INTEZER

Improving SOC Efficiency in 2024

Transforming Security Operations Processes with Artificial Intelligence

By Ursula "Ushi" Heffernan,

HackerHaus Security, Co-Founder and Lead Security Engineer

HackerHaus Security Solutions, LLC

INTEZER

Table of Contents

INTEZER

About Ursula “Ushi” Heffernan

Co-Founder & Lead Security Engineer

Ushi is a seasoned professional with two decades of experience in incident response, security research, technical writing, and computer forensics. She has a proven track record in criminal investigations, insider threat detection, cybersecurity incident response, and mobile forensics. Ushi was trained in digital forensics by the US Secret Service and earned her Master’s degree from the University of Central Florida (go Knights!).

Ushi is committed to enhancing SOC efficiency and empowering small- and medium-sized businesses to fortify their defenses against the ever-evolving cyber threat landscape. Ushi has a forward-thinking approach, commitment to process improvement, team mentorship, and inclusive leadership that aims to ensure the highest standards in security services.

INTEZER

Foreword

As a SOC analyst who got her start in a large organization, I'm passionate about ensuring we have good working conditions for our organization's most important security asset. SOC is the first line of defense against cyber criminals. Good working conditions include having tools that allow them to complete their job efficiently without being overwhelmed and training to reduce significant knowledge gaps. The industry broadly considers a SOC analyst role an entry-level security role. While this publication does not seek to argue this one way or the other, it is crucial to understand that the more knowledge an analyst has, the better and more efficient they will be able to complete their investigations and ensure quick mitigation or escalation.

Alert fatigue is one of, if not the, biggest challenges facing incident first responders. Wading through an endless pool of phishing emails and low-priority alerts, trying to ensure every alert is given its due diligence while also trying to work quickly, knowing that when the "real" alert is found, this will take more time—time in which additional alerts (both false and true positive) will continue to pile up. As an industry, we have known for some time that this exists. I genuinely believe that Intezer has a product that can help automate much of the tier 1 investigation, freeing analysts to focus on the higher threat alerts.

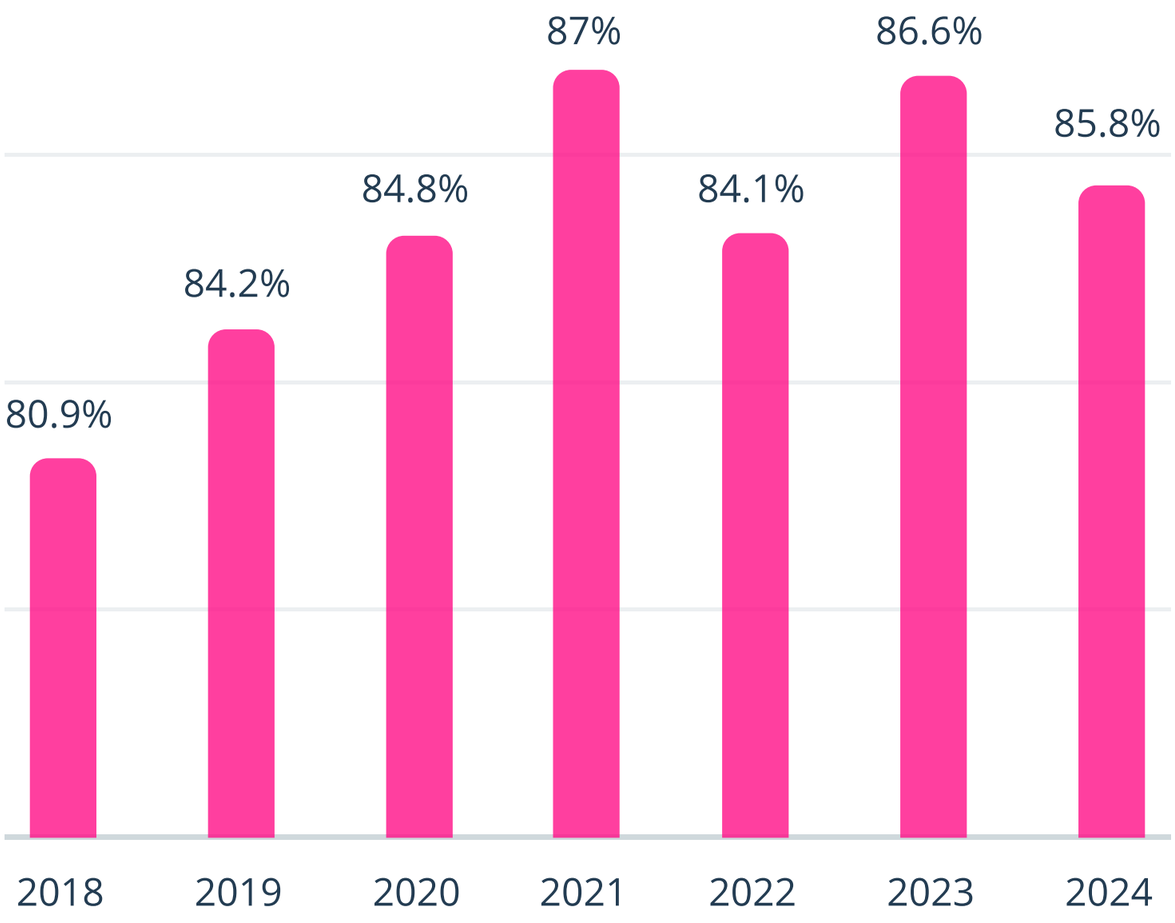
For organizations that either don't have a full-time SOC or outsource their incident response, using automated SOC tools can help decrease costs by allowing the processing of tier 1 functions prior to outsourcing legitimate incidents.

Intro

As the threat landscape of the world's data continues to grow and expand, the needs of our security methodologies must also grow and expand. The Security Operations Center (SOC) needs to be an integral part of this evolution. The SOC is the first line of defense, and the analysts are the first responders in security incidents. Their importance cannot be overstated. Cybercriminals continue to adapt and overcome detection and prevention methods. Therefore, incident responders must also continue to adapt their strategies to ensure the security of an organization's crown jewels, users/customers' private information, etc.

In a perfect world and perfect company, we would have as many analysts and funds to devote to security as we needed. In the absence of perfection, let's discuss the challenges facing our SOC analysts and how reconsidering some of the processes and policies in place could help save money while also ensuring continued effective security coverage.

Percentage of organizations experiencing a shortfall of skilled IT security personnel in at least one role



Source: 2024 Cyberthreat Defense Report, CyberEdge Group

As mentioned, staffing is one of the most significant challenges facing every SOC I've encountered. Putting together a team of competent individuals AND keeping the roles filled can seem nearly impossible. Much of the SOC revolving door issue can be attributed to the incredibly demanding work that incident response can require. Other problems include analysts outgrowing their roles and looking to do more advanced security work.

General SOC Roles/Responsibilities

Tier 1	Tier 2	Tier 3	Tier 4	Tier 5
Security Analyst	Security Analyst	Threat Hunter	SOC Manager	Security Architect
Monitors security systems and tools for potential incidents. Investigate and analyze alerts. Identifies and contains security threats. Escalates severe incidents to a tier 2 analyst.	Investigates and analyzes complex security incidents. Identifies and contains threats. Collaborates with tier 1 analysts to resolve incidents. May escalate severe incidents to tier 3 analysts.	Proactively searches for and identifies advanced threats, updates alert rules to ensure coverage for current and evolving threats. As an analyst, this may be the last line of escalation for complex incidents/ investigations. Often provides guidance and training to tier 1 and 2 analysts.	This individual tends to be more technical and oversees the training of analysts, may assist in leading responses to incidents, and communicates with the CISO and other stakeholders within the organization.	A security architect is a professional responsible for designing and implementing robust security solutions to protect an organization's systems, networks, and data. They assess potential risks, develop security frameworks, and collaborate with stakeholders to ensure comprehensive protection against cyber threats. Their expertise lies in creating resilient architectures that safeguard digital assets from vulnerabilities and attacks.

Each of these roles requires employees with unique cybersecurity and organizational knowledge. This limits the candidate pool. Additionally, there is a high turnover and burnout rate. According to Ponemon's 2021 SOC survey, many SOC employees describe their job as "painful," and analysts only stay in their position on average for 26 months with an organization. This is mainly due to the stress of continually being vigilant of breaches, the high stakes if one were to fail, and the ever-rising alert fatigue.

Another challenge that directly ties into staffing is time. I worked in a SOC of rockstars, but we always felt we needed more time and more people. But the reality is that even a SOC staffed to the max doesn't have enough time to go through all alerts and phishing emails submitted manually.

The world of automation within SOCs has come a long way with the introduction of SOAR (Security Orchestration, Automation, and Response) tools and platforms. SOAR allows for a centralized console for integrating and coordinating security tools, automating repetitive tasks, and reducing time to respond to incidents. This happens by ingesting alert data, which triggers playbooks that automate the response workflows or tasks.

However, like any tool, SOAR is only as good as its ability to be implemented efficiently, and even then, it's not a silver bullet for dealing with security challenges. Challenges include complexity, skill gaps, and false positives (FPs) and negatives (FNs). Additionally, there is a lack of time to fine-tune the rules and response action to minimize the issue of FPs and FNs, compliance, resource constraints, and adaptability to evolving threats. We'll discuss later considerations on how to decrease some of these SOAR challenges utilizing Intezer.

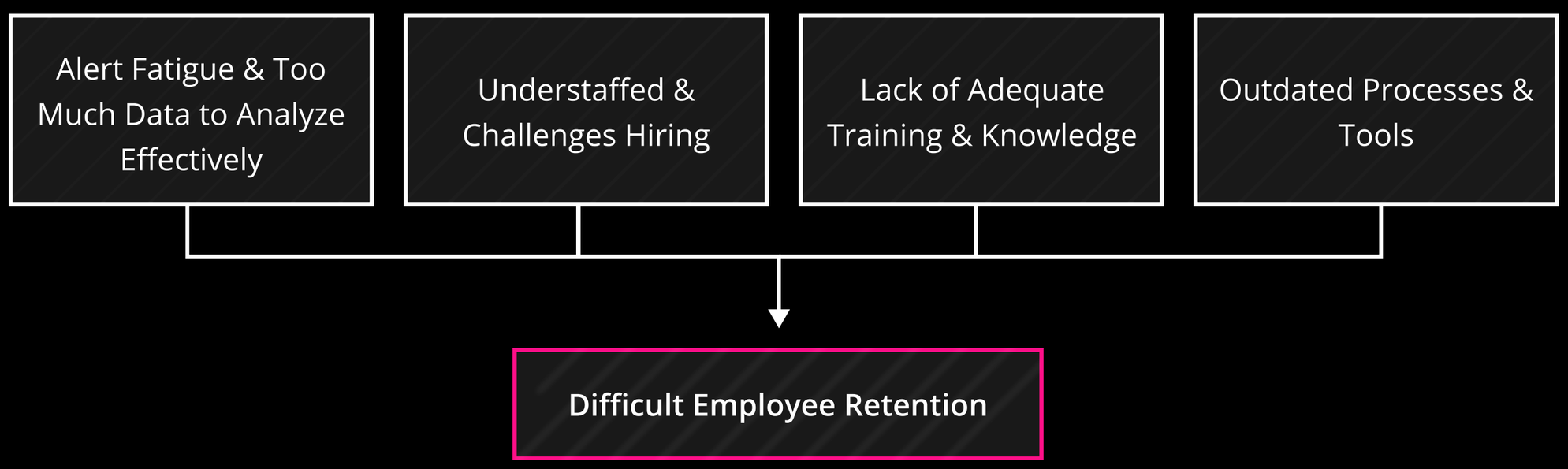
Major Challenges

As discussed, a top challenge for SOC analysts is **alert fatigue**. Every device connected to the network is a potential door for malicious activity and breach. For many security defenders, ensuring that every endpoint is being monitored can lead to a vast number of alerts. Each alert must be given due diligence as the alternative is data loss; where there's data loss, there is usually a corresponding monetary loss. This makes the day-to-day tasks critical. Add to that the sheer volume, pace required, and the stress of ensuring no missed positive incidents, and you have the perfect recipe for burnout and high turnover of analysts.

The **high turnover of analysts** can also account for the **operational knowledge** gaps and **poor or incomplete documentation**. This often leads to "tribal knowledge," which is undocumented information that has been acquired. However, due to the high turnover, and the fact that analysts are only staying for an average of 26 months in their current organization and role, not enough tribal knowledge is accumulated to overcome the lack of process documentation.

In addition, SOC analysts often **lack training**. However, they need to be able to increase their skills and keep up to date on the industry's leading threats. Without understanding the threat landscape and how adversaries are using different techniques and tools and are constantly evolving to mitigate their own exposure, analysts will be less effective in protecting the organization from data loss or compromise.

Average Tenure of a SOC Analyst



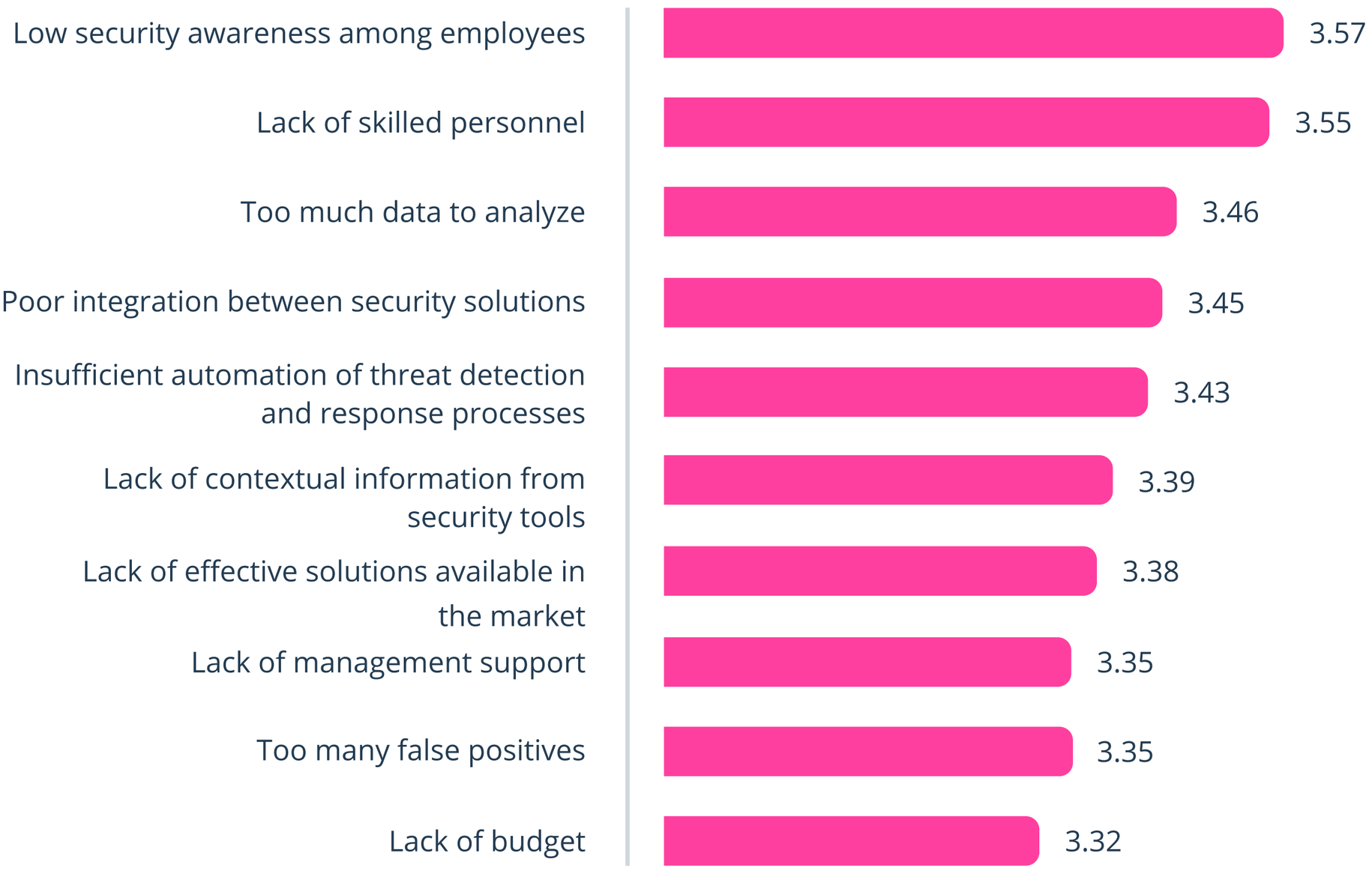
Another obstacle to ensuring properly trained analysts, training, resources, etc, is simply funding. Either the funding issue is that a small organization may not have the room in their budget, or both small and large organizations may not want to invest their budget in security because of the budget availability and the perception of a diminished ROI (Return of Investment).

We could spend chapters on all of the challenges SOC analysts face on a daily basis. However, the final one to be discussed is tools. Even large corporate SOCs are dealing with clunky, outdated, misconfigured, or highly complex tools. Oftentimes the SOC analysts have little training, understanding, or documentation on how to use these tools.

Additionally, many SOCs and security teams simply don't know how to properly set up tools, causing misconfigurations and holes in their security.

In addition to misconfigured and outdated tools, the issue of complexity is a large one. Whether it's SOAR, SIEM, or other security technologies, many of these tools are set up and managed by analysts who lack the training, experience, and understanding to properly configure these tools for efficiency. When a tool doesn't work properly, an investigation can suffer or even be missed due to no fault of the analyst.

Analysts must be given the proper tools and resources to do their job effectively. This also means the personnel to set up the tools properly and train the analysts on how to use them.



Source: 2024 Cyberthreat Defense Report, CyberEdge Group

INTEZER

Challenge Overview

What Plagues the SOC

It’s pretty easy to see that most of the challenges discussed all intertwine in some way. When challenges are not addressed, analysts will not be able to do their best work. Alert fatigue can lead to missed true alerts. Lack of documentation and training can lead to alerts that are not handled properly. Complex tools that are not set up properly or utilized to their fullest potential is simply bleeding money from an already tight security budget.

Addressing these challenges requires a combination of skilled personnel, technology, processes, and documentation. SOCs must continuously evolve to improve their capabilities and stay ahead of cyber threats so that they may most effectively protect their organization's assets.

INTEZER

Strategies to Improve Your SOC

We can achieve improvement in many ways.

5 Keys to Modernizing the SOC:

1

Engage Stakeholders

Engage with stakeholders in the security team as well as the greater organization. Stakeholders and budgetary decision-makers need to understand the effect that a lack of adequate security can have on the organization.

2

Ensure the Mission is Clear

Ensure that the security team as a whole understands which assets/data/etc. is most important to protect, and design security architecture, tools, and processes around that.

3

Work Alongside DevOps

So many SOCs expect their analysts to do all of the automation and tooling. Many times, analysts either don’t have the skills or the time or both to take away from chasing alerts so they can work on automation. Utilizing DevOps can provide a learning environment for the analysts to level up their skills, while also having an experienced DevOps professional to guide them.

4

Ensure Good Leadership

Leadership in a SOC is critical to the entire organization's security posture. A SOC manager should create incident response plans and ensure proper documentation or create that documentation themselves. They should have a very good pulse on what is going on in the SOC on a day-to-day basis. While they don’t need to micromanage, they should stop by regularly to ensure that analysts don’t need assistance and to understand the reality in which the analysts are working each day. Further, security leadership needs to have excellent communicators who can bridge the gap of understanding between not only the SOC analyst's work environment (and what improvements need to be made) as well as the security posture as a whole. Stakeholders and keepers of the budget should understand the state of security or lack thereof so they can make the best financial decisions for both security and the organization as a whole.

INTEZER

5 Automation

Automation, Automation, Automation! A look through any SOC analyst job description will likely have a section about contributing to the automation efforts/tooling the analysts use to help perform their jobs more efficiently. SOAR is a huge industry that lots of companies are throwing money towards. However, as previously discussed, there can be a ton of challenges with automating SOAR platforms. The majority of the issues reported by cybersecurity experts are a lack of understanding of how to properly set up and maintain their SOAR solutions. Additionally, the time it takes to set up playbooks has been identified as a pain point. However, properly implemented, SOAR is a powerful tool to leverage.

Supporting Analysts in the SOC

It can’t be stressed enough that when you give your analysts the environment, tools, and knowledge that they need to effectively do their job, they will be protecting assets and preventing security incidents that could cost the organization money, reputation, and customers.

Intezer has come up with some unique, artificial intelligence-led solutions that address the majority of the challenges outlined above. We are going to dive into what their platform does, and why I make that bold statement. But first, let’s have a quick recap lesson on Artificial Intelligence.

Artificial Intelligence

The Buzzword in the Room

If you have been in technology for even an hour, then the industry has likely cycled through 5 buzzwords already! While funny as a joke, buzzwords have become a way to show everyone that your product has some technology that everyone is talking about. Buzzwords are simply a way of life that generally comes out when a fairly new piece of technology that isn't completely understood is introduced to the market. It usually brings with it a lot of speculation, grandstanding, high claims, and expectations. Artificial Intelligence (AI) is one of the loudest buzzwords in the current market due to some new and popular large language models (LLMs), such as ChatGPT by OpenAI and Gemini by Google. But chatbots and assistants aren't the only branch of artificial intelligence, and it certainly isn't a new concept.

Artificial Intelligence (AI) is a branch of computer science that aims to create machines capable of performing tasks that would usually require human intelligence. AI is an interdisciplinary science with multiple approaches. Advancements in machine learning and deep learning, specifically, are creating a paradigm shift in practically every industry.

Key Branches of AI to Understand

Machine Learning (ML)	Neural Networks	Deep Learning (DL)
ML is a branch of AI and computer science that focuses on using data and algorithms to enable AI to imitate the way that humans learn. This allows machines to learn and improve performance over time without being explicitly programmed to do so.	Neural networks, also known as artificial neural networks (ANNs), are node layers containing an input layer, one or more hidden layers, and an output layer. Each node is connected to another and has a specified threshold value. If the output of any individual node is above the threshold value, the attached node is activated, and data is sent to the next layer of the network by that node.	DL is a sub-field of neural networks. The word "deep" in DL is referring to the number of layers in a neural network. Deep learning, like ML, is an AI algorithm. DL can ingest large amounts of unstructured data in raw form and can determine the features which distinguish data categories from one another.

Positive Outcomes for Security Teams from AI

Source: 2024 Cyberthreat Defense Report, CyberEdge Group

Getting Past the AI Hype to Streamline Processes

While the hype is still high, many security teams have existing products that already utilize AI and machine learning, or have recently launched new AI-based features using LLMs.

Security teams are also testing and evaluating new AI-based tools into their workflows, assessing their actual capabilities, ease of implementation, and potential for real ROI.

What is Intezer?

Intezer describes themselves as AI-powered, 24/7 alert triage and response. They aim to automate your Tier 1 SOC activities. Why an organization may want to automate these activities depends on the organization and will be discussed later. The key claims that Intezer makes are:

Monitor

Intezer automatically ingests alerts from your connected sources 24/7 and collects evidence

Investigate

Intezer investigates evidence related to each alert to determine a clear classification, assessment, and recommended next steps.

Triage

Intezer auto resolves false positives, escalating only the important incidents to your team with a complete analysis report.

Respond and Hunt

Intezer auto-remediates confirmed threats and provides ready-use rules for response and hunting.

Report

Intezer generates reports to provide tuning suggestions and give you full visibility over your security operations and alert pipelines.

More about Intezer's AI Technology

Intezer leverages proprietary artificial intelligence models, a variety of trusted techniques, and unique Genetic Code Analysis technology. For crafting the bottom-line incident triage assessments, Intezer uses machine learning and AI models that take into account the multiple analysis results for each individual evidence alongside information from the user's existing security tools.

You can read more in this blog post about Intezer's AI Framework.

Intezer's automated alert triage process starts by collecting all evidence associated with an alert (file, process, command line, IP, URL, memory image, etc.), deeply analyzes each artifact, and then builds an overall assessment for the incident with smart recommendations.

Read more about the five stages in Intezer's autonomous process in their blog post about how the Autonomous SOC platform works.

INTEZER

But Does It Really Do All That?

Y'all... I admit, I was super skeptical at first. How in the heck can you automate something like closing out alerts after a full investigation? And further, can it be trusted??

First and foremost, Intezer has given its users control over every step in the process. If you want to trial its decision-making before going full send, you can. While Intezer is capable of auto-closing alerts that it has determined are false, and including a detailed note as to the findings and determination, you can also simply not enable that feature until you feel comfortable. Since we shouldn't be pushing to prod on anything new anyway (we gotta get to know each other a bit first!), take her for a whirl. I think you'll probably agree with me that the analysis being made here is pretty impressive.

Intezer ingests alerts from pretty much wherever. You can connect your endpoint security product, your SIEM, your user-reported phishing pipeline, and your SOAR tools.

It uses AI (similar as described on the previous page) to classify each alert, and then pass it off to the next algorithm to determine which type of investigation it needs.

Once an alert is detected, Intezer then collects evidence and relevant data, **just as a human analyst would do.** They aim to gather as much evidence as possible to provide a complete understanding of the potential threat.

The evidence collected depends on what is needed. If there is a phishing email with a link to a credential harvester, then Intezer will use automated research tools to gain information about the link, IP info, owner info if available, screenshots, etc. If there is a file or a file-related incident, such as an executed file, Intezer will utilize your integrated security tools to carry out actions such as executing a remote memory scan, grabbing files, and analyzing them. Intezer is even capable of analyzing file-less attacks and reporting back.

Example Strategy for Autonomous SOC

1. Alert Monitoring

Files | Living -off-the land | Identity | Suspicious activity | Email

2. Evidence Collection

Files | URLs | memory images | process dumps | command | scripts | logs...

3. Investigation

Analysis
Sandboxing, AI, disassembly, unpacking static analysis, ...)

Correlation
Code similarities, behavior similarities, reputation checks, ...)

Verdict
Good/Bad, malware family, IOCs and behavioral rules)

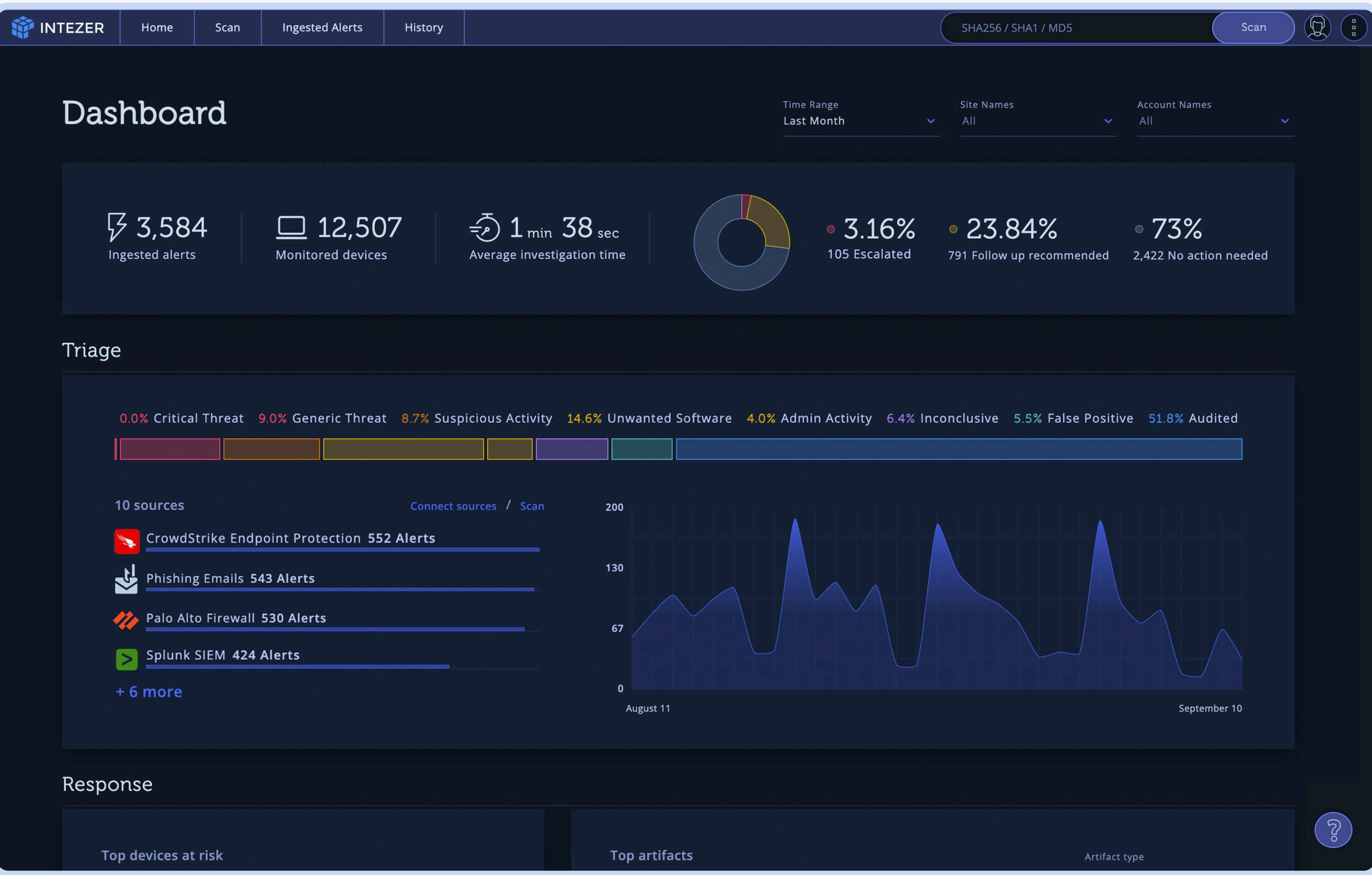
4. Decision Making

Combining original alert data with analysis of multiple evidence to compute the ideal triage assessment

- Determine false positive or true positive
- Classification and prioritization
- Escalate only serious incidents

5. Response

- Auto-resolve false positives
- Auto-apply IOCs and detection content
- Proactively hunt for similar threats
- Report with tuning recommendations



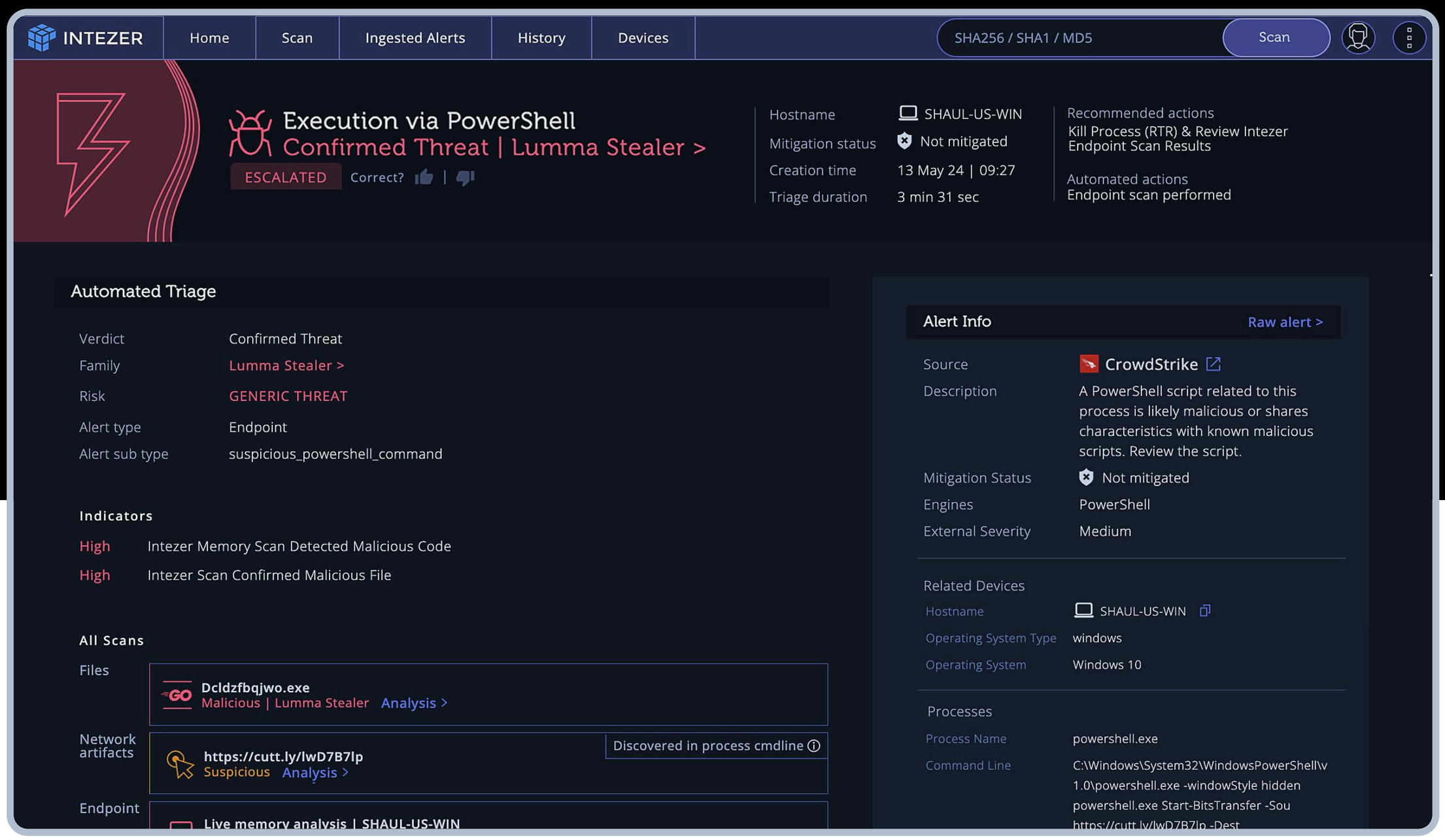
One of the most impressive alerts I've encountered so far is a malicious powershell command being run. Intezer gave back specific details about what the command does, why that's bad, and what steps to do next. But before we get ahead, let's discuss their process for investigations.

Each artifact is analyzed individually utilizing a combination of traditional techniques and AI. Intezer uses their own proprietary AI models and genetic analysis, along with sandboxing, static analysis, open-source intelligence (OSINT), memory analysis, and reverse engineering.

Intezer then takes all of the individual pieces that have been analyzed and use smart machine learning models and algorithms to put together a summary report pulling all of the information together to create an incident-wide verdict, risk level, and then recommended next steps.

In the image below you can see this Execution via PowerShell alert. The automated Triage shows that Intezer determined the threat to be confirmed, related to the malware family Lumma Stealer; it came from an endpoint, has a suspicious PowerShell command, and other information. The Alert info on the right shows the source information and description, related users and devices.

As you scroll further down you see the scans that were done, with links to more information about their analysis. Under that we can see more information about the analysis of the alert. I like that the analysis is not overly technical while also being technical enough for a tier 2 analyst to know exactly where they need to look. The findings are outlined to show each facet of the investigation in the way a human would have worked through the problem.



Finally, an analyst can follow their standard operating procedures for mitigation. If there are potentially multiple other endpoints, Intezer is able to conduct deeper automated memory forensics and triage accordingly.

I would be remiss if I didn't point out that triage/ investigation time in the image above. Under four minutes. Check out another alert, you'll see triage time happening seconds. The average triage time is less than 5 minutes.

This includes gathering the needed evidence. This is obviously an impossible task for any human analyst. This shows just how much time can be saved using automated triage.

SOAR tools also fit into this SOC automation picture. If you have a SOAR tool/platform that you want to integrate, you can utilize SOAR with Intezer to help streamline response and case management.

INTEZER

EXAMPLE CASE STUDIES

Let’s Operationalize It

The size of the organization will determine how Intezer’s SOC automation tool can best support your specific mission and needs.

Small to Medium-Sized Organizations

Many small to medium-sized organizations don't have the luxury of a budget that allows for a full-time security team, including a SOC. Many of these organizations utilize a range of different roles frankensteined together into a security team. This could be something as simple as the IT person responsible for the entire infrastructure of a large medical office or a small, few-person security team tasked with all security-related issues.

Inside a smaller organization, Intezer's SOC automation could be easily used to automate the basic tier 1 tasks and forward true alerts to the security person, team, or external response provider. This could also potentially save money for those smaller companies that want to save money on outsourcing their tier 1 SOC expenses.

Large Corporate Security Team & Managed Security Service Providers

In a corporate environment, there is often a team of tier 1 analysts and a team of tier 2 analysts. You may even be lucky enough to have the team doing both tier 1 and tier 2 tasks. While this means that alerts can pile up while analysts are working on investigations and cases, it also allows for continuity in the investigation.

In this example, Intezer can free up the analysts from the tier 1 tasks to work on mitigating true alerts. This helps reduce the time to mitigation, potentially preventing lateral movement, additional infected machines, or some other further stronghold.

Managed Security Services Provider (MSSP) organizations could benefit from this product like a large organization would. What's great is that you can ingest alerts from multiple sources and businesses. Freeing up your analysts to focus on investigating and mitigating your customers' true threats!

INTEZER

Conclusion

Building Trust in AI for SOC Teams

I have watched, on many occasions, alert after alert pile up while also watching the phishing inbox get overloaded, scanning the open alerts for the one I think is the highest priority, mentally triaging the things I can, and stressing about getting to all of the alerts. Worrying that the alert I didn't choose is the one that is making lateral movement right now. Asking myself all of the questions: Did I get all of the users that received that email? Did we block the email address? Have we seen it before? What does this command mean? Is there any attribution to a group or family? Did I remember everything in the report? The questions and stress are endless.

The security industry has given us some truly amazing and innovative tools. But the tools simply aren't enough. We need more intelligent and critical thinkers. Thankfully, computer science has given us artificial intelligence. As I mentioned before, the key concepts of AI are not new. Many of the tools I've reviewed in the past have utilized one component of AI, usually machine learning, or a combination ineffectively designed and/or implemented. Tools that require a long period of time to "learn" the users and environment to work effectively are risky and not helpful on day 1 out of the box.

Between not understanding what AI is, immature AI, and poorly implemented AI, it is not surprising that so many people are skeptical about claims of what AI can do when implemented correctly.

Intezer was founded by a former SOC and incident response leader who understands that analysts need tools that work and will allow them to do their best investigations. This platform is built for analysts by people who know what analysts need. Our analysts are BURNING OUT at an alarming rate. Tools must be implemented to decrease their challenges while allowing them to improve the efficacy of their investigations. Intezer's platform has been thoughtfully designed to address these challenging areas by utilizing AI, genetic analysis, and traditional DevOps concepts.

While I'm quite impressed with Intezer's implementation of AI to automate tier 1 SOCS services, I wouldn't just take my word for it. The list of long-time customers who have been using Intezer's platform since it was in beta and beyond speaks for itself. Companies such as Booz Allen, PepsiCo, Equifax, CheckPoint, and the list goes on.

Booz Allen · PEPSICO · EQUIFAX · CHECK POINT · legato security · MGM RESORTS INTERNATIONAL

INTEZER

References

Common Challenges of SOC Teams | RSI Security
https://blog.rsisecurity.com/common-challenges-of-soc-teams/

SANS 2023 SOC Survey | Splunk
https://www.splunk.com/en_us/pdfs/gated/analyst-report/sans-soc-survey.pdf

Cyberthreat Defense Report 2024 | CyberEdge Group
https://cyberedgegroup.com/cdr/

What is Artificial Intelligence (AI)? | IBM
https://www.ibm.com/topics/artificial-intelligence

What Is Machine Learning (ML)? | IBM
https://www.ibm.com/topics/machine-learning

How Intezer's AI-Powered Autonomous SOC Platform Works | Intezer
https://intezer.com/blog/incident-response/how-intezer-works/

Mastering SOC Automation in 2024: Tips, Trends and Tools | Intezer
https://intezer.com/blog/incident-response/soc-automation-in-2024-tips-trends-tools/

About Intezer

At Intezer, we believe security teams can use AI and automation to shift from feeling stretched thin to having every alert fully investigated and triaged, quickly and comprehensively.

Our mission is to empower SOC and incident response teams – accelerating, automating, and improving the tedious day-to-day tasks to help your people to stay ahead of relentless threat actors.

Behind Intezer's AI-powered platform is a dedicated team with deep experience in security operations, incident response, reverse engineering, malware analysis, and product development. With a focus on innovation and quality, we've designed the Autonomous SOC Platform to investigate incidents, make triage decisions, and escalate findings about serious threats like an expert tier 1 SOC analyst.

Without burnout, skill gaps, or alert fatigue.

See how Intezer works for yourself and try it for free:

Get a Demo >