Solving Alert Fatigue in Cyber Security

What Cyber Security Teams Can Learn from Healthcare Alarm Fatigue

1st Edition

HEXADITE
Intelligent Security Orchestration and Automation

HEXADITE
Intelligent Security Orchestration and Automation

A Similar Problem

In healthcare, the term "alarm fatigue" refers to the phenomenon where alarms are so frequent that they're often ignored despite the fact that they may be signaling an emergency. Similar to alarm fatigue in healthcare, today's cyber security teams are dealing with "alert fatigue", the constant notifications from detection systems

> Various devices, including beds, infusion pumps, cardiac monitors, ventilators, mechanical vital-sign machines, sequential compression stockings, and many others, have audible alarms competing for caregivers' attention. Unless managed properly, alarms meant to alert clinicians to problems that require action may put patients at risk.
>
> Many alarms are false; an estimated that 85% to 95% require no intervention. As a result, caregivers have become desensitized—a phenomenon called alarm fatigue—and simply ignore the alarms. But not all alarms are false, and assuming they're false can lead to dangerous delays in response.
>
> From The Official Journal of the American Nurses Association
> "Do you hear what I hear? Combating alarm fatigue"

HEXADITE
Intelligent Security Orchestration and Automation

Alarms and alerts are meant to signal a potential problem that needs immediate attention and action. However, when alarms are constant and have a high false positive percentage, they end up losing their meaning. Think of a nagging car alarm: what was meant to signal a theft in progress now just makes people think “somebody shut that off!”

In today’s Security Operations Centers (SOCs), cyber security incident response teams are dealing with their own version of alert fatigue. While they have invested millions in systems that detect and alert them to potential problems, the sheer volume and high rate of false positives undermine the value of the detection systems.

Alert Fatigue by the Numbers

Why Incident Response Teams Are Swamped

> Alerts can number in the thousands, or tens of thousands, a month. According to a survey by International Data Corporation (IDC), 37 percent of cyber security professionals reported facing 10,000 alerts per month of which 52 percent are false positives. The end result is a swamped staff.
>
> Bill Sweeney for SecurityWeek
>
> "Cutting Through the Noise: How to Manage a Large Volume of Cyber Alerts"

In his article "Cutting Through the Noise: How to Manage a Large Volume of Cyber Alerts", Bill Sweeney presents a set of statistics that highlight the scope of the problem facing IR teams:

- 37% of cyber security professionals face 10,000 alerts per month
- 52% of alerts are false positive
- A business with 3 full-time personnel can face 300 alerts daily
- 35% of companies spend 500+ hours per month responding to alerts
- Simply hiring more people is not a solution

The problem is only getting worse, as Sweeney states in his article "As the number of cyber attacks increase exponentially and these attacks become more complex, the volume of alerts facing today's cyber professionals will only continue to grow."

As cyber criminals count on an overwhelmed staff, the volume will only rise.

Contributing Factors

Staggering Similarities in Healthcare and Cyber Security

Healthcare alarm fatigue has become such a widespread critical problem that The Joint Commission (TJC) issued a sentinel event alert on alarms in April 2013 and made alarm management a National Patient Safety Goal starting in 2014. In its sentinel event alert, TJC identified several factors that contribute to alarm fatigue:

- Alarm parameter thresholds set too tight
- Alarm settings not adjusted to the individual patient
- Poor ECG electrode practices resulting in frequent false signals
- Inability of staff to hear alarms or detect where an alarm is coming from
- Inadequate staff training on monitors and alarms
- Inadequate staff response to alarms
- Malfunctioning alarms.

From The Official Journal of the American Nurses Association
"Do you hear what I hear? Combating alarm fatigue"

HEXADITE
Intelligent Security Orchestration and Automation

The same contributing factors to healthcare alarm fatigue apply to cyber security alert fatigue as well:

Alert threshold too strict

Although controversial for reasons we'll explore later, many feel that tuning the detection systems to receive fewer alerts will decrease the potential for alert fatigue. Fewer alerts mean fewer false positives leaving less to ignore.

Alert settings not customized

An alert detecting malware and one finding a phishing email are different and require different action. When all alerts are treated with the same degree of certainty and priority, all alerts are considered the same.

Frequent false positives

With false positive rates between 52% and up to 80%, the amount of time spent investigating false leads becomes tiring, and responders simply stop trusting the detection system.

Inability to respond to alerts

In some cases the issue is one of response. If an IR team member gets an alert but cannot access the endpoint, why bother getting the alert in the first place?

Inadequate response training

Without knowing how to respond properly, staff members don't know what to do.

Diminishing the Value of Detection Systems

How Tuning Alert Volume Decreases Value

> We were working, before automation, to try and lower the number of alerts that we saw, when in fact, what we really needed to do was expand the number of alerts that we see and respond to all of them.
>
> Golan Ben-Oni
> CIO, IDT Corp.

In the evolution of cyber security defense, detection systems have represented a monumental shift in the way companies deal with threats. Before the availability of SIEMs, network-based malware detection systems, and log repositories, companies were left in the dark knowing that they were facing malicious adversaries but having no visibility.

HEXADITE
Intelligent Security Orchestration and Automation

Today, however, the pendulum has swung to the other side. Using multiple detection systems in concert, the problem is no longer being able to detect issues, the problem is determining how to sift through the alerts to decide which are important enough to demand action.

Some organizations approach the problem with a solution that treats the symptoms while ignoring the real problem: they tune the detection system to see fewer alerts. While this method may solve the short term issue of seeing too many alerts, it effectively just ignores what the detection system was brought in to do in the first place: find and alert when potential threats exist.

Results

Real Cases of Healthcare Alarm Fatigue and Security Alert Fatigue

Bringing Healthcare Alarm Fatigue to the Forefront

> The case that brought alarm fatigue to the forefront occurred in a Boston hospital. A patient being treated for a head injury was on a cardiac monitor and pulse oximetry. Because he'd been restless, he was receiving an anti-anxiety drug. According to reports, alarms sounded indicating an increased heart rate and reduced oxygenation 1 hour before the nurse discovered he was unresponsive. (He eventually died.) An investigation found the alarm volume had been turned off.
>
> From The Official Journal of the American Nurses Association
> "Do you hear what I hear? Combating alarm fatigue"

When alarms are ignored in hospitals, people can die. And while the death of a patient is hardly comparable to what can happen to a business by ignoring alerts, the consequences can be devastating.

Real World Alert Fatigue: The Target Breach

Moving from the realm of theoretical to something more tangible, the following is a real illustration of how increased alerts, overburdened staff, and alert fatigue culminated in one of the most devastating security breaches in history.

A few days prior to Thanksgiving in 2013, someone installed malware in Target's (TGT) security and payments system. When Christmas gifts were scanned and bagged and a card was swiped the malware would step in, capturing the shopper's credit card number, and storing it on a Target server commandeered by the hackers.

Six months earlier, the company installed a $1.6 million malware detection tool made by FireEye. Target had a team of security specialists in Bangalore to monitor its computers around the clock. If the team in Bangalore noticed anything suspicious, they were to notify Target's Security Operations Center (SOC) in Minneapolis.

On Saturday, Nov. 30, the hackers set their traps and had just one thing to do before starting the attack: plan the data's escape route. As they uploaded exfiltration malware to move stolen credit card numbers—first to staging points spread around the U.S. to cover their tracks, then onto their computers in Russia—FireEye spotted them. Bangalore got an alert and notified the security team in Minneapolis.

And then.....nothing happened. Minneapolis didn't react to the sirens.

Pouring over the logs, Target found FireEye's alerts from Nov. 30 and more from Dec. 2, when hackers installed yet another version of the malware. The alarms, which went off before the attackers had started transmitting the stolen credit card data out of Target's network were early enough that if the alerts were investigated and resolved, the breach would have been contained.

Instead the theft engulfed Target, touching as many as one in three American consumers, and led to an international manhunt for the hackers.

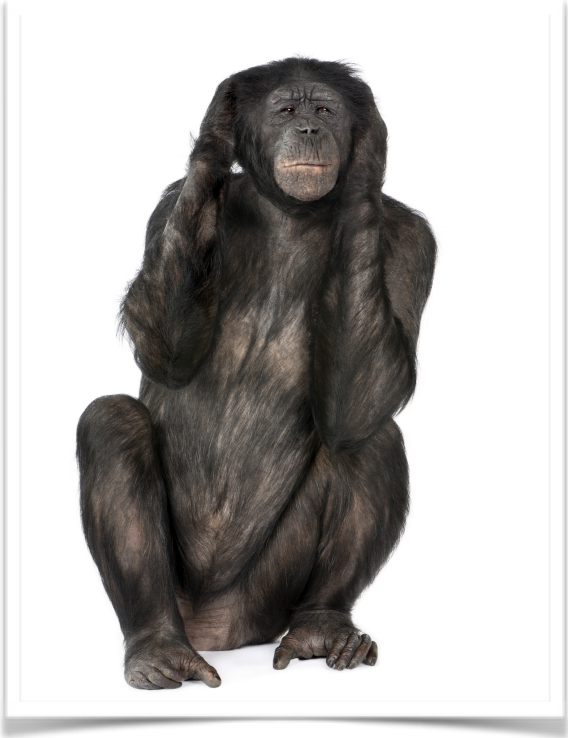
The breach compromised credit card numbers and other personal information of 40 million customers. Target racked up $61 million in expenses in the final months of 2013 because of the hack and the greatest risk it faces is the negative impact on its reputation and loss of confidence of its customers.

Two Approaches

When it comes to solving the alert fatigue problem, there are two approaches that organizations can take. While both can address the issue, one approach causes additional problems while the other is a comprehensive solution.

Approach One: Get Fewer Alerts

As stated earlier, if we just look at the problem in a vacuum we could say that the volume of alerts is the issue. If we just tune the detection systems so we see fewer alerts, people will respond appropriately and will not ignore the alarms when they go off. Fewer alerts lead to better response and less fatigue.



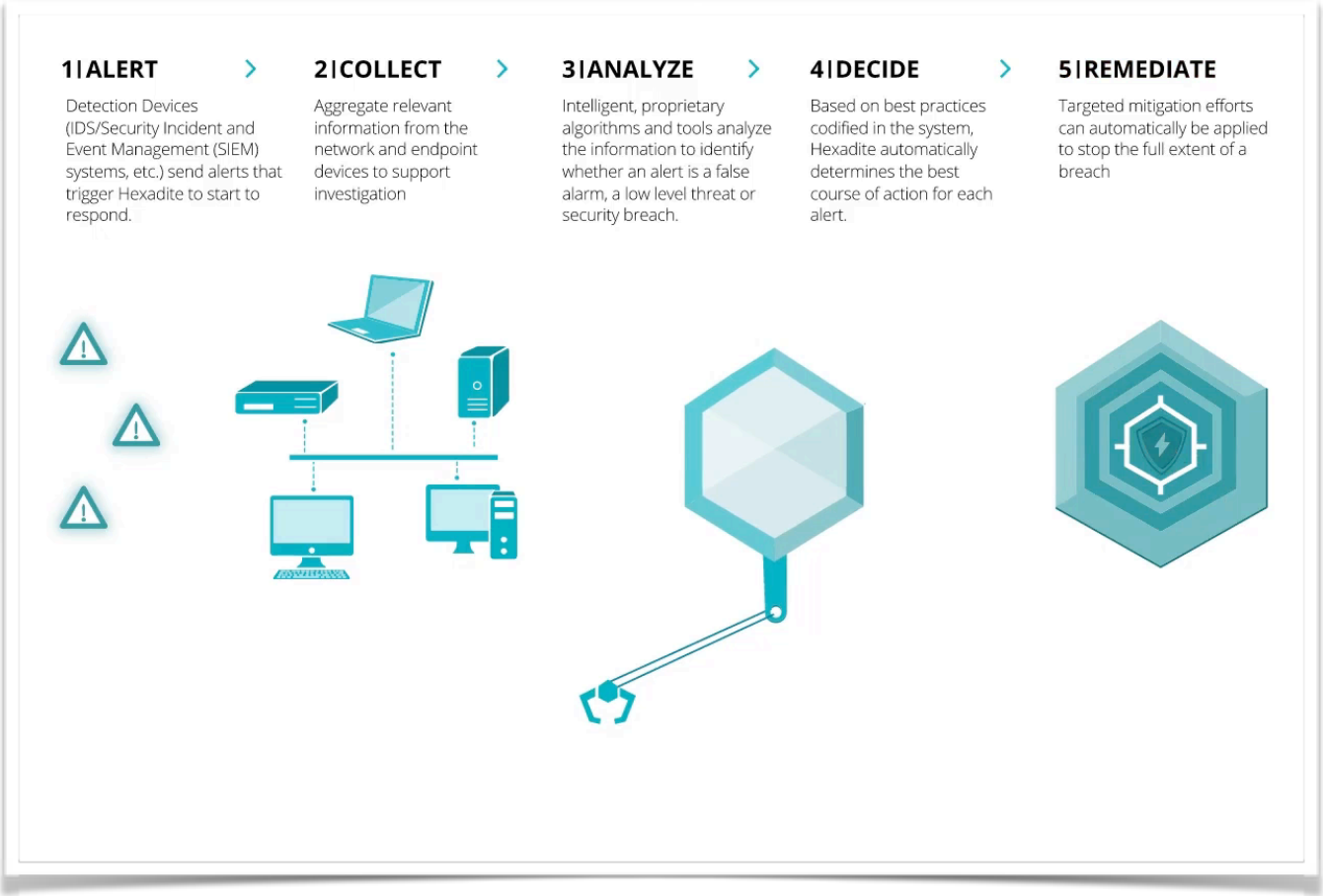
While factually correct, this approach ignores the larger issue: the problem isn't that there are too many alerts. The problem is that there are too many alerts for IR teams to reasonably respond to and investigate.

Ignoring alerts by tuning the system is a gamble. It assumes that because there is a high false positive rate, only showing high priority alerts will let responders focus only on what is important. Unfortunately, however, sometimes it is the incident behind the low fidelity alert that ends up being the way in for adversaries. Prioritization is compromise, and purposefully ignoring detected threats is what cyber criminals love to see.

Approach Two: Automatically Investigate Every Cyber Alert

Instead of ignoring alerts, another approach takes the opposite angle: if you automatically investigate every cyber alert from every detection system, you maximize the potential to mitigate any threat.

Security orchestration and automation solutions like Hexadite allow for a simple, yet comprehensive method to deal with the mismatch between alert volume and resources:

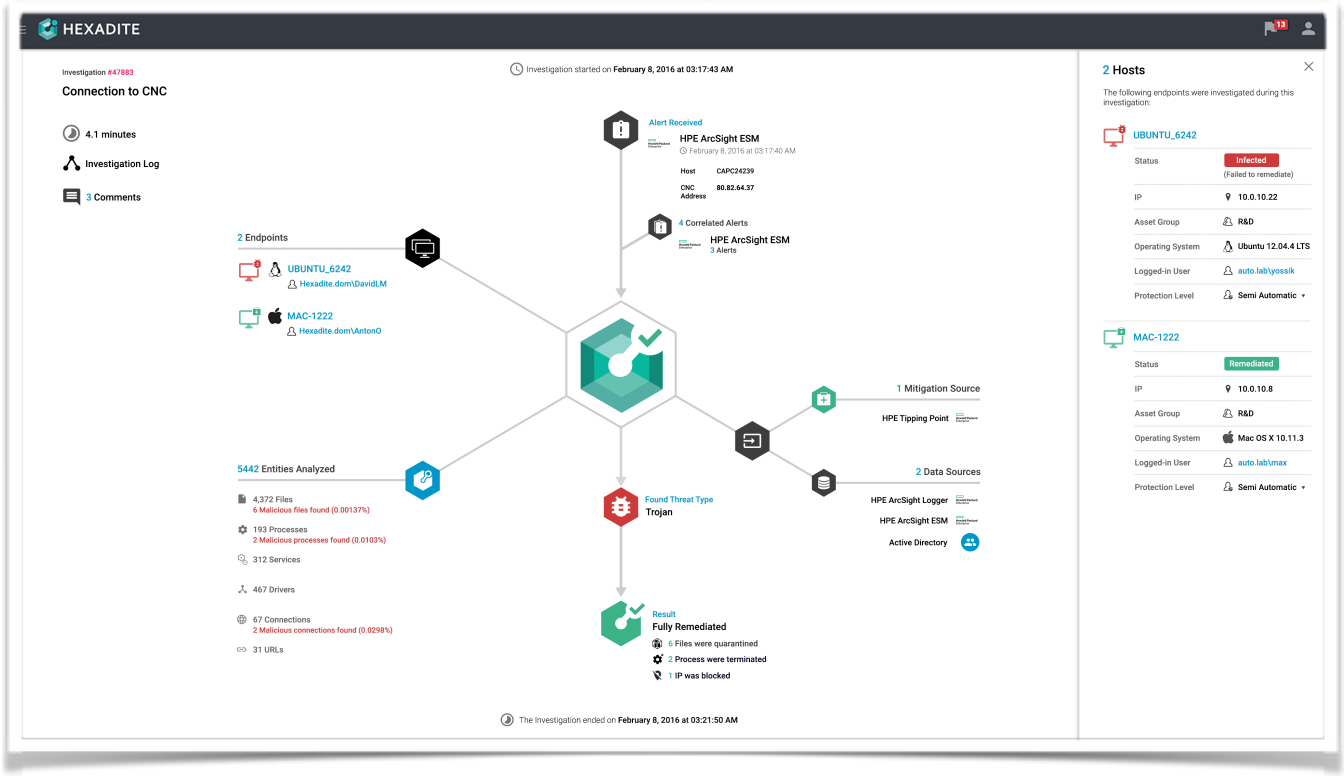


Automating the collection, analysis, decision, and remediation actions post-detection allows organizations to go from alert to remediation in minutes at scale.

HEXADITE
Intelligent Security Orchestration and Automation

About Hexadite

Hexadite is the only agentless intelligent security orchestration and automation platform for Global 2000 companies. By easily integrating with customers' existing security technologies and harnessing artificial intelligence that automatically investigates every cyber alert and drives remediation actions, Hexadite enables security teams to amplify their ability to mitigate cyber threats in real-time.



To request a demo or to learn more, please visit hexadite.com.

HEXADITE
Intelligent Security Orchestration and Automation