Monthly Cyber Briefing

November 6, 2025

Clearwater

Meeting Logistics

Microphones

All attendees are on mute.

Questions

Type your questions in the Q&A box.

Resources

Upcoming events, slides & resources linked.

Recording

Recording will be provided after event.

Survey

Survey will prompt at the end of webinar.

Healthcare's Monthly Cyber Briefing

Agenda + Speakers:

- Cyber & Regulatory Update
- From Point-in-Time to Real-Time - How Continuous Threat Exposure Management Strengthens Cyber Resilience
- Q+A

Dave Bailey, VP of Security Services, Clearwater

Jeremy Hughes, Manager, Security Engineering Services, Clearwater

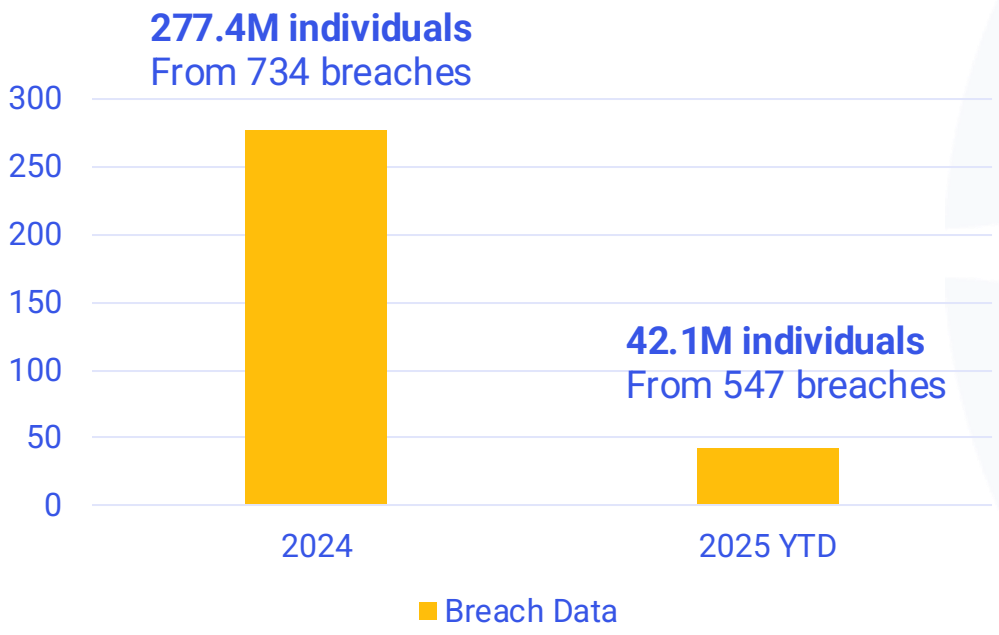
Cyber & Regulatory Update

Dave Bailey, VP of Security Services, Clearwater

Clearwater

No Updates to Reported Breaches Since October 1st

Breach Data Dashboard



1 The HHS Breach Portal (2024 data through 12/31/24, pulled on 3/30/25; 2025 data through 10/31/25, pulled 11/2/25)

Notable Breaches:

- **10.5M+** patients impacted by Conduit Business Solutions data breach: **8th largest healthcare breach reported** & claimed by **SafePay** ransomware gang in Oct 2024, stealing 8.5T of data

Class Action Impact

- CA-based network of affiliated physician practices to pay $50M
- Integris Health to pay $30M
- Yale New Haven Health to pay $18M
- Court finalizes HCA data breach class action settlement

Clearwater

Industry Threat Brief Summary

Healthcare and Pharmaceuticals Industry Threat Reports Q3 2025

Clearwater | Google Threat Intelligence

Industry Snapshot for Healthcare Provides an Overview of Relevant Threats Based on Google Threat Intelligence (GTI)

Industry Snapshot: Healthcare (Q3 2025)

A stark new reality for the healthcare sector emerged in October 2025, with a landmark report revealing that cyberattacks are now directly linked to adverse clinical outcomes, including a **rise in mortality rates** at 29% of affected organizations.

This fourth annual study from Proofpoint and the Ponemon Institute found that cyber incidents caused patient care disruptions at 72% of healthcare organizations, leading to increased medical procedure complications and longer patient stays.

While **cloud account compromises** were the most prevalent threat type, **supply chain attacks proved most likely to impact patient care**.

Industry Snapshot for Pharmaceuticals Provides an Overview of Relevant Threats Based on Google Threat Intelligence (GTI)

Industry Snapshot: Pharmaceuticals (Q3 2025)

The pharmaceutical sector is facing a severe and multifaceted threat landscape, underscored by the August 2025 ransomware attack on drug research firm Inotiv by Qilin. The incident, which Inotiv confirmed in an SEC filing, caused significant disruptions to business operations, encrypted internal systems, and resulted in the theft of approximately **176 GB of proprietary research data**.

This attack exemplifies a **broader strategy** where threat actors **target critical "middle systems"** that bridge IT and operational technology, knowing that disrupting processes like drug development or product labeling is **more likely to compel a ransom payment**.

Compounding these extortion threats is the emergence of new malware such as ResolverRAT, a remote access trojan observed since early 2025 using localized phishing and in-memory execution to specifically compromise healthcare and pharmaceutical firms.

In October, CISA Published 30 Advisories Related to Vulnerabilities in Industrial Control Systems (ICS) and Medical Devices

Key Impacts:

- **Critical Weaknesses Identified:** Vulnerabilities such as out-of-bounds writes, missing authentication, and OS command injections were found across various vendor products. These weaknesses pose a direct threat to the security and reliable operation of affected medical devices.
- **High Exploitation Potential**: Multiple advisories received critical CVSSv3 scores. This indicates that the identified vulnerabilities have a severe potential for exploitation by malicious actors, which could lead to unauthorized access, data manipulation, denial of service, or even direct harm to patients through compromised device functionality.

Medical Device(s):

- **NIHON KOHDEN:** manufacturer of medical electronic equipment, including patient monitors, defibrillators, and neurology equipment.
- **Siemens:** produces a wide range of medical devices and solutions.
- **Oxford Nanopore Technologies**: Specializes in DNA/RNA sequencing technology, which is increasingly vital for medical diagnostics and research.
- **Vertikal Systems:** software and systems used in hospital environments, which often manage or integrate with medical devices.

Ransomware Update

Impacts from Ransomware in October

Clearwater | Google Threat Intelligence

October Demonstrated a Multi-Actor Escalation of Ransomware with Sinoibi & Qilin Leading the Way

Most of these attacks were **publicly exposed via dark web leak sites**, continuing the trend of **double extortion** and **data exposure** seen throughout the year

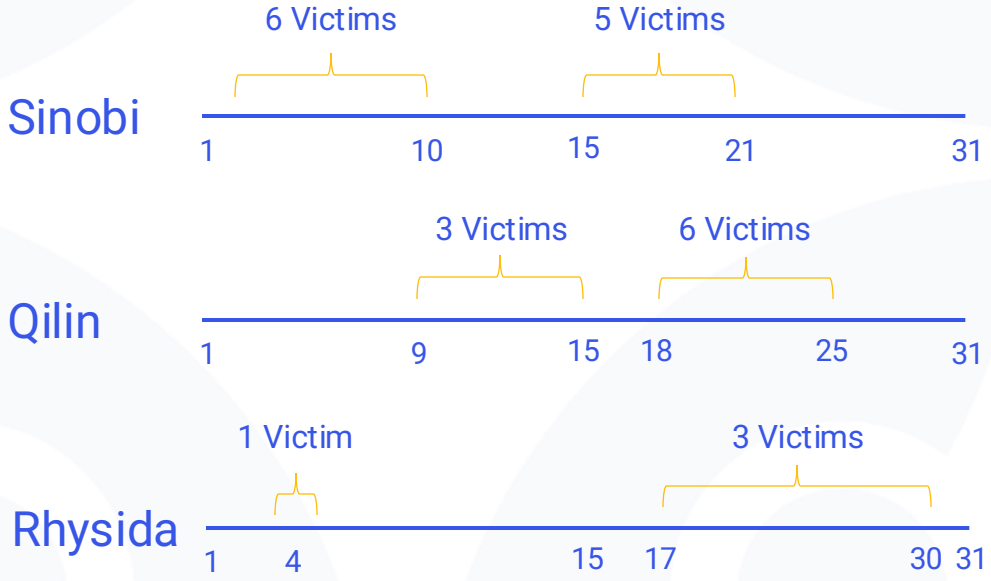
50

October marked a notable escalation **(67% increase)** in ransomware activity against the U.S. healthcare sector, with **50** confirmed incidents recorded across **hospitals, medical practices, dental offices, and behavioral health facilities**.

62%

Key ransomware operators—**Sinobi**, **Qilin**, **Rhysida**, **World Leaks** and **DevMan 2.0**—accounted for over **62%** of total activity, underscoring sustained, coordinated targeting of healthcare networks and patient information systems.

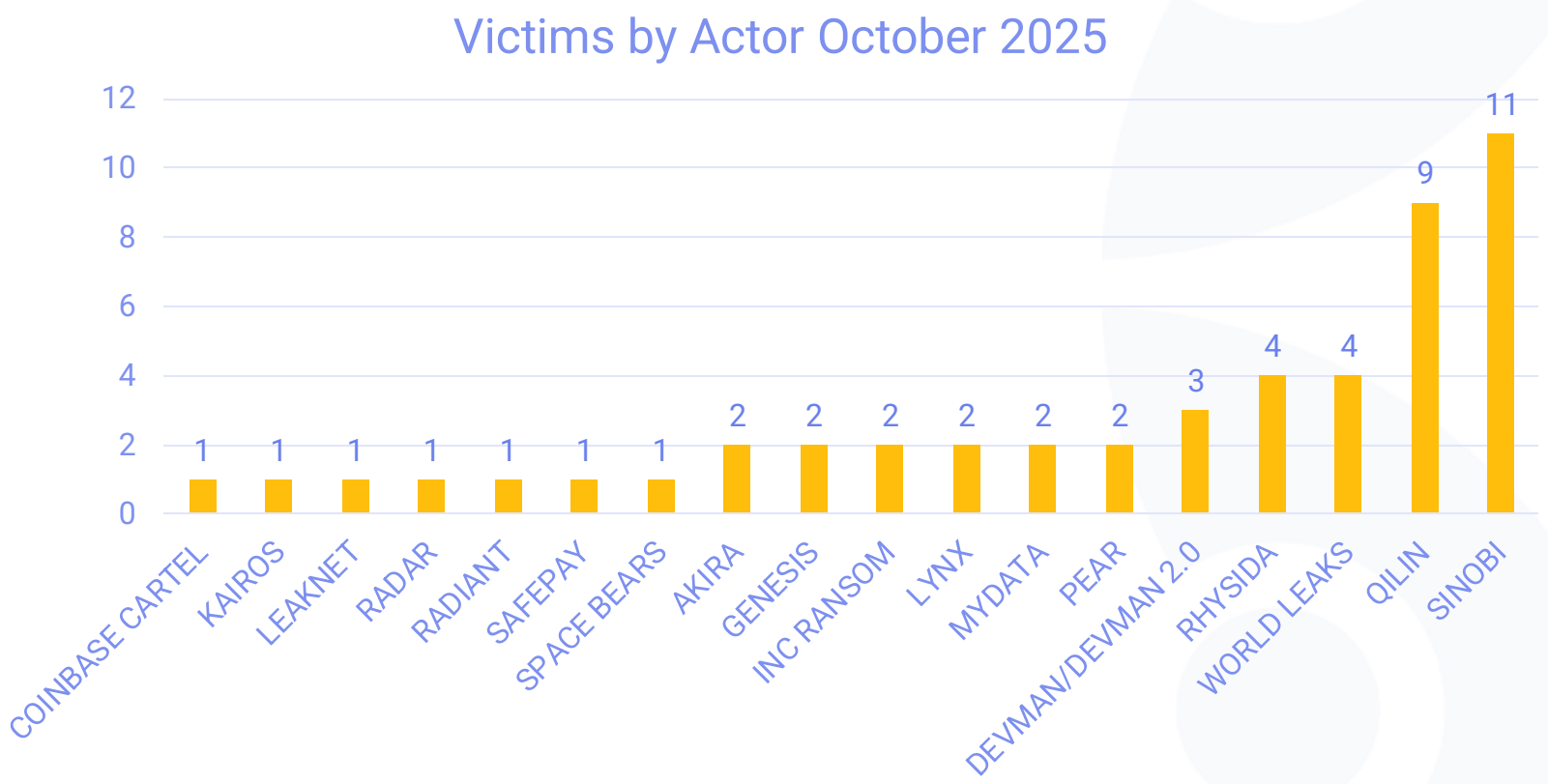
Notable Oct Campaign Timelines



Clearwater

Google Threat Intelligence

Ransomware Attacks Continue to Disrupt Operations, Delay Patient Care, and Expose Millions of Patient Records



Industry Focus:

- **Shift in Targeting**: Increase in attacks on mid-size organizations and other healthcare business
- **Dominance in Data Exfiltration**: Data theft is a critical component with many groups abandoning encryption
- **Geographic Concentration**: The U.S. remains the country with the highest number of ransomware attacks on healthcare orgs

A Fast Start to November:

- Nov. has already claimed (8) victims
  - (4) **Qilin**
  - (2) **Akira**
  - (1) **Inc Ransomware**
  - (1) **MyData**

Clearwater Google Threat Intelligence

Ransomware Targeting Patterns

Impacts from Ransomware in October

Clearwater | Google Threat Intelligence

Shift Towards Mid-Sized and Specialty Care Providers

Threat actors have significantly shifted their focus towards U.S. mid-sized and specialty care providers over the past 90 days (from August 2025 thru October 2025), driven by financial motives and an increased exploitation of third-party vendors for broader access.

Observation	Typical Victim Type	Motive
Ransomware groups—particularly **Qilin**, **Rhysida**, and **Sinobi** focused on mid-sized healthcare networks, specialty clinics, and outpatient practices rather than large national hospital chains.	▪ Lack dedicated cybersecurity teams or managed detection response (MDR) support ▪ Depend heavily on unsegmented, legacy systems ▪ Have high patient data value relative to their ability to defend or negotiate effectively	**Attackers can rapidly exfiltrate data** and achieve faster ransom conversions (often within 3–5 days) without triggering major federal response coordination seen in large hospital breaches

High Concentration on Sensitive Health Data Repositories

The past 90 days have revealed a pronounced and sustained focus by threat actors on sensitive U.S. health data repositories, ranging from patient records and personally identifiable information (PII) to protected health information (PHI) and valuable research data. This concentration is a critical element of the broader shift in targeting within the healthcare sector.

Observation	Typical Victim Type	Motive
Actors such as **DevMan 2.0** and **Genesis** were observed targeting radiology, pathology, and laboratory groups — entities that handle: Diagnostic imagery (MRI, CT, X-ray metadata). Genomic or pathology results linked to identifiable health records. Shared data pipelines across multiple hospital partners	These targets yield large volumes of sensitive Protected Health Information (PHI) and research data, which can be repurposed for secondary extortion or sold on dark web forums (e.g., Genesis Market).	Breaches of these facilities amplify downstream exposure—data from one compromised lab may contain patients from dozens of unaffiliated hospitals.

Behavioral and Mental Health Facilities Under Increased Pressure

This type of information is extremely valuable to cybercriminals for various purposes, such as identity theft, extortion, and targeted social engineering. The value of this data aligns with the overall trend of data theft as a primary objective for many financially motivated groups.

Observation	Typical Victim Type	Motive
October saw multiple claimed compromises of behavioral and mental health service providers, such as: Spindletop Center Richmond Behavioral Health Authority Greater Mental Health of New York	These organizations store **high-sensitivity psychological and addiction treatment data, which carries extreme blackmail potential.** Threat actors appear to understand this **leverage** — extorting victims not only for decryption keys but also for non-disclosure of patient information to regulators or media.	Psychological data offers ransomware groups **dual monetization** — ransom recovery and dark market resale (for identity exploitation, social engineering, or stalking).

Dental, Optometry, and Small Clinical Targets as “Low-Hanging Fruit”

Threat actors' renewed focus on smaller, specialized healthcare providers highlights the value of patient data, reliance on third-party services, and potential to attack less mature cybersecurity programs.

Observation	Typical Victim Type	Motive
Groups like **Sinobi** and **World Leaks** heavily targeted **dental and small specialty clinics**	These facilities: Commonly outsource IT to small managed service providers. Operate with **flat networks and minimal endpoint protection**. Hold valuable financial and insurance data, despite limited cyber maturity.	These actors exploit **insecure remote access portals (RDP/VPN)** and **third-party IT supply chains**, then pivot laterally to extract billing and claims databases.

Highly Motivated and Active Threat Actors Targeting Healthcare

Qilin

- The Qilin ransomware group, active since at least August 2022, operates a ransomware-as-a-service (RaaS) model, employing **double extortion tactics**: The ransomware used is known as “Agenda”
- Recently enhanced its offerings to affiliates, introducing a "Call Lawyer" feature in early May 2025
- Introduced a distributed denial-of-service (DDoS) capability in April 2025. Other planned features include a DDoS panel, an email spamming tool, a call/SMS spamming tool/service, and the involvement of journalists.
- Initial access is typically gained through leaked credentials via a virtual private network (VPN), followed by the deployment of tools like Cobalt Strike and Mimikatz for persistence and further credential theft

Sinobi

- The malware family known as "INC" is also identified by the aliases "Sinobi" and "Lynx".
- INC is a Windows-based ransomware, developed in C, that encrypts files across local, removable, and network drives
- INC ransomware can empty the Recycle Bin, deleting volume shadow copies, terminating processes, modifying the Desktop background to display a ransom note, and printing the ransom note via connected printers.
- Sinobi Data Leak Site emerged in July 2025 and reported 45 victims in Q3 2025 targeting Healthcare, Legal & Professional Services, and Media & Entertainment, as well as the Technology sector

Sector Updates

HHS Focus on Cybersecurity

Clearwater | Google Threat Intelligence

Relevant Updates From the HSCC CWG

Publication of the "Health Industry Cybersecurity – Sector Mapping and Risk Toolkit (SMART)"
The HSCC CWG published a toolkit in October 2025 called **SMART** ("Sector Mapping and Risk Toolkit") which provides templates and a methodology for visualizing, identifying and measuring systemic risk posed by third-party technology, software, and communications services essential to clinical, administrative and manufacturing workflows

Updated Task Groups for 2025 Work Plan Released
The HSCC CWG's task-group list for 2025 was updated very recently and publicly posted:
Some highlights:

- *Artificial Intelligence Cybersecurity* – focus on emerging risks for AI/ML-based products and services
- *Cybersecurity Board Governance* – toolkit development for boards and CISOs
- *Cybersecurity Updating & Patching* – defining "reasonably updateable/patchable" and best practices
- *Post Quantum Cryptography* – roadmap and inventory for cryptographic risk and migration in the sector
- *Under-Resourced Provider Cybersecurity Advisory Group* – support for smaller/underserved health providers

Recommended Actions for Healthcare Organizations

Focus Area	Actions
Strengthen Access & Identity Controls	▪ Enforce MFA on all accounts, especially remote access, VPNs, RDP and admin ▪ Limit external remote access to minimum necessary; strong RBAC ▪ Monitor & restrict third-party/vendor access
Vulnerability Management & Patch Hygiene	▪ Maintain a robust vulnerability management program ▪ Prioritize patching ▪ Ensure secure configuration of devices and hardening
Backup, Disaster Recovery & Resilience	▪ Maintain immutable, offline, air-gapped backups ▪ Regularly test backup restorations (table-top and live tests) ▪ Maintain an incident response plan for ransomware
Detection & Monitoring	▪ Deploy advanced endpoint detection & response (EDR) ▪ Have continuous monitoring of events ▪ Use threat intelligence to monitor for TTPs
Network Architecture & Segmentation	▪ Segment critical clinical networks ▪ Harden and monitor network boundaries ▪ Logically isolate backups
Vendor & Third-Party Risk Management	▪ Assess cybersecurity posture of vendors, MSPs, medical-device suppliers ▪ Require vendor access to be tightly controlled ▪ Include in contracts obligations for incident reporting, security reqs, and audits

Healthcare's Cyber Briefing

From Point-in-Time to Real-Time - How Continuous Threat Exposure Management Strengthens Cyber Resilience

Jeremy Hughes, Manager, Security Engineering Services, Clearwater

What is Continuous Threat Exposure Management?

Periodic Assessments

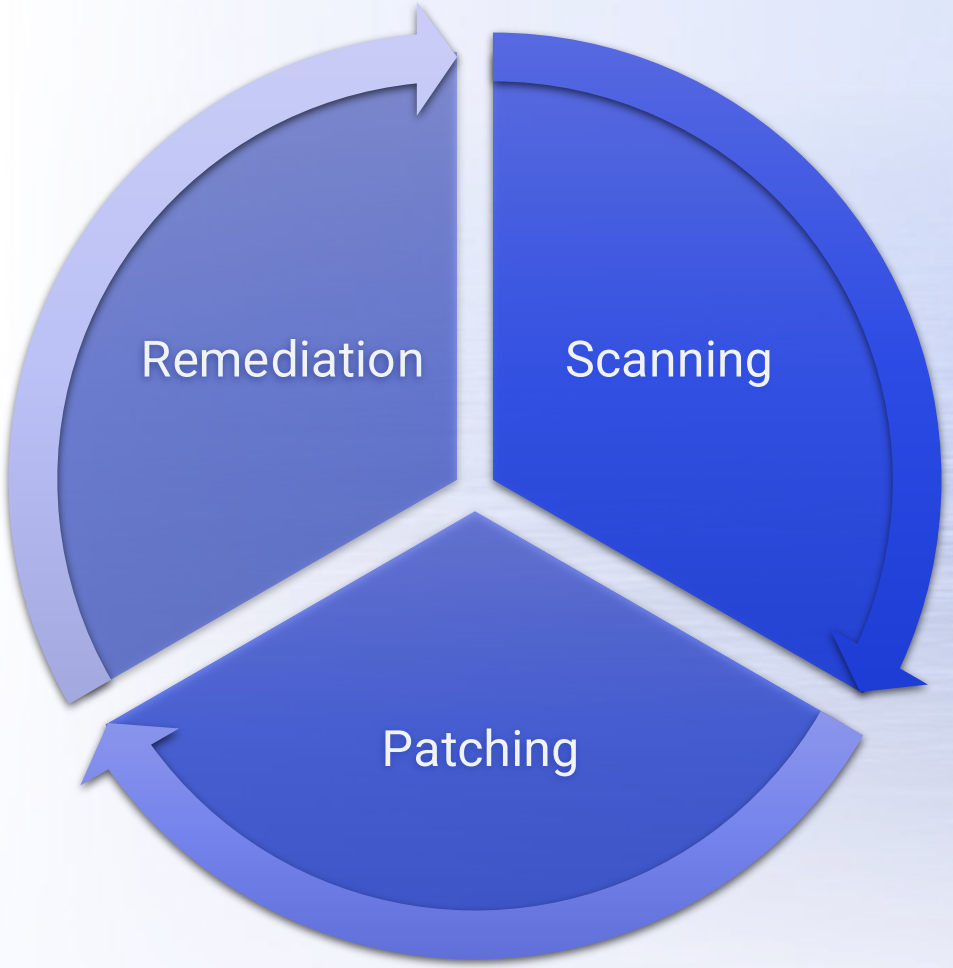
Near Real-Time Monitoring

Some of Today's Challenges in Healthcare Security

- Monthly vulnerability reports with thousands of findings
- Limited knowledge around what systems are externally facing
- Implemented security tools with questionable effectiveness

Clearwater

Vulnerability Management



Clearwater

Vulnerability Management Shift to CTEM

Legacy Scanning

- Weekly/Monthly

CTEM Scanning

- Frequent Discovery Scans
- Agent-Based Vulnerability Scans

Vulnerability Management Shift to CTEM

Legacy Patching

- SCCM/WSUS
- Scripting
- Manual Update

CTEM Patching

- Automated patching of OS and 3rd Party Applications

Clearwater

Vulnerability Management Shift to CTEM

Legacy Remediation

- Remote Access
- Scripting

CTEM Remediation

- Gold Images
- Group Policy/Central Management

External Attack Surface Management (EASM)

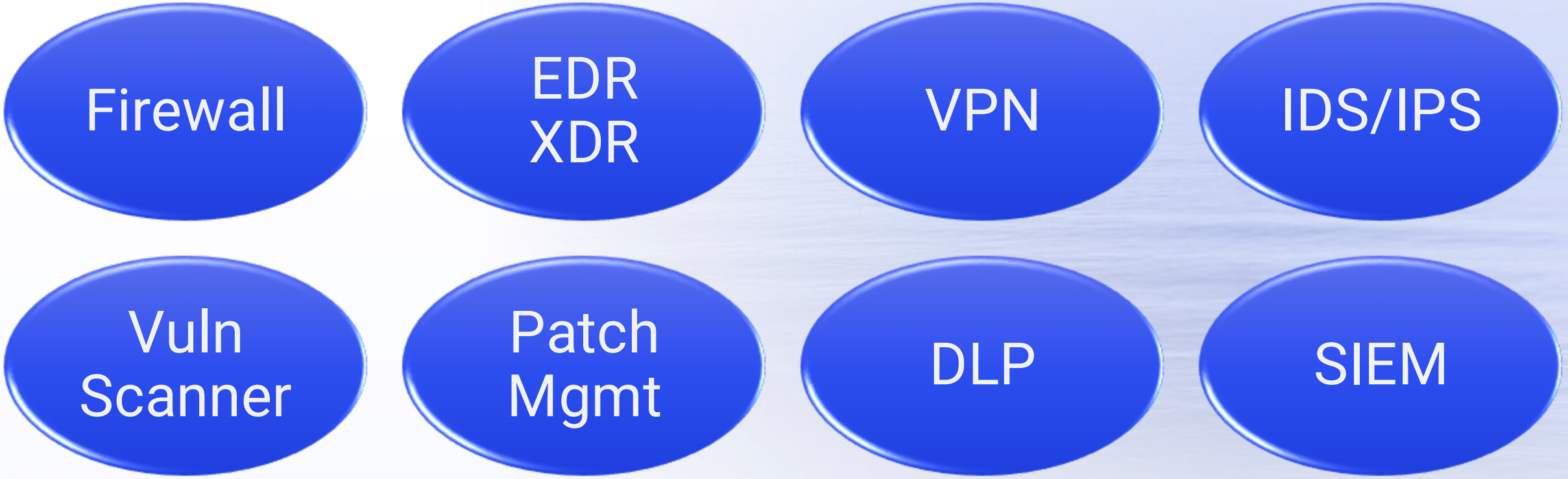
Legacy EASM

- Spreadsheets
- Annual pen tests
- Or nothing at all

CTEM EASM

- Daily discovery and vulnerability scans
- More frequent or even automated external pen tests

Today’s Healthcare Security Controls



> **Misconfiguration** of technical security controls is a **leading cause** for continued success of **attacks**.
>
> **Align** security controls optimization efforts with a continuous threat exposure management (**CTEM**) **program** to support a **repeatable** process for prioritizing and implementing improvements. Investing in **automated assessment** and **validation** tools and services can help **alleviate** some of the burden.

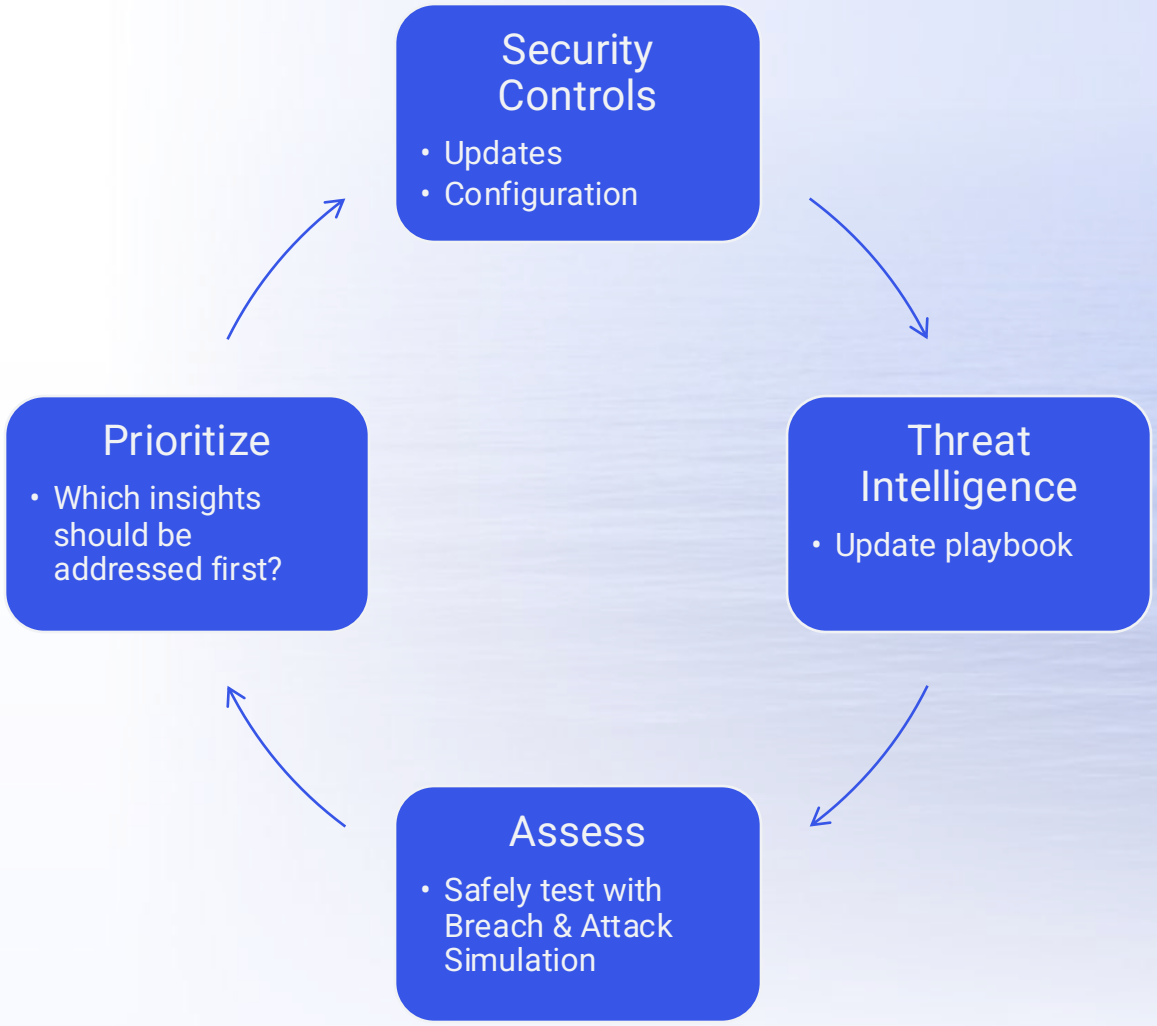
April 2025 – Gartner Reduce Threat Exposure With Security Controls Optimization

What is Breach and Attack Simulation (BAS)?

- Safely simulate real-world attacks across entire kill chain
- Validate control effectiveness across entire security stack
- Comprehensive threat library
- Rapid threat updates
- Actionable Insights with remediation guidance
- Dashboards and Comprehensive Reporting

Clearwater

Security Control Validation Architecture



Clearwater

What is the Difference Between BAS and Pen Testing

BAS

- Action: Safely launch full playbook of attacks against test systems
- Objective: Record success rate of attacks and security control performance
- Outcome: Results and remediation guidance

Pen Test

- Action: Leverage Ethical Hacker and technical tools
- Objective: Verify whether a threat actor could breach your environment, often in a pre-determined way
- Outcome: Results and remediation guidance

Current Emerging Threat Mitigation Process

Situation: A new critical zero-day vulnerability or attack vector is released

- Threat Intelligence:
  - Use web resources to identify potential risk
  - Gather IOCs and file hashes
- Validation
  - Scan for vulnerable systems
- Mitigation:
  - Apply patches if possible
  - Block identified file hashes
  - Configure alerting for evidence of compromise
  - Poll vendors for mitigation assurance

CTEM-Aligned Emerging Threat Mitigation Process

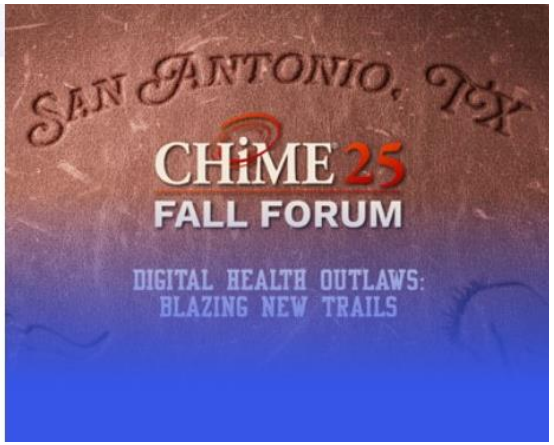
Situation: A new critical zero-day vulnerability or attack vector is released

- Threat Intelligence:
  - BAS automatically updates playbooks
- Validation
  - Vulnerability data automatically updated within hours from agents
  - Run BAS simulations against your representative architecture
- Mitigation:
  - Deploy patch automatically when available
  - Implement remediation guidance supplied by BAS
  - Configure alerting for evidence of compromise

Clearwater

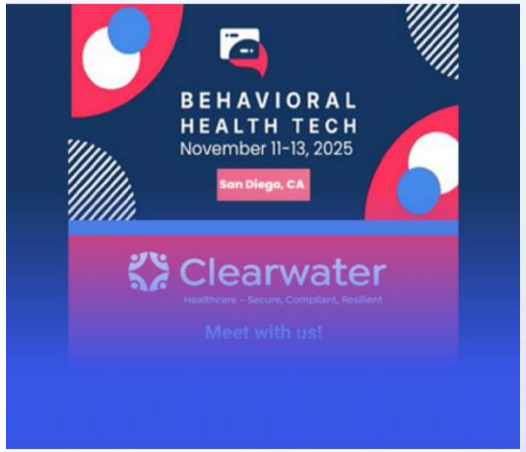
Q&A

Upcoming Webinars + Events



CHIME Fall Forum | November 10-13 | San Antonio, TX

- Clearwater is a proud sponsor and is hosting a focus group on Medical Device/IoT Vulnerability Management on Nov. 11
- Learn more here



Behavioral Health Tech Conference| November 11-13 | San Diego, CA

- Clearwater is proud to sponsor and participate in BHT2025, to explore how technology, security, and compliance are shaping the future of behavioral health and driving better, more connected care.
- Learn more here

SCCE AI & Compliance Virtual Conference | November 20

- Clearwater's VP of Privacy and Compliance Services, Andrew Mahler, will share expert insights on global AI governance and strategies for responsible innovation during his session, "**Navigating Global AI Regulations: A Compliance Roadmap**".
- Register Here

Monthly Cyber Briefing | Thursday, December 4 | 12:00 pm CT

- **2025 in Review: What the Breaches, Threats, and Data Tell Us Now**
- Dave Bailey, VP Security Services & Steve Akers, CTO & Corporate CISO, Clearwater
- You are already auto-enrolled and will receive an updated link for December soon.

Clearwater

We are here to help.

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

Clearwater

Healthcare – Secure, Compliant, Resilient

www.ClearwaterSecurity.com

800.704.3394

LinkedIn | linkedin.com/company/clearwater-security-llc/

Legal Disclaimer

Although the information provided by Clearwater Security & Compliance LLC 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 Security & Compliance LLC.