Clearwater

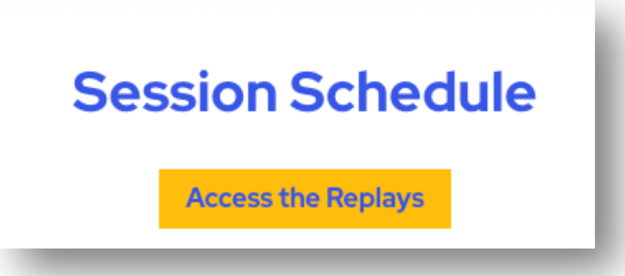
Healthcare – Secure, Compliant, Resilient

Monthly Cyber Briefing

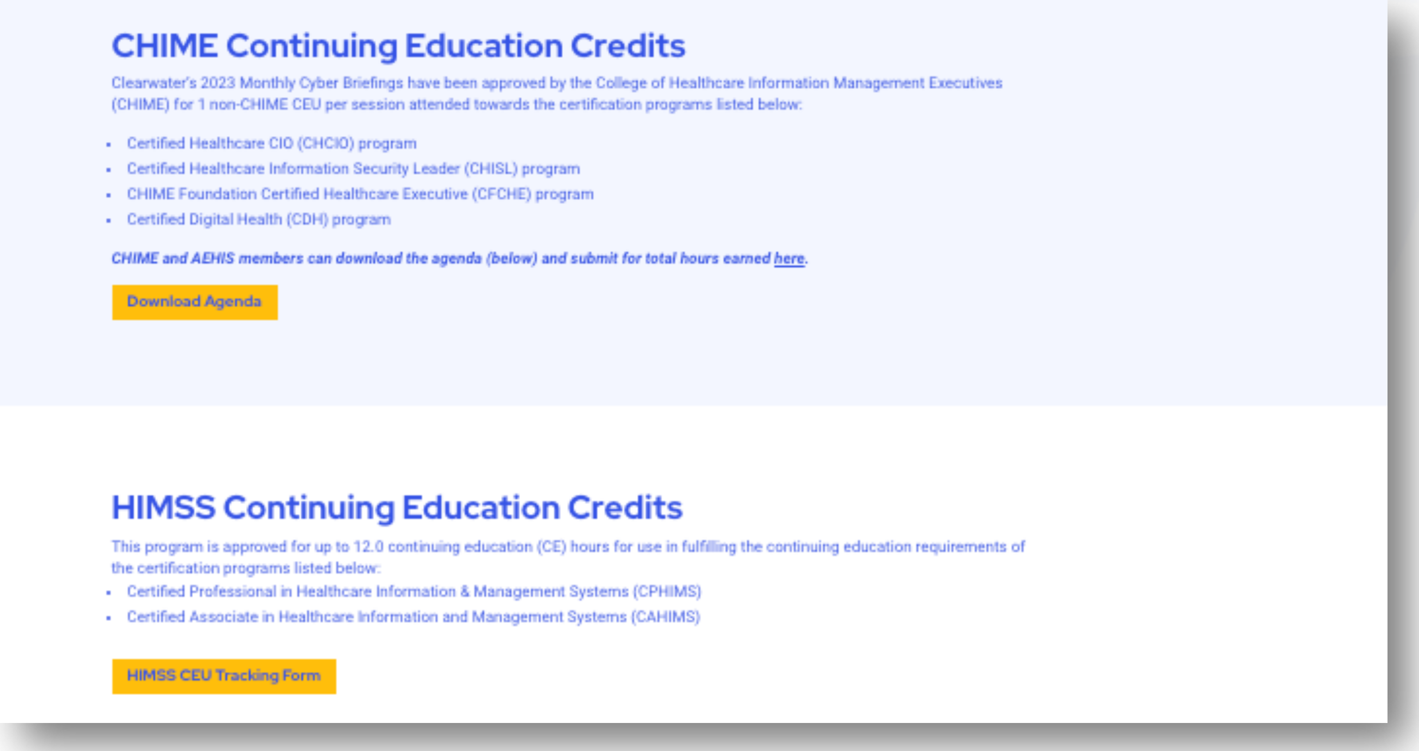
December 2023

Logistics

- All attendees in “Listen Only Mode”
- Please ask content related questions in Q&A
- Cyber Briefings are eligible for HIMSS & CHIME CE credit
- Recording and final slides shared within 48 hours
- Please take a few minutes to provide feedback via survey prompt at the end of this session



Session Schedule



CHIME Continuing Education Credits

Clearwater's 2023 Monthly Cyber Briefings have been approved by the College of Healthcare Information Management Executives (CHIME) for 1 non-CHIME CEU per session attended towards the certification programs listed below:

- Certified Healthcare CIO (CHCIO) program
- Certified Healthcare Information Security Leader (CHISL) program
- CHIME Foundation Certified Healthcare Executive (CFCHE) program
- Certified Digital Health (CDH) program

CHIME and AEHIS members can download the agenda (below) and submit for total hours earned here.

HIMSS Continuing Education Credits

This program is approved for up to 12.0 continuing education (CE) hours for use in fulfilling the continuing education requirements of the certification programs listed below:

- Certified Professional in Healthcare Information & Management Systems (CPHIMS)
- Certified Associate in Healthcare Information and Management Systems (CAHIMS)

Clearwater

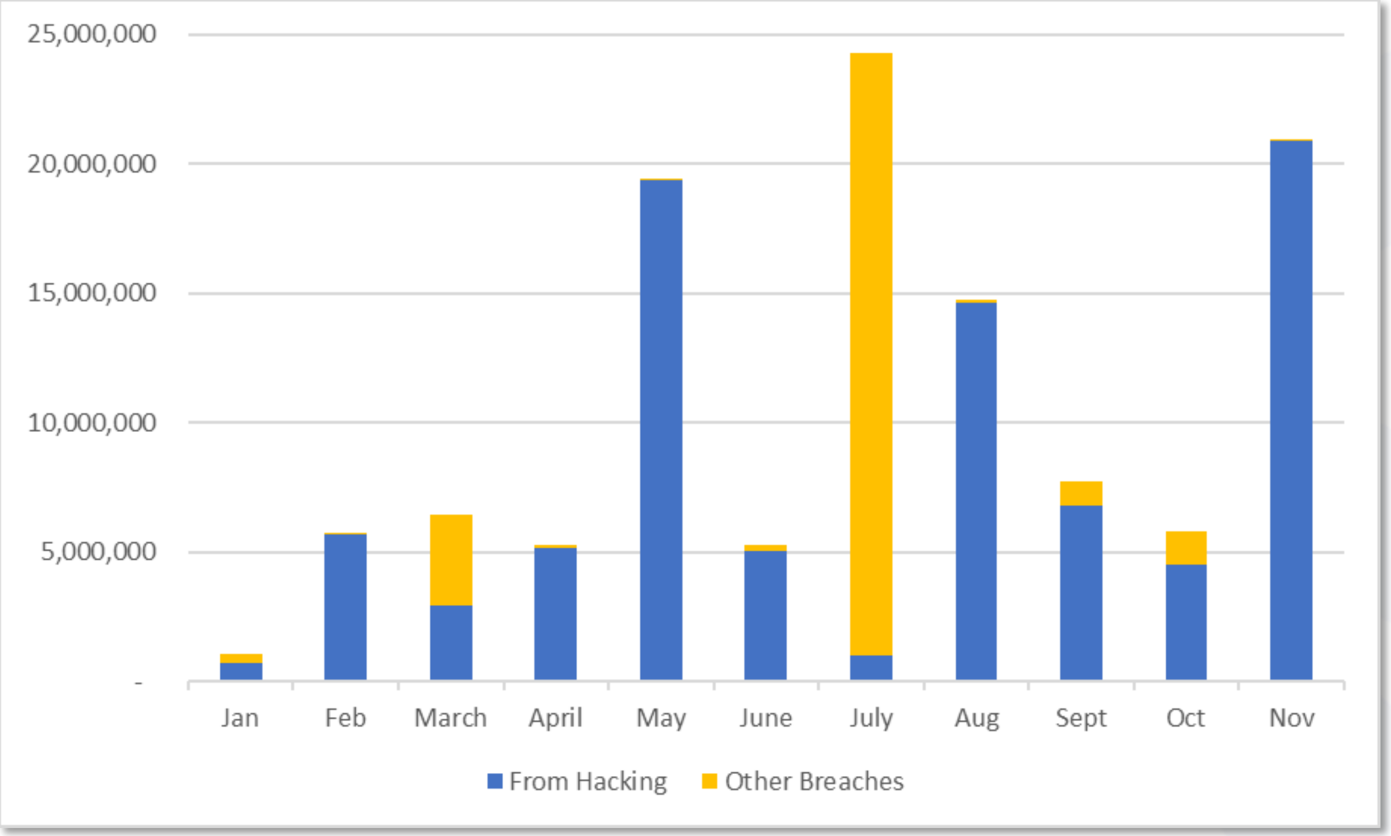
Agenda: Cyber Update

- Know your adversary
- Identify and address your vulnerabilities

Cyber Update

Dave Bailey

Healthcare Breaches

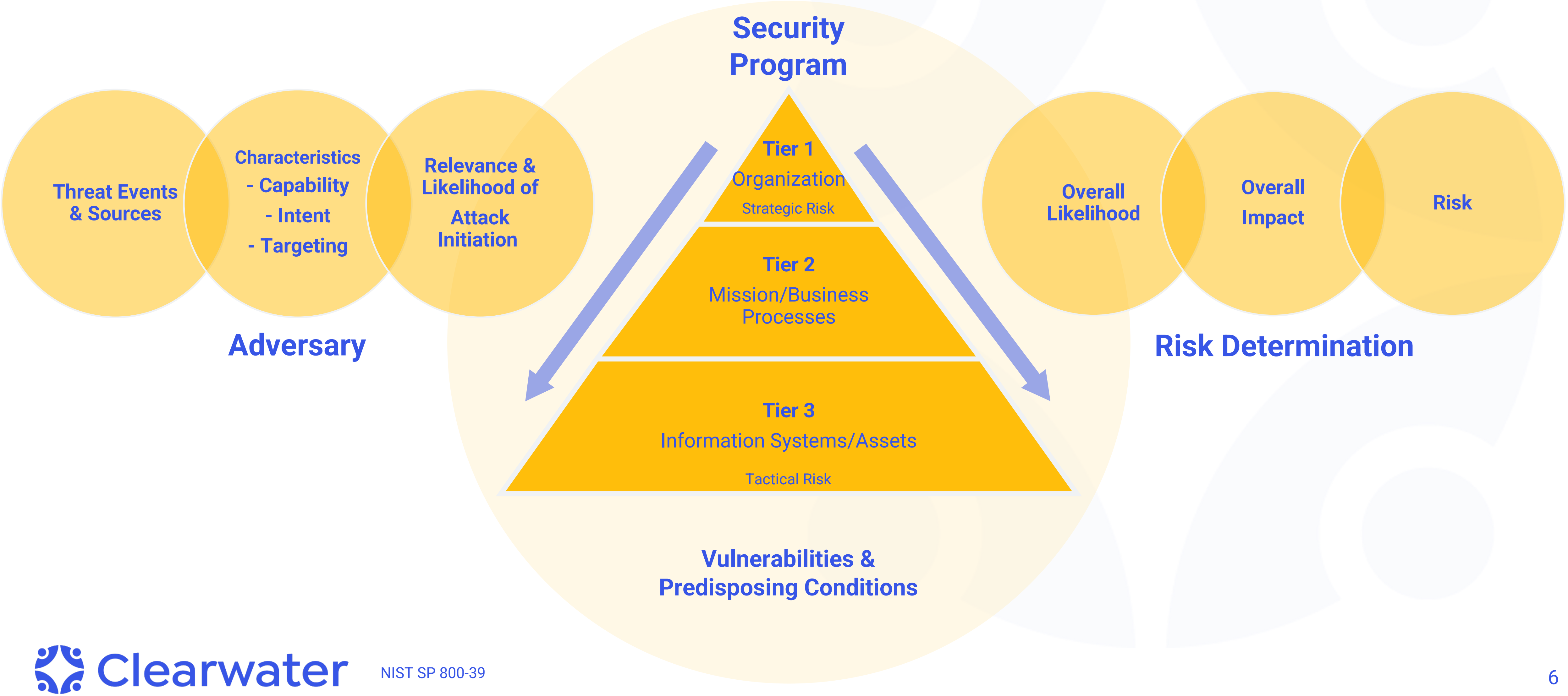


	Count of Breaches	Affected Records
YTD 2023	621	116,672,559
2022	719	55,458,966

Clearwater

Source: HHS Breach Portal Nov 30

Effective Risk Management = Knowing The Adversary



Security Program

Threat Events & Sources

Characteristics
- Capability
- Intent
- Targeting

Relevance & Likelihood of Attack Initiation

Adversary

Tier 1
Organization
Strategic Risk

Tier 2
Mission/Business Processes

Tier 3
Information Systems/Assets
Tactical Risk

Vulnerabilities & Predisposing Conditions

Overall Likelihood

Overall Impact

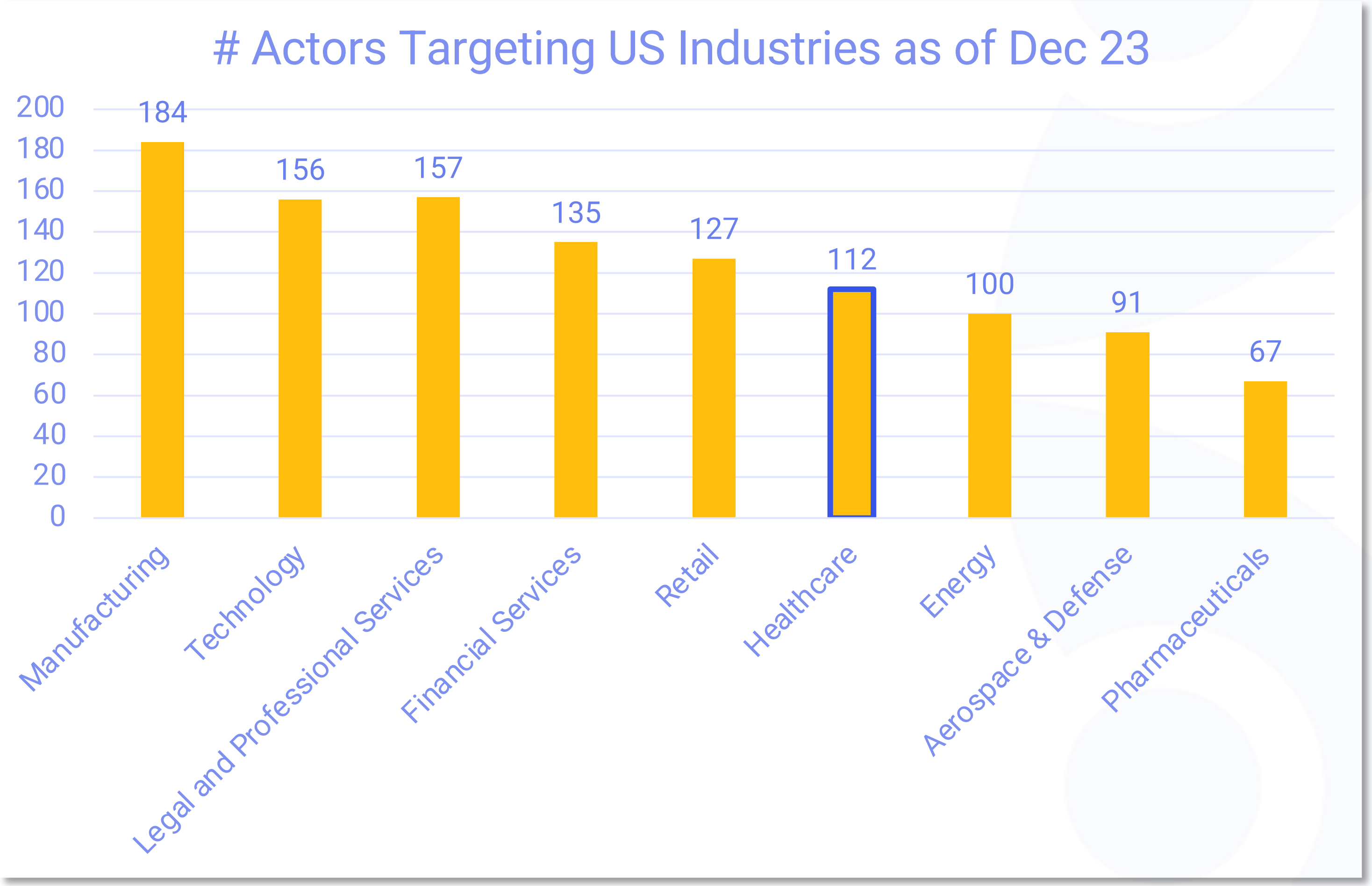
Risk

Risk Determination

Clearwater

NIST SP 800-39

Cyber Actors Targeting the US



Source: Mandiant Threat Intelligence

Top Attacks Utilized by Cyber Threat Actors

1. Social Engineering
2. Phishing & Business Email Compromise
3. Distributed Denial of Service
4. Botnet (deny service, spread ransomware and malware, steal data and more)
5. Zero-day Vulnerability/Exploit

Types-threat-actors-threaten-healthcare

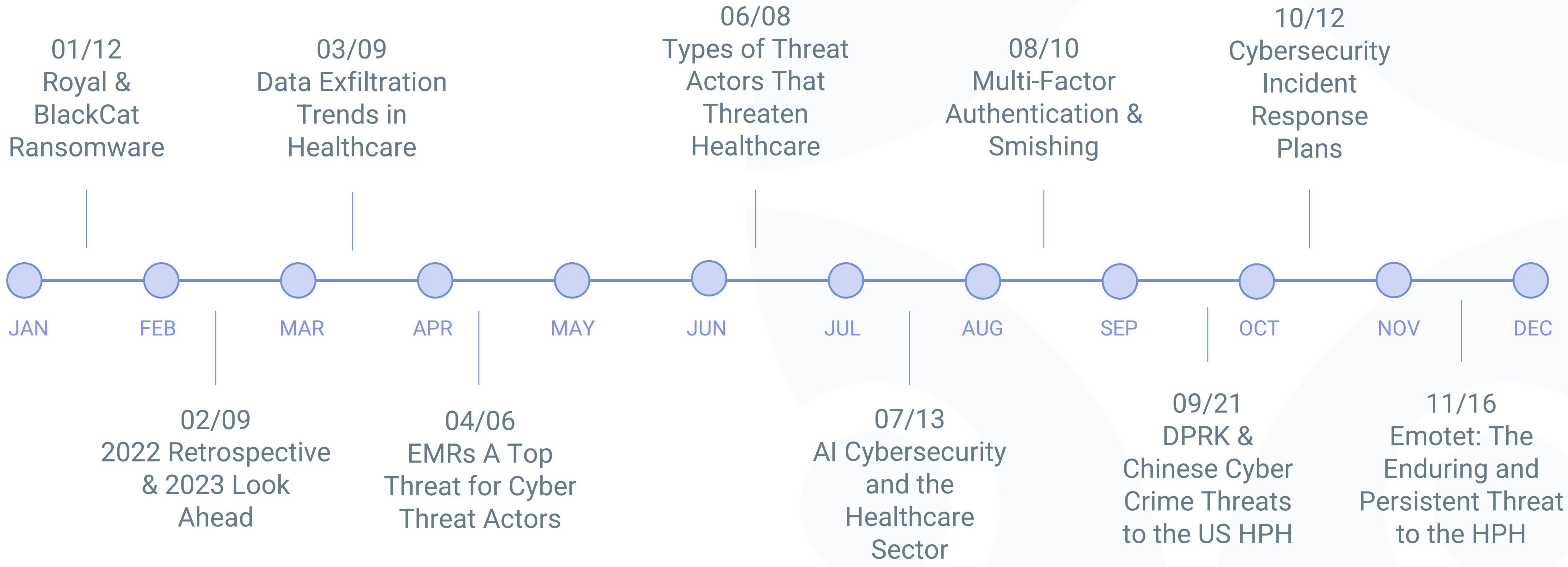
Clearwater

HC3 Threat Briefings – 2023 YTD

Office of **Information Security** Securing One HHS

Health Sector Cybersecurity Coordination Center

Relevant cybersecurity topics to raise HPH's situational awareness of current cyber threats, threat actors, best practices, and mitigation tactics



01/12
Royal & BlackCat Ransomware

02/09
2022 Retrospective & 2023 Look Ahead

03/09
Data Exfiltration Trends in Healthcare

04/06
EMRs A Top Threat for Cyber Threat Actors

06/08
Types of Threat Actors That Threaten Healthcare

07/13
AI Cybersecurity and the Healthcare Sector

08/10
Multi-Factor Authentication & Smishing

09/21
DPRK & Chinese Cyber Crime Threats to the US HPH

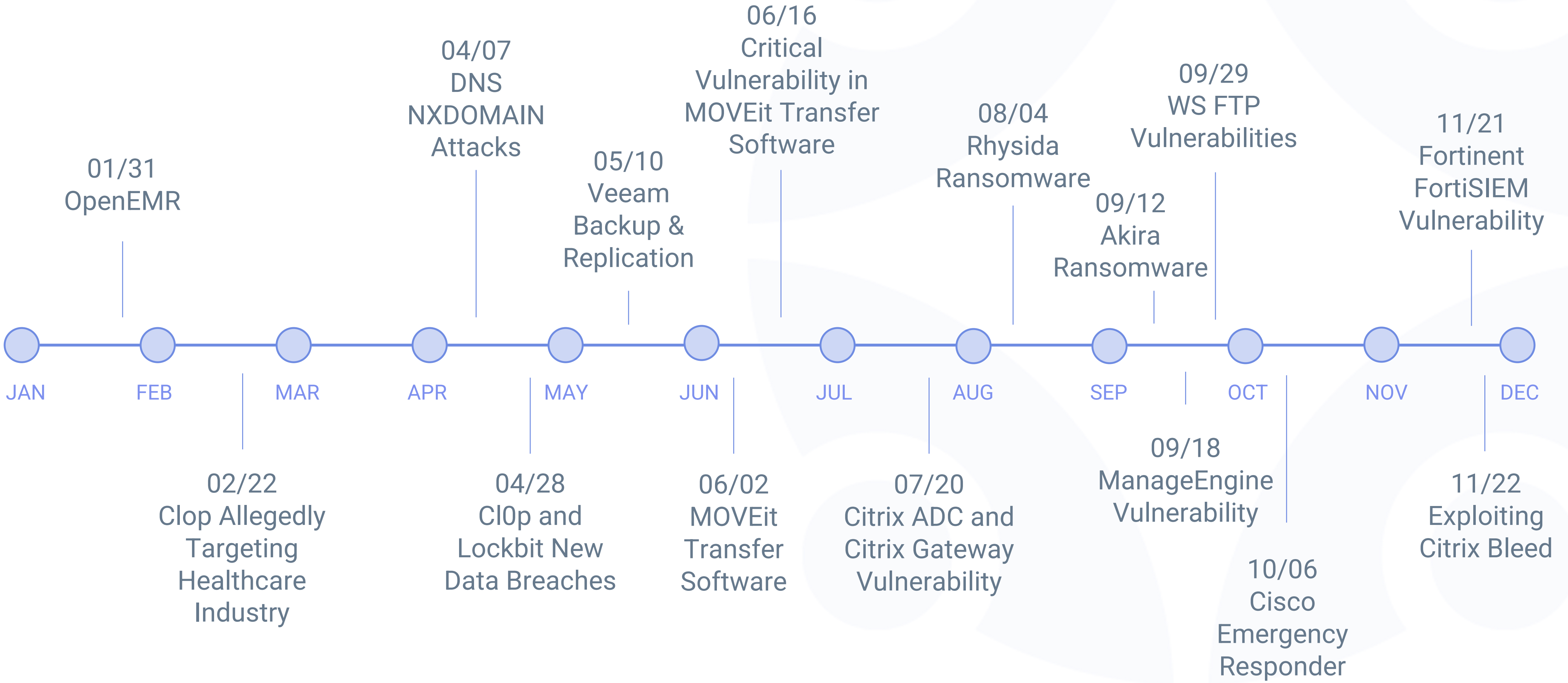
10/12
Cybersecurity Incident Response Plans

11/16
Emotet: The Enduring and Persistent Threat to the HPH

https://www.hhs.gov/about/agencies/asa/ocio/hc3/products/index.html#threat-briefs

HC3 Sector Alerts – 2023 YTD

Designed to assist the sector with defense of large scale and high-level vulnerabilities



01/31 OpenEMR

02/22 Clop Allegedly Targeting Healthcare Industry

04/07 DNS NXDOMAIN Attacks

04/28 Cl0p and Lockbit New Data Breaches

05/10 Veeam Backup & Replication

06/02 MOVEit Transfer Software

06/16 Critical Vulnerability in MOVEit Transfer Software

07/20 Citrix ADC and Citrix Gateway Vulnerability

08/04 Rhysida Ransomware

09/12 Akira Ransomware

09/18 ManageEngine Vulnerability

09/29 WS FTP Vulnerabilities

10/06 Cisco Emergency Responder

11/21 Fortinent FortiSIEM Vulnerability

11/22 Exploiting Citrix Bleed

https://www.hhs.gov/about/agencies/asa/ocio/hc3/products/index.html#sector-alerts

Emotet Threat to the Health Sector

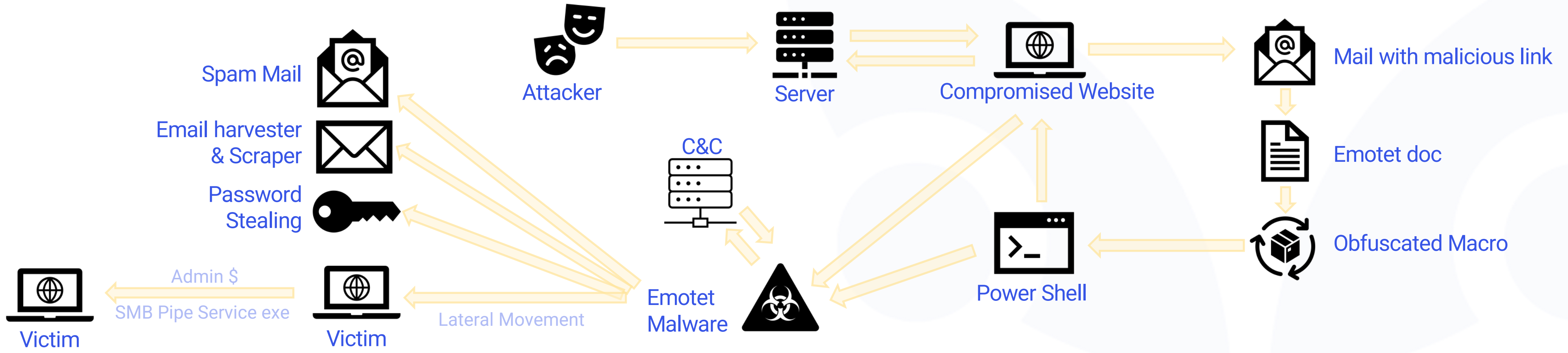
Emotet Overview

- Operational since at least 2014
- A significant part of the cybercriminal ecosystem, which maintains many working relationships with other major cybercriminal gangs
- Often delivered via **phishing**, but also via **known vulnerabilities** and **brute force**
- Modular, primarily capable of:
  - Infection, persistence, lateral movement
  - Data exfiltration (traffic capture, credential theft)
- Dropping additional malware/ransomware
  - Azorult, TrickBot, IcedID, Qbot, CobaltStrike & Ryuk, Bitpaymer

Emotet Returns

- Returned after government takedown in 2021 with new capabilities
  - Changes to the loader with new commands available
  - Changes to the dropper
  - New command and control infrastructure operational

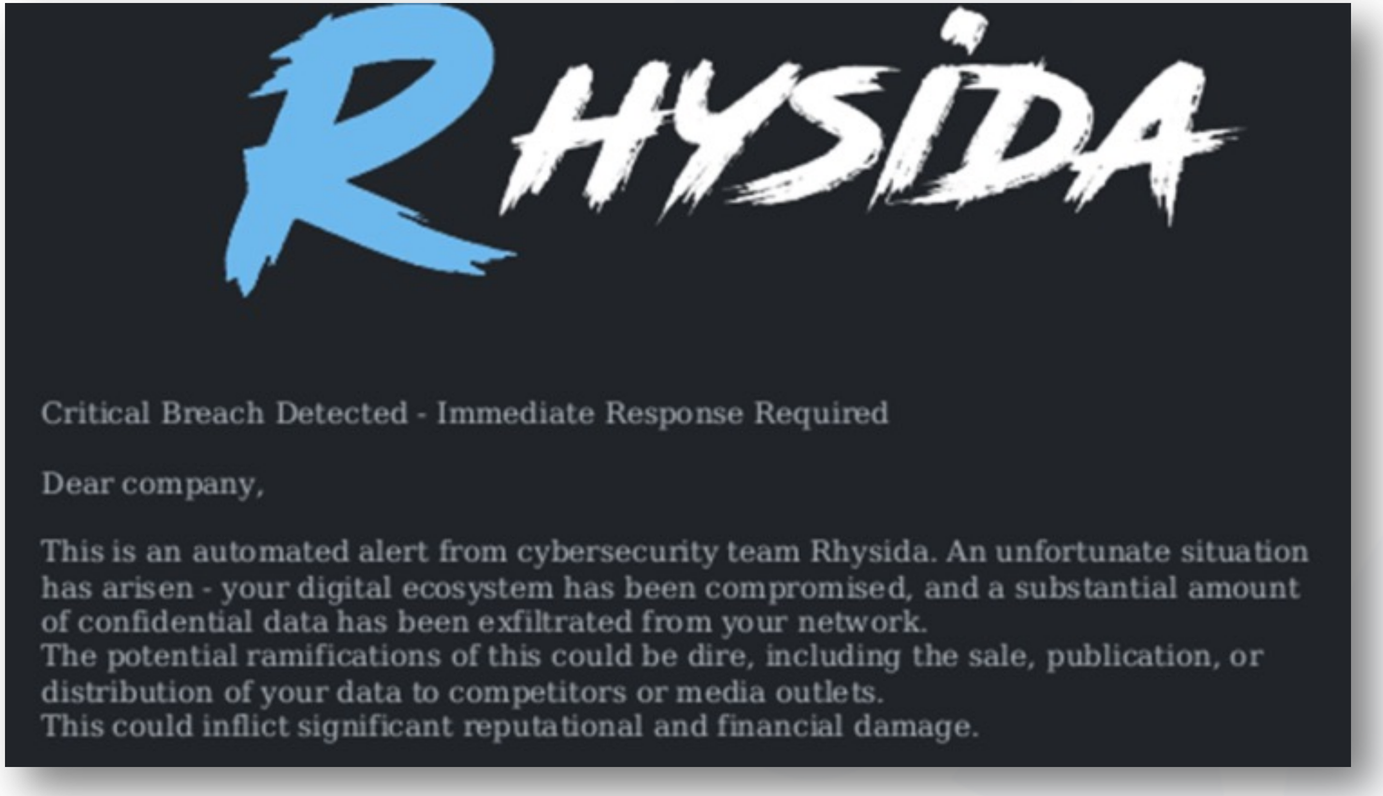
Basic Emotet Infection



Clearwater https://www.hhs.gov/sites/default/files/emotet-the-enduring-and-persistent-threat-to-the-hph-tlpclear.pdf

Ransomware "An unfortunate situation has arisen"

Ransomware as a Service (RaaS)



Critical Breach Detected - Immediate Response Required

Dear company,

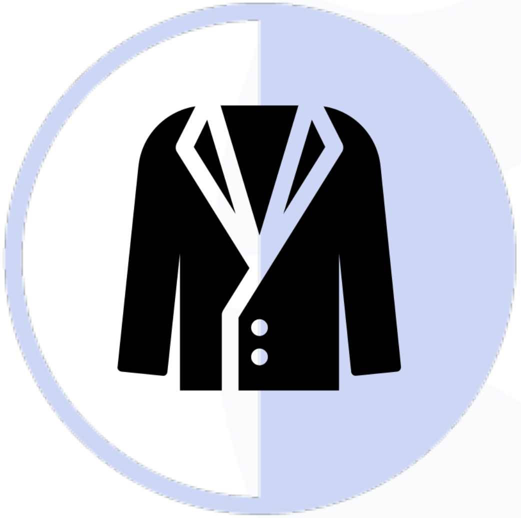
This is an automated alert from cybersecurity team Rhysida. An unfortunate situation has arisen - your digital ecosystem has been compromised, and a substantial amount of confidential data has been exfiltrated from your network.
The potential ramifications of this could be dire, including the sale, publication, or distribution of your data to competitors or media outlets.
This could inflict significant reputational and financial damage.

https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-319a

Double Extortion

BlackSuit operates using a double extortion method that steals and encrypts sensitive data on a compromised network.

Operates as a private ransomware operation without any known affiliates



- Data was successfully encrypted in 75% of ransomware attacks on healthcare
- Just 24% of healthcare organizations were able to disrupt a ransomware attack before their data was encrypted, a reduction from 34% in 2022

https://www.hhs.gov/sites/default/files/blacksuit-ransomware-analyst-note-tlpclear.pdf

data points from Sophos research: https://www.infosecurity-magazine.com/news/data-encrypted-ransomware/

Homeland Security Calling

Homeland Security warns Indiana hospital of an incident

https://www.beckershospitalreview.com/cybersecurity/homeland-security-warns-indiana-hospital-of-breach.html

Ransomware – Continuous Threats

Ransomware attack forces hospitals in multiple states to divert some emergency room patients

Hospitals across 6 states have been diverting patients from their emergency rooms due to a recent cyberattack on a major health system.

2 N.J. emergency rooms diverting patients due to ransomware attack

Hacked to Pieces?

The Effects of Ransomware on Hospitals

- Ransomware attacks decrease hospital volume by 17-25% during the initial attack week, reducing revenue.
  - Hospitals are forced to treat fewer patients during ransomware attacks
  - They provide less care (especially imaging and testing services) for the patients they do treat.
  - Approximately 25% of all hospital markets experienced a ransomware attack *and* its potential spillover effects to other providers (2016-2021)

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4579292

Extortion Escalation to SEC

ALPHV/BlackCat reporting their breach of a financial business directly to the SEC when a ransomware request was ignored. With the new SEC regs about to go into effect December 15, we'll likely see more of this tactic.

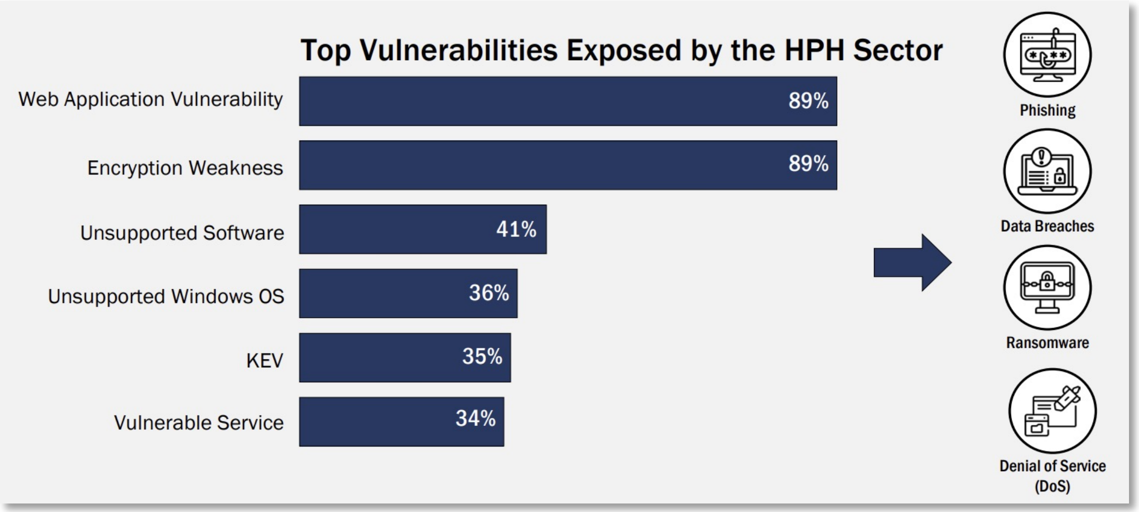
https://www.scmagazine.com/perspective/alphv-blackcat-reporting-to-the-sec-could-become-the-new-normal-for-ransomware-operators

Assumptions & Takeaways From an Attack

- A threat actor was present in your environment
- Assume data was exfiltrated and prove otherwise
- At least one account was compromised (most likely many)
- Assume the attack is on-going, an attacker is still in your environment and prove otherwise

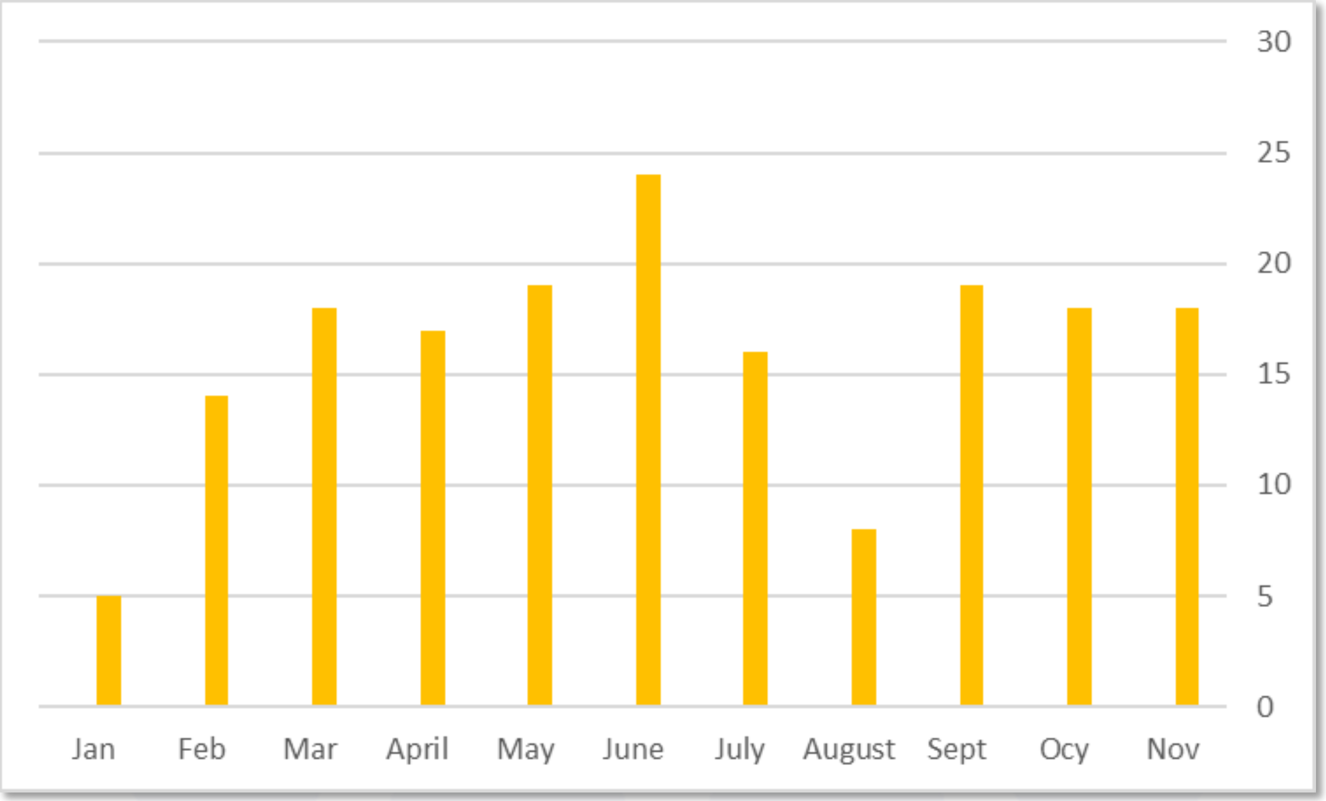
Clearwater

Vulnerabilities open doors to Attacks



"Exposure of these vulnerabilities can result in detrimental cyber activity, such as ransomware, data breaches, or denial-of-service."

CISA Known Exploited Vulnerabilities (KEV) – Monthly count



https://www.cisa.gov/resources-tools/resources/mitigation-guide-healthcare-and-public-health-hph-sector

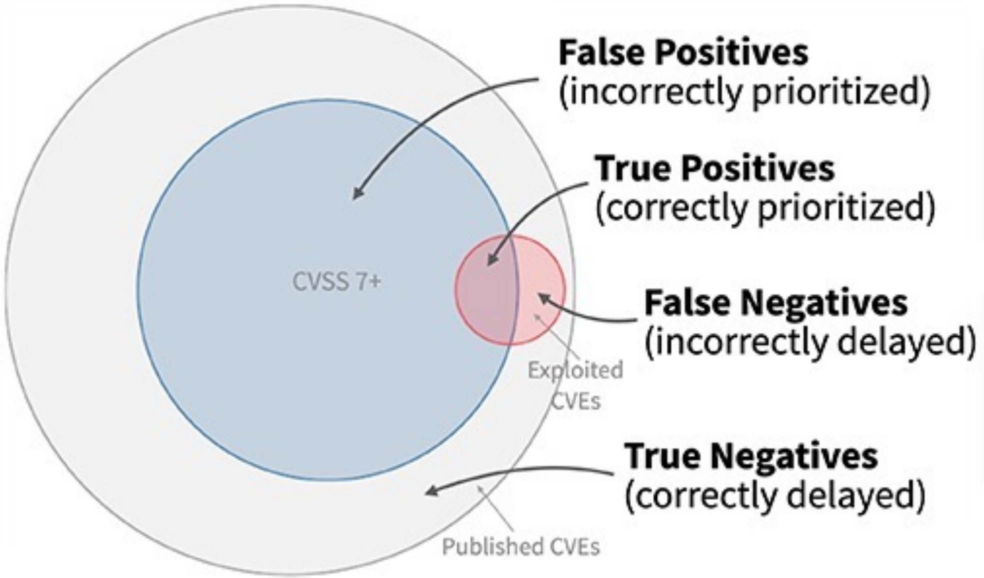
Exploit Vulnerability, Rinse & Repeat

The disclosure of a vulnerability, particularly one acknowledged as previously exploited in the wild, highlights potentially viable mechanisms for future exploitation.

Zero-day and N-day vulnerabilities observed in 2022 demonstrated threat actors' ability to leverage specialized knowledge to circumvent mitigations from previous patches to target the same vulnerable components.

Vulnerability Management – Risk Prioritization

- Primary prioritization for many is by CVSS
  - In 2022 – ~25K Vulnerabilities Released
  - Of those ~15K had a CVSS >=7
  - Using this method, we need to focus on 15K
- <8% of published vulns. are exploited
  - ~1200-2000 actual exploits
- Orgs that only use CVSS, working on 7–12x more vulnerabilities than those that use known exploit



Prioritize based on known exploited risk

Clearwater H-ISAC Risk-Based Approach to Vulnerability Prioritization White Paper

Assumptions and Takeaways

- Use Risk / Known Exploit Based Prioritization of Remediation
  - Couple with Asset Criticality, Device Placement, Compensating Controls
- Curate a list of credible sources (H-ISAC for example) along with direct critical vendors to obtain alerts/notifications about vulnerabilities and patches that are relevant to your organization
  - Assume vendors may not get it right the first time
  - Even once “fixed”, will need to monitor for carry-on/follow-on fixes
- Confirm with Critical Partners/Third Parties or any party with access to sensitive data, like ePHI, their susceptibility and response to critical vulnerabilities
  - Challenge any vague or inconclusive response

Q&A

We are here to help.

Moving healthcare organizations to a more secure, compliant, and resilient state so they can achieve their mission.

Cyber Briefings will continue in 2024!

Next session = Jan. 11th

Access replays: Clearwater's Resource Center > Webinars and Events

New York Hospital Cybersecurity: A Look at the Proposed Regulations, Implementation, and Grant Impact | December 14 @ 2:00 CT

Episode #40: Managing Cybersecurity for Legacy Medical Devices

Clearwater

Healthcare – Secure, Compliant, Resilient

Contact us

info@clearwatersecurity.com

www.clearwatersecurity.com

1.800.704.3394

Legal Disclaimer

Although the information provided by Clearwater Compliance may be helpful in informing customers and others who have an interest in data privacy and security issues, it does not constitute legal advice. This information may be based in part on current federal law and is subject to change based on changes in federal law or subsequent interpretative guidance. Where this information is based on federal law, it must be modified to reflect state law where that state law is more stringent than the federal law or other state law exceptions apply. This information is intended to be a general information resource and should not be relied upon as a substitute for competent legal advice specific to your circumstances. YOU SHOULD EVALUATE ALL INFORMATION, OPINIONS AND RECOMMENDATIONS PROVIDED BY CLEARWATER IN CONSULTATION WITH YOUR LEGAL OR OTHER ADVISOR, AS APPROPRIATE.

Copyright Notice

*The existence of a link or organizational reference in any of the following materials should not be assumed as an endorsement by Clearwater Compliance LLC.