster-may-2024

Ticketmaster Data Breach Lawsuit Investigation

May 20, 2024 — Were you affected by the **Ticketmaster** data **breach**? A class action could help you recover money for exposure of your info. Learn more.

bigt.net
http://bigt.net › Blog

Snowflake Data Breach: What Really Happened - Insights

May 23, 2024 — Notably, companies like Santander and **Ticketmaster** were impacted, with sensitive customer and employee data being compromised. The ShinyHunters group ...

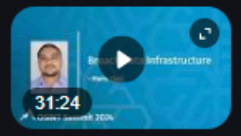
Reddit · r/pcloud
20+ comments

pCloud Data Breach?

Hello Everyone,. 4 days ago, I received a suspicious email claiming to be from pCloud about my account being accessed from an unknown location.

YouTube · SANS Cyber Defense
840+ views · 11 months ago

Breach Data Infrastructure



Snowflake Data Breach impacts Ticketmaster & Others, The Rise of ShinyHunters, Hugging Face Hack. The CyberHub Podcast•1K views · 21:43 · Go to channel ...

10 key moments in this video

Facebook
https://m.facebook.com › ... › Cybersecurity | Facebook

Another example of why having a robust, layered approach ...

News of the **Snowflake breach** potentially involving customer data from **Ticketmaster** and Santander Bank continues to evolve.

santander.com
https://www.santander.com › stories › statement

Statement - Banco Santander

May 14, 2024 — We recently became aware of an unauthorized access to a Santander database hosted by a third-party provider. We immediately implemented measures to contain ...
Missing: ~~Ticketmaster~~ ~~Snowflake~~

The Cyber Express
https://thecyberexpress.com › ... › Hacker Claims

Hacker Claims QuoteWizard Data Breach

May 28, 2024 — Dark web hacker, Sp1d3r, allegedly pilfered 2TB of data from QuoteWizard data breach, compromising 190M records.

Facebook · Cybersecurity
70+ followers

Cybersecurity

News of the **Snowflake breach** potentially involving customer data from **Ticketmaster** and Santander Bank continues to evolve. SOCRADAR.IO. Overview of the ...

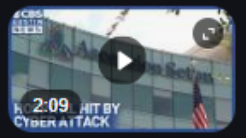
Wikipedia
https://en.wikipedia.org › wiki › Live_Nation_(events_...

Live Nation (events promoter)

May 15, 2024 — "**Ticketmaster** data **breach**? Hackers claim over 500 million users ... "**Ticketmaster breach** linked to growing **Snowflake** attack". Silicon Republic ...

YouTube · CBS Austin
2.3K+ views · 10 months ago

Patients sue Ascension over data breach from cyberattack



Patients sue Ascension over data breach from cyberattack ... **Snowflake Data Breach impacts Ticketmaster** & Others, The Rise of ShinyHunters, Hugging Face Hack.

MSN
http://www.msn.com › en-us › technology › cybersecurity

What Goes into an Effective Incident Response Plan ...

Apr 15, 2024 — In April 2024, a major data **breach** affected **Snowflake's** cloud platform due to insufficient security measures, including the absence of multifactor ...

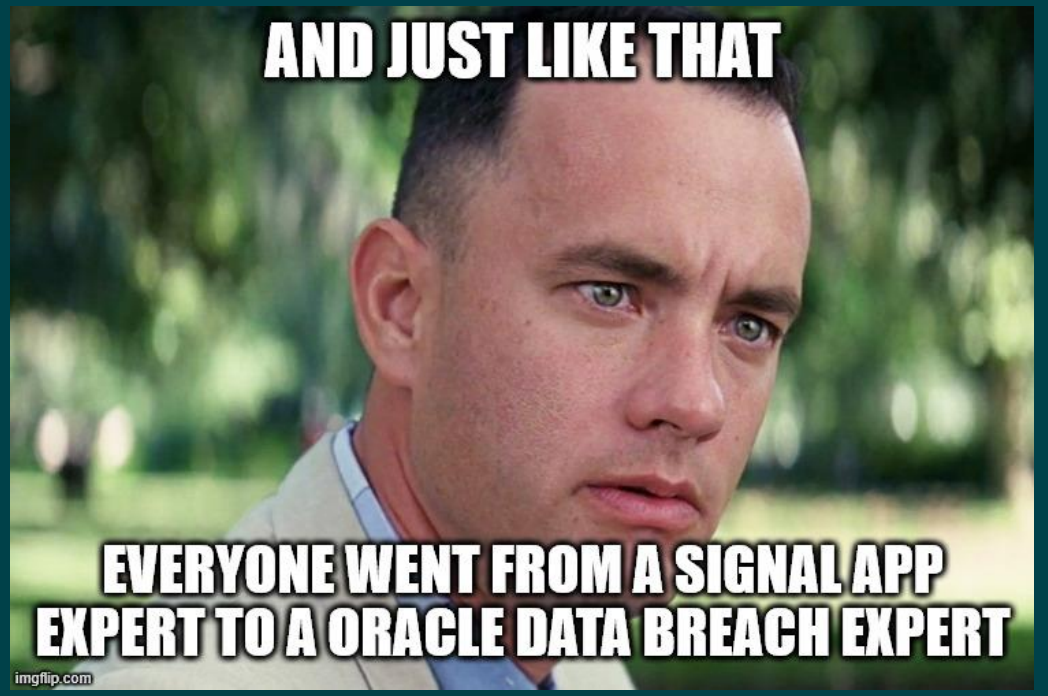
Why we need the Admiralty System

- Unverified claims spread rapidly
- Amplified by the media and security researchers
  - **Eager to break news** before conducting thorough verification
- Speculation turns into accepted facts
- Harder to separate legitimate intelligence from opportunistic noise
- One word: BIAS

Why we need the Admiralty System

Instead, intelligence teams should

- Emphasize critical thinking & structured analysis
- Applying rigor, SATs, and frameworks like the Admiralty System
  - Assess both the reliability of sources and the credibility of claims before making public assertions
- If urgency demands preliminary reporting, it should be accompanied by clear disclaimers:
  - "We assess this to be… based on available information, with the following limitations…"



Introducing the Admiralty System

- Admiralty in the British Royal Navy (hence the name ‘Admiralty System’)
- Naval intelligence in the early 20th century
- Information and intelligence received were uniform and standardized
- Compare the various pieces of information, often received weeks or months apart, about the same observation

Freddy Murstad

Enhance your Cyber Threat Intelligence with the Admiralty System

The Admiralty System, when adapted for cyber threat intelligence, offers a robust framework for enhancing the reliability of your intelligence.

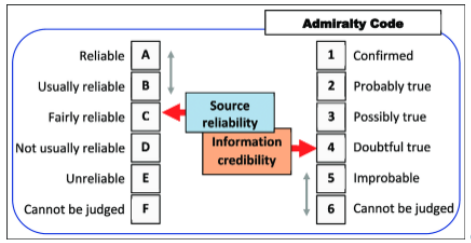
September 10, 2024

This three-part blog series is jointly authored by Sean O'Connor, co-author of *SANS FOR589: Cybercrime Intelligence*, and Freddy Murstad, PhD. candidate researching traditional intelligence methodology application into cyber threat intelligence (CTI). The blog series will highlight the benefit of using the Admiralty System when assessing cybercriminals and their claims of data breaches within cybercrime underground communities. In part 1, we will focus on the background and essential elements of the Admiralty System as well as highlighting some of the benefits and drawbacks of using the system. One of the focal points of FOR589 is learning to filter out the noise in the 'underground' and bring structure to an otherwise unstructured flow of data and sources. In part 2, we will evaluate cybercriminal sources and claims and discuss how to align them with this system.

Picture this: You're drowning in alerts, your open-source intelligence (OSINT) and threat intel feeds are going berserk, and your team is playing whack-a-mole with potential threats. You're constantly bombarded with information from countless sources—some reliable, others not so much. Sound familiar? Enter the Admiralty System - a robust framework that can revolutionize how we assess and utilize CTI. But what exactly is this system, and why should you consider implementing it in your CTI program? Let's dive in.

What the Heck is the Admiralty System Anyway?

The Admiralty System was originally designed for naval intelligence in the early 20th century and has since been adapted by intelligence agencies worldwide. The system was developed to ensure the information and intelligence received by the Admiralty in the British Royal Navy (hence the name 'Admiralty System') were uniform and standardized. This allowed them to compare the various pieces of information – often received weeks or months apart – about the same observation. (Yes, there was a time without the internet, gasp!) Playfully, we can call this system a sort of 'BS detector' for intelligence. Simply put, it's all about figuring out if your intel sources are credible and if the information the 'other side' is feeding you is genuine or just hot air and lies. Ludo Block provides additional insights into the Admiralty System via his blog, The Origin of Information Grading Systems.



Introducing the Admiralty System

- Adopted by intelligence communities worldwide
- Sort of ‘BS detector’ for intelligence
- Figuring out if your sources are credible and if the information is genuine, or just hot air and lies.

Freddy Murstad

Enhance your Cyber Threat Intelligence with the Admiralty System

The Admiralty System, when adapted for cyber threat intelligence, offers a robust framework for enhancing the reliability of your intelligence.

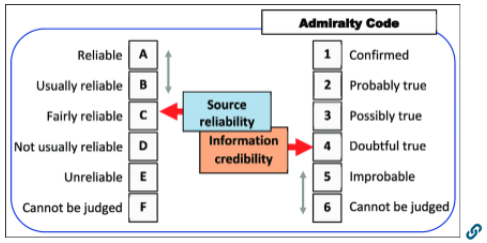
September 10, 2024

This three-part blog series is jointly authored by Sean O'Connor, co-author of *SANS FOR589: Cybercrime Intelligence*, and Freddy Murstad, PhD. candidate researching traditional intelligence methodology application into cyber threat intelligence (CTI). The blog series will highlight the benefit of using the Admiralty System when assessing cybercriminals and their claims of data breaches within cybercrime underground communities. In part 1, we will focus on the background and essential elements of the Admiralty System as well as highlighting some of the benefits and drawbacks of using the system. One of the focal points of FOR589 is learning to filter out the noise in the 'underground' and bring structure to an otherwise unstructured flow of data and sources. In part 2, we will evaluate cybercriminal sources and claims and discuss how to align them with this system.

Picture this: You're drowning in alerts, your open-source intelligence (OSINT) and threat intel feeds are going berserk, and your team is playing whack-a-mole with potential threats. You're constantly bombarded with information from countless sources—some reliable, others not so much. Sound familiar? Enter the Admiralty System - a robust framework that can revolutionize how we assess and utilize CTI. But what exactly is this system, and why should you consider implementing it in your CTI program? Let's dive in.

What the Heck is the Admiralty System Anyway?

The Admiralty System was originally designed for naval intelligence in the early 20th century and has since been adapted by intelligence agencies worldwide. The system was developed to ensure the information and intelligence received by the Admiralty in the British Royal Navy (hence the name 'Admiralty System') were uniform and standardized. This allowed them to compare the various pieces of information – often received weeks or months apart – about the same observation. (Yes, there was a time without the internet, gasp!) Playfully, we can call this system a sort of 'BS detector' for intelligence. Simply put, it's all about figuring out if your intel sources are credible and if the information the 'other side' is feeding you is genuine or just hot air and lies. Ludo Block provides additional insights into the Admiralty System via his blog, The Origin of Information Grading Systems.



The Admiralty System Rating Scale

- Assessing two distinct components
  - Source Reliability
  - Information Credibility
- Separated to ensure a clear and unbiased data assessment
- It uses alphanumeric codes to rate these two crucial aspects
- A1 -> F6

NATO Standard AJP-2.1

Source Reliability	Information Credibility
A Completely Reliable	1 Completely Credible & Confirmed
B Usually Reliable	2 Probably True
C Fairly Reliable	3 Possibly True
D Not Usually Reliable	4 Doubtful
E Unreliable	5 Improbable
F Reliability Cannot be Judged	6 Truth Cannot be Judged

The Admiralty System Rating Scale

Source Reliability

- Rated from
  - A (Completely reliable) to
  - F (Cannot be judged)
- Refers to the trustworthiness of the **origin** of the information
- Evaluating the source independently of the data itself, analysts can assess whether a particular piece of intelligence is likely to be accurate based on the source's history, skills, knowledge of the subject, how close they were to the incident, and many other attributes.

NATO Standard AJP-2.1

Source Reliability	Information Credibility
A Completely Reliable	1 Completely Credible & Confirmed
B Usually Reliable	2 Probably True
C Fairly Reliable	3 Possibly True
D Not Usually Reliable	4 Doubtful
E Unreliable	5 Improbable
F Reliability Cannot be Judged	6 Truth Cannot be Judged

The Admiralty System Rating Scale

Information Credibility

- Rated from 1 (Confirmed by other sources) to 6 (Truth cannot be judged)
- Refers to the trustworthiness of the **data and information** provided, regardless of the source
  - This is important!
- Considers whether the information makes sense, is consistent with other known facts, and has been corroborated by other independent sources.

NATO Standard AJP-2.1

Source Reliability	Information Credibility
A Completely Reliable	1 Completely Credible & Confirmed
B Usually Reliable	2 Probably True
C Fairly Reliable	3 Possibly True
D Not Usually Reliable	4 Doubtful
E Unreliable	5 Improbable
F Reliability Cannot be Judged	6 Truth Cannot be Judged

The Reliable Threat Report

You receive a report from a top-tier cybersecurity firm.

The source has consistently provided accurate and timely information in the past.

- How would you rate the source?

Source **Information**

Their report claims that a new zero-day vulnerability in widely used software is being actively exploited.

This claim is backed up by multiple independent and trusted sources.

- How would you rate the information?

Nordic Financial CERT

The Dubious Social Media Claim

You see an account on X claiming that a major financial institution has been hacked.

The account usually posts about topics proven to be untrue and has no previous track record of posting this kind of information.

- How would you rate the source?

No other credible sources have confirmed the claim

- How would you rate the information?

Source **Information**

Nordic Financial CERT

The New Kid on the Block

You come across a post on a Dark Web forum about a breach they allegedly have data from.

The source is not a known forum user, but the post is supported by an admin and another trusted user.

The users' identity and true motivations are unclear.

- How would you rate the source?

Source

Information on the breach is gaining traction by other researchers.

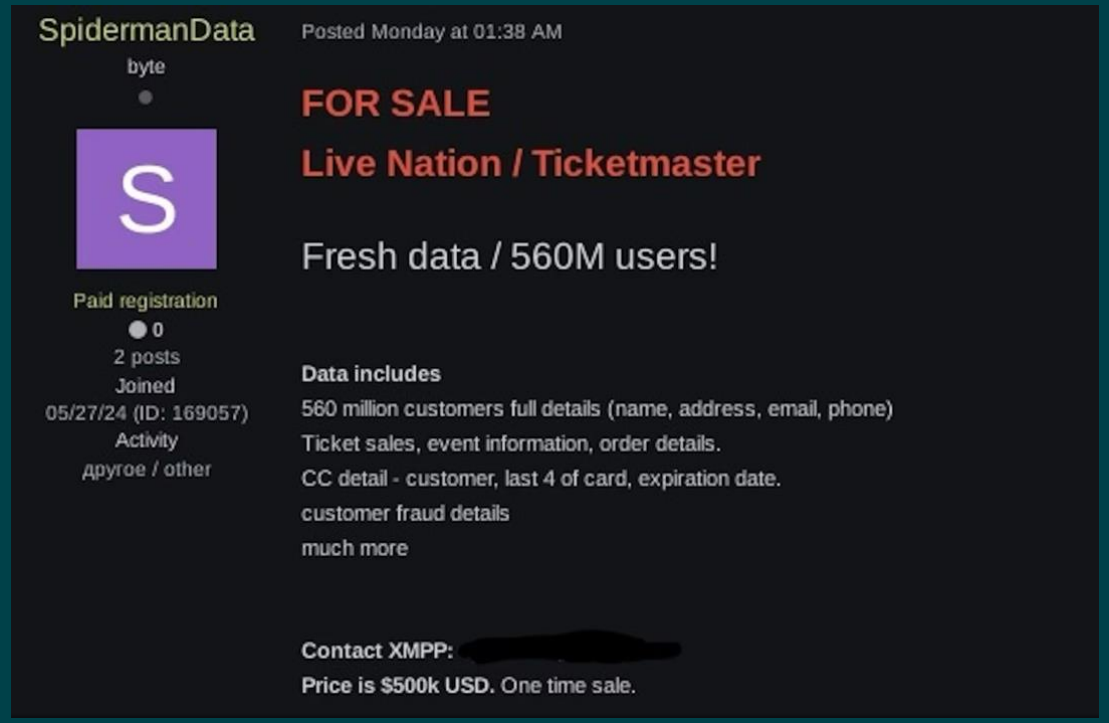
You are still trying to get independent verification or concrete evidence.

- How would you rate the information?

Information

Nordic Financial CERT

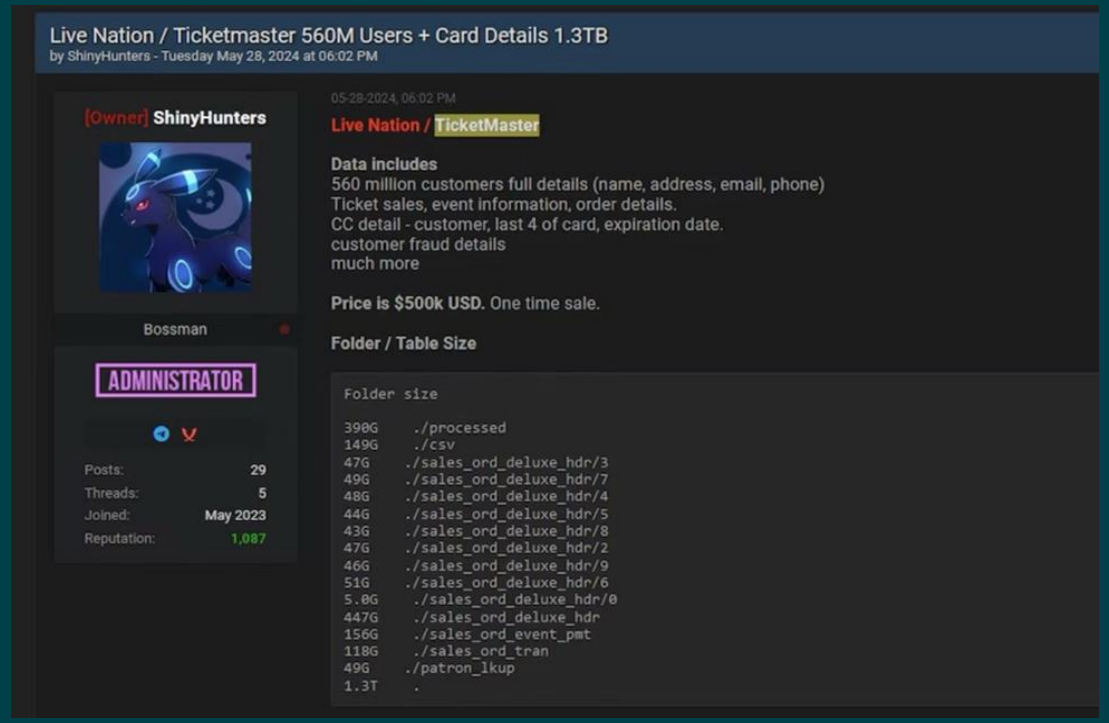
Case Study: The Ticketmaster and Snowflake breach



May 26, 2024, at 22:38 UTC: SpidermanData

"SpidermanData" offers data from Ticketmaster for $500,000

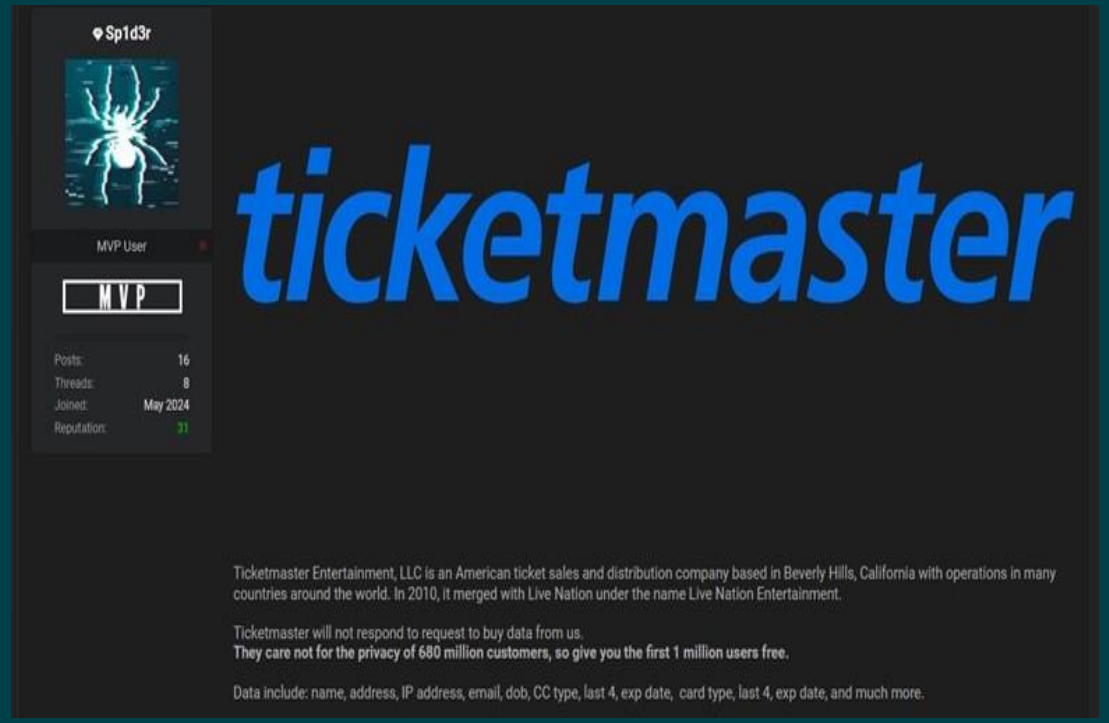
Case Name	Live Nation/Ticketmaster Breach
Forum Name	Exploit[.]in
Post Content	SpidermanData offers user data for $500,000 including names, addresses, emails, phone numbers, partial credit card details, and ticket order information.
Date of Post	May 26, 2024, 22:38 UTC
Author	SpidermanData
Communication Identifiers	Spiderman@xmpp[.]cn
Associated With	Likely linked to “ellyel8”
Forum Section	[Other] - everything else
Post Link	hxxps://forum[.]exploit[.]in/topic/242659
Author First Seen	May 26, 2024
Author Involved in Other Cases	No known cases at the time of the post
Author Forum Reputation	Low Reputation, Limited History
Author Observed in Other Forums	No known observations at time of original post
Source Reliability	**F** – Reliability cannot be judged
Information Credibility	**6** – Truth cannot be judged



May 28, 2024, at 14:41 UTC: ShinyHunters

“ShinyHunters” mirrors Ticketmaster breach post on BreachForums

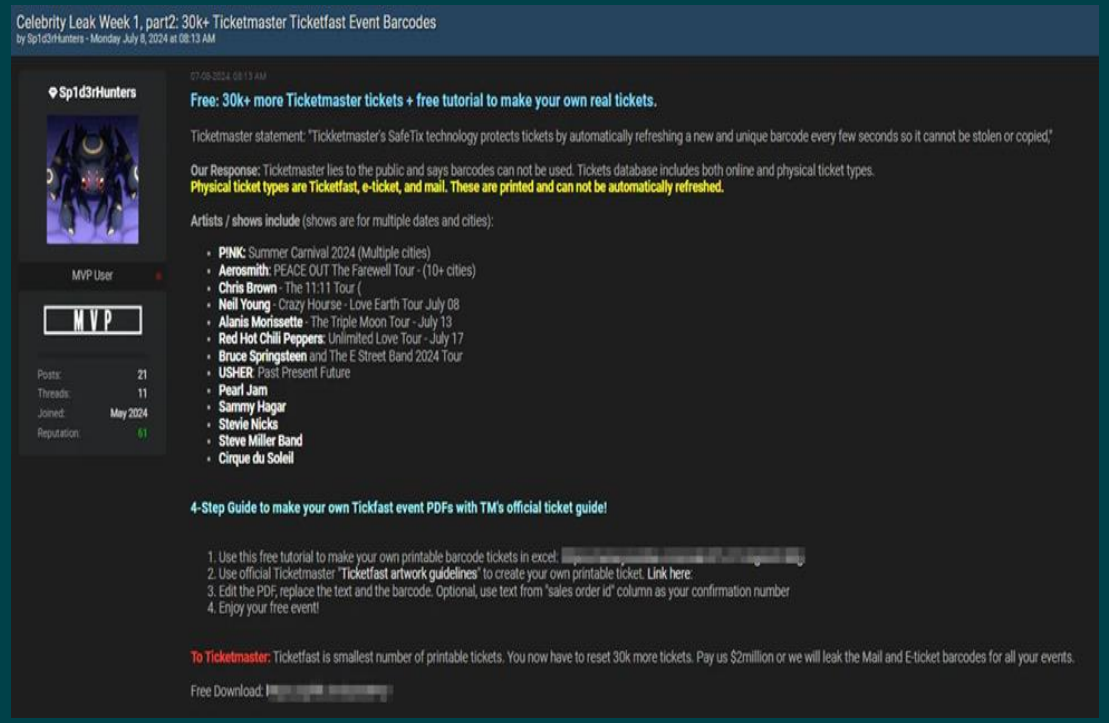
Case Name	Live Nation/Ticketmaster Breach
Forum Name	BreachForums
Post Content	ShinyHunters advertises Ticketmaster data for $500,000 including names, addresses, emails, phone numbers, event details, order information, and partial credit card details.
Date of Post	May 28, 2024, 14:41 UTC
Author	ShinyHunters
Communication Identifiers	Fs0c131y, whysodank, shinyhunters@xmpp[.]jp, shinyhunters@xmpp[.]cx, @sh_corp @Wearelegionnn, @shinycorp
Associated With	Breach Forums Administrator and possible connection to SpidermanData
Forum Section	Sellers Place
Post Link	hxxps://breachforums[.]st/Thread-SELLING-Live-Nation-Ticketmaster-560M-Users-Card-Details-1-3TB
Author First Seen	April, 18, 2020
Author Involved in Other Cases	Known involvement in multiple breaches, such as, Tokopedia, AT&T and Santander Bank
Author Forum Reputation	Administrator, High Reputation Score (1,087)
Author Observed in Other Forums	Active in multiple forums and marketplaces
Source Reliability	**B** – Usually Reliable
Information Credibility	**3** – Possibly True



June 20, 2024: Sp1d3r

Sp1d3r leaks data of 1 million Ticketmaster users for free

Case Name	Live Nation/Ticketmaster Breach
Forum Name	BreachForums
Post Content	Sp1d3r offers a free leak of 1 million Ticketmaster user records, including names, addresses, IP addresses, dates of birth, and partial credit card details. This sample is part of a larger dataset of 680 million users.
Date of Post	June 20, 2024
Author	Sp1d3r
Communication Identifiers	sp1d3r@nigg[.]ir
Associated With	Possible connection to SpidermanData and Shinyhunters
Forum Section	Databases
Post Link	hxxps://breachforums[.]st/Thread-TicketMaster-Live-Nation-1M-users-LEAK
Author First Seen	May 2024
Author Involved in Other Cases	QuoteWizard, Advance Auto Parts, Cylance, Truist, Santander Groupo Bank, LAUSD, Edgenuity and Jollibee
Author Forum Reputation	MVP Designated user, Reputation Score: 31
Author Observed in Other Forums	XSS (previously DamageLab)
Source Reliability	**C** – Fairly Reliable
Information Credibility	**3** – Possibly True



July 8, 2024: Sp1d3rHunters

Sp1d3rHunters leaks over 30,000 TicketMaster TicketFast barcodes

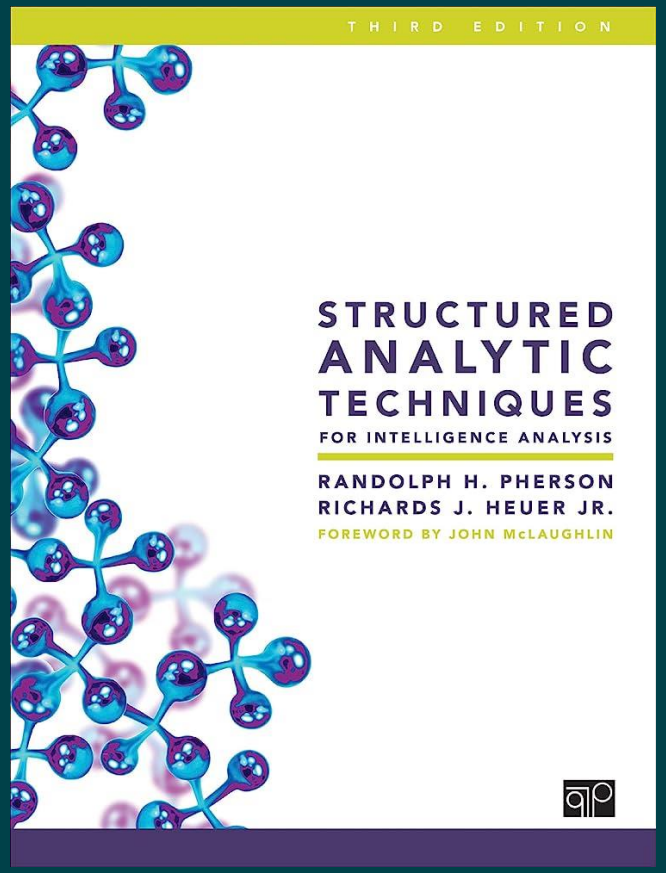
Case Name	Live Nation/Ticketmaster Breach
Forum Name	BreachForums
Post Content	Sp1d3rHunters leaked over 30,000 TicketMaster TicketFast barcodes, provided a guide for generating fraudulent tickets, and demanded a $2 million ransom to prevent further leaks.
Date of Post	July 8, 2024
Author	Sp1d3rHunters (aka Sp1d3r)
Communication Identifiers	sp1d3r@nigg[.]ir
Associated With	Sp1d3r, andSp1d3r, Sp1d3rHunters. Possible connection to ShinyHunters, and Spidermandata
Forum Section	Leaks Market
Post Link	hxxps://breachforums[.]st/Thread-REPOST-Celebrity-Leak-Week-1-170k-Taylor-Swift-Event-Barcodes-Ticketmaster
Author First Seen	May 2024
Author Involved in Other Cases	QuoteWizard, Advance Auto Parts, Cylance, Truist, Santander Groupo Bank, LAUSD, Edgenuity, Jollibee and Neiman Marcus
Author Forum Reputation	MVP Designation, Reputation Score: 61
Author Observed in Other Forums	XSS (previously DamageLab) as Sp1d3r
Source Reliability	**B** – Usually Reliable
Information Credibility	**2** – Probably True

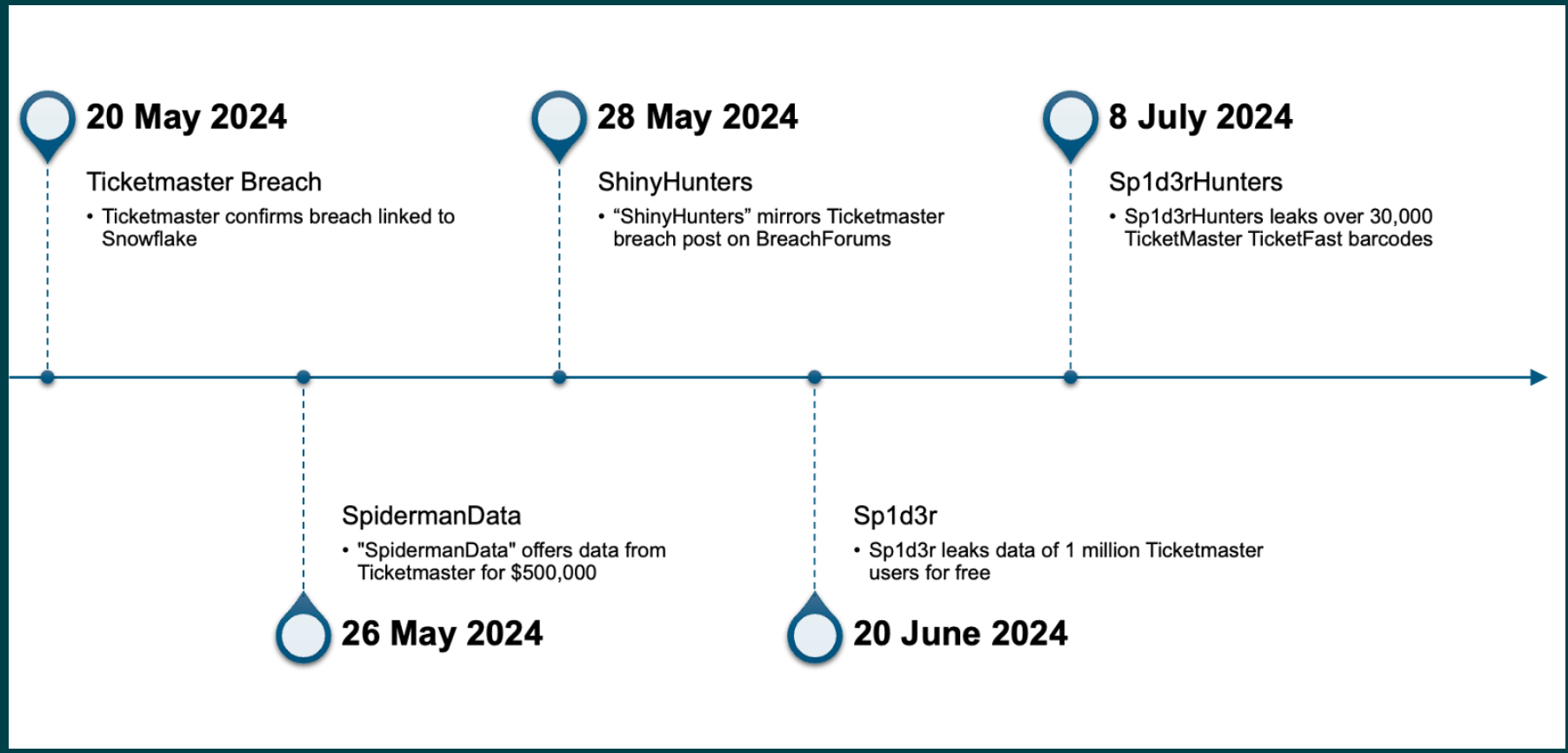
Structured Analytic Technique (SAT)

How do we determine the reliability and credibility of the claims made by various sources?

SAT: Timeline

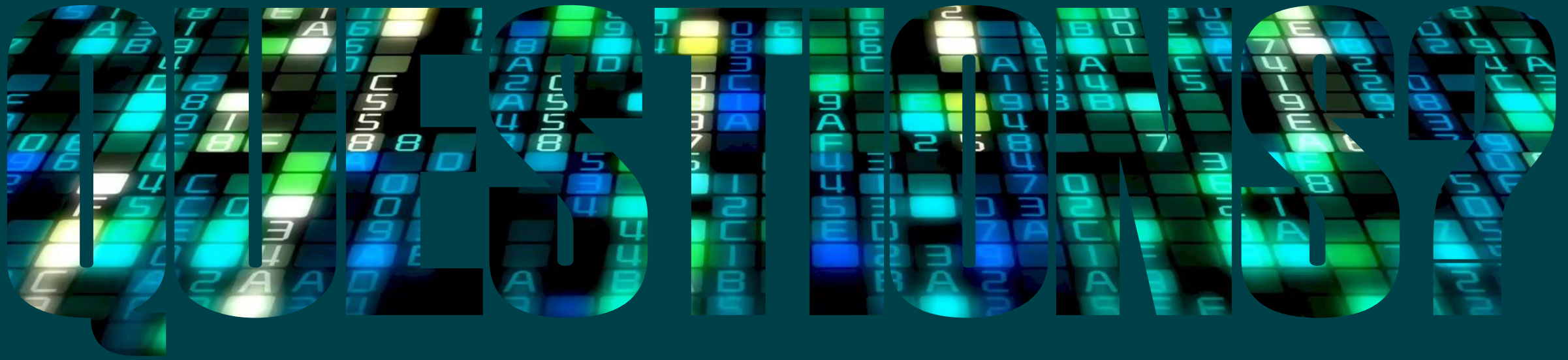
Aims to counter the impact of cognitive biases including **accepting data as true without assessing its credibility**...

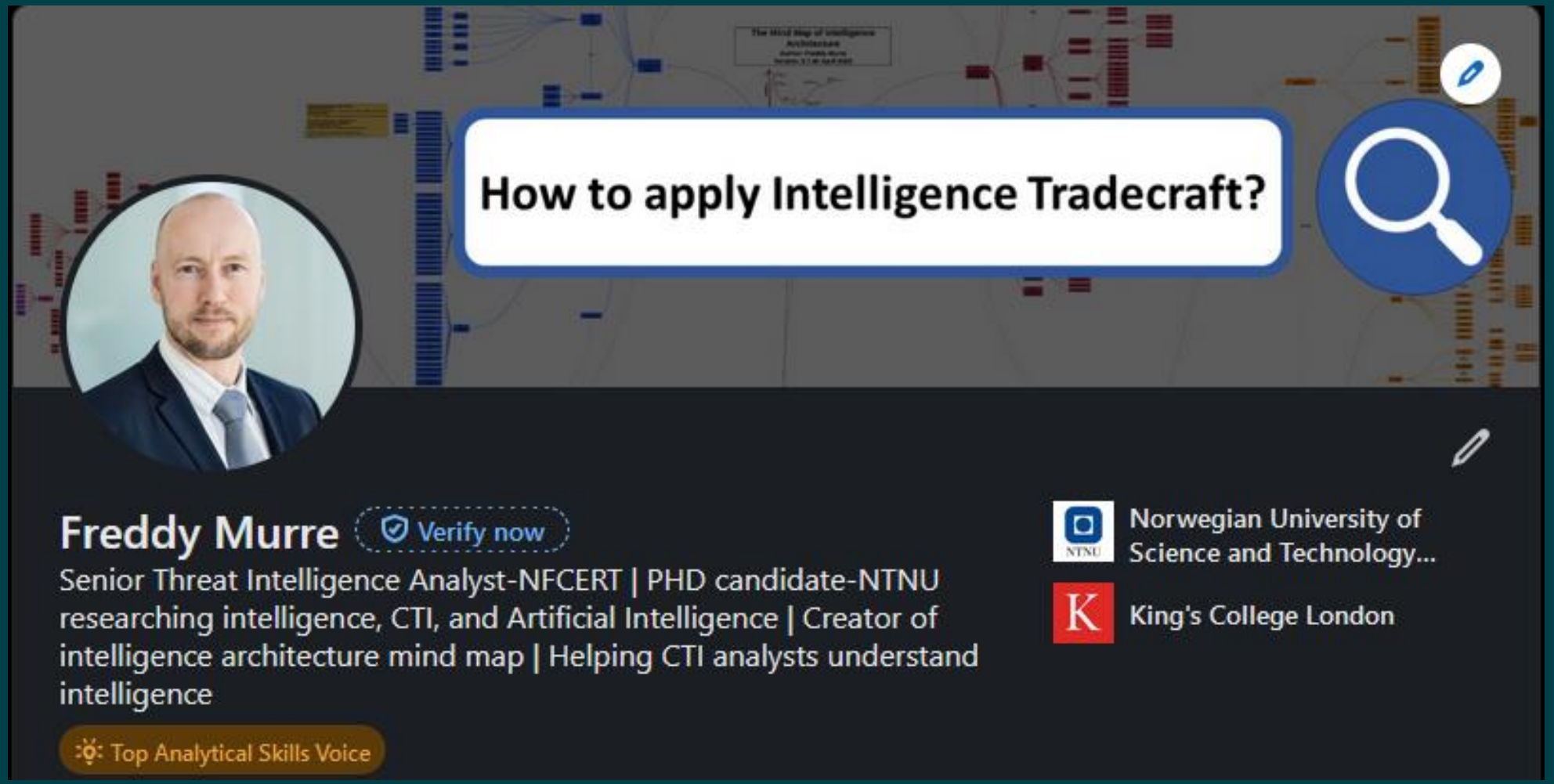



20 May 2024
Ticketmaster Breach
• Ticketmaster confirms breach linked to Snowflake
28 May 2024
ShinyHunters
• “ShinyHunters” mirrors Ticketmaster breach post on BreachForums
8 July 2024
Sp1d3rHunters
• Sp1d3rHunters leaks over 30,000 TicketMaster TicketFast barcodes
SpidermanData
• "SpidermanData" offers data from Ticketmaster for $500,000
26 May 2024
Sp1d3r
• Sp1d3r leaks data of 1 million Ticketmaster users for free
20 June 2024

Conclusion and Key Takeaways

- Use the Admiralty System to analyze claims by sources
- Look for alternative explanations to avoid confirmation bias
- Externalise your thinking using SATs
- Assess source, THEN information to quickly sift through and eliminate the noise
- The Admiralty System can help CTI teams navigate the claims my by threat actors, other researchers, and vendors with greater confidence


QUESTIONS?


How to apply Intelligence Tradecraft?
Freddy Murre
Verify now
Senior Threat Intelligence Analyst-NFCERT | PHD candidate-NTNU researching intelligence, CTI, and Artificial Intelligence | Creator of intelligence architecture mind map | Helping CTI analysts understand intelligence
Top Analytical Skills Voice
Norwegian University of Science and Technology...
King's College London