Analyst1 for the Healthcare Industry

Overview

The healthcare industry consists of various sectors: medical services, medical equipment manufacturers, pharmaceuticals, medical insurance, and healthcare for patients. With the plethora of sensitive and lucrative data stored via these sectors, it's no wonder the industry as a whole is vulnerable to cyber attacks.

For cybercriminals these attacks can be rewarding, but in many caess, these bad actors exploit networks/ devices just to create chaos, leading to significant losses. Data breaches alone cost the sector $4B in 2019, and to punctuate the severity of cybercrime in healthcare, a Ponemon study found healthcare data breaches cost more per record to resolve than in any other industry.

> "The **attack surface is growing** and cybercriminals are developing more sophisticated tools and techniques to attack healthcare organizations, gain access to data and hold data, and networks to ransom."
>
> HIPAA Journal

What is the problem?

The healthcare industry is uniquely vulnerable to cyberattacks. Healthcare organizations store vast quantities of valuable data, and while investment in cybersecurity has improved, 59% of healthcare organizations do not believe their cybersecurity budgets are enough to prevent data breaches.

Black Book Research found that nearly all health IT professionals stated threat actors outpace security technology and processes. And with the number of sophisticated criminal and nation-state attacks growing exponentially, the industry struggles to employ experienced personnel to mitigate the constant barrage of threats.

Most prevalent threats in the healthcare arena:

- Ransomware
- Data Breaches
- DDoS Attacks
- Insider Threat
- Phishing schemes
- Medjacking

The Solution

Security teams need help in making better decisions about how and where to allocate their resources — both human and financial. Mature organizations have many security tools at their disposal, but with the number of bad actors detected daily, it is often overwhelming to keep up. Investing in the right tools can help healthcare organizations respond faster to security incidents, and improve breach identification and containment times.

Analyst1 for the Healthcare Industry

Results with Analyst1

Analyst1 establishes an evolving knowledge base of correlated insights about threats, attack patterns, malware families, vulnerabilities, internal assets, mission-critical systems at risk, and the defensive posture of a network over time.

Analyst1 reduces tool fatigue by providing a "single pane of glass" that facilitates seamless integration of multiple sources of information and eliminates labor-intensive tasks of assembling all information needed to prioritize mitigation actions.

$10.91 million per organization:
annual cost of cybercrime for life sciences industry

Accenture Ninth Annual Cost of Cybercrime Study

Analyst1 is a powerful solution for training threat teams on the critical skills needed to identify malicious activity. By determining the severity of threats to an organization, analysts can better defend against sophisticated attacks.

Analyst1 Capabilities

- Automate identification, collection, and correlation of diverse information
- Provide context and insights required to take action
- Author, text, and deploy effective countermeasures across multiple intrusion detection and prevention systems
- Detect and mitigate threat activity codifying cyber threat workflows
- Maintain traceability between evidence, indicators, rules and sensors to identify why a rule was created, the type of activity it detects, and what sensors are tasked.
- Obtain visibility into intrusion detection and prevention systems to maintain awareness of sensor types, enforced rules, POCs, physical locations, and logical locations.

(888) 4-ANLYST | info@analyst1.com
11921 Freedom Dr #550, Reston, VA 20190