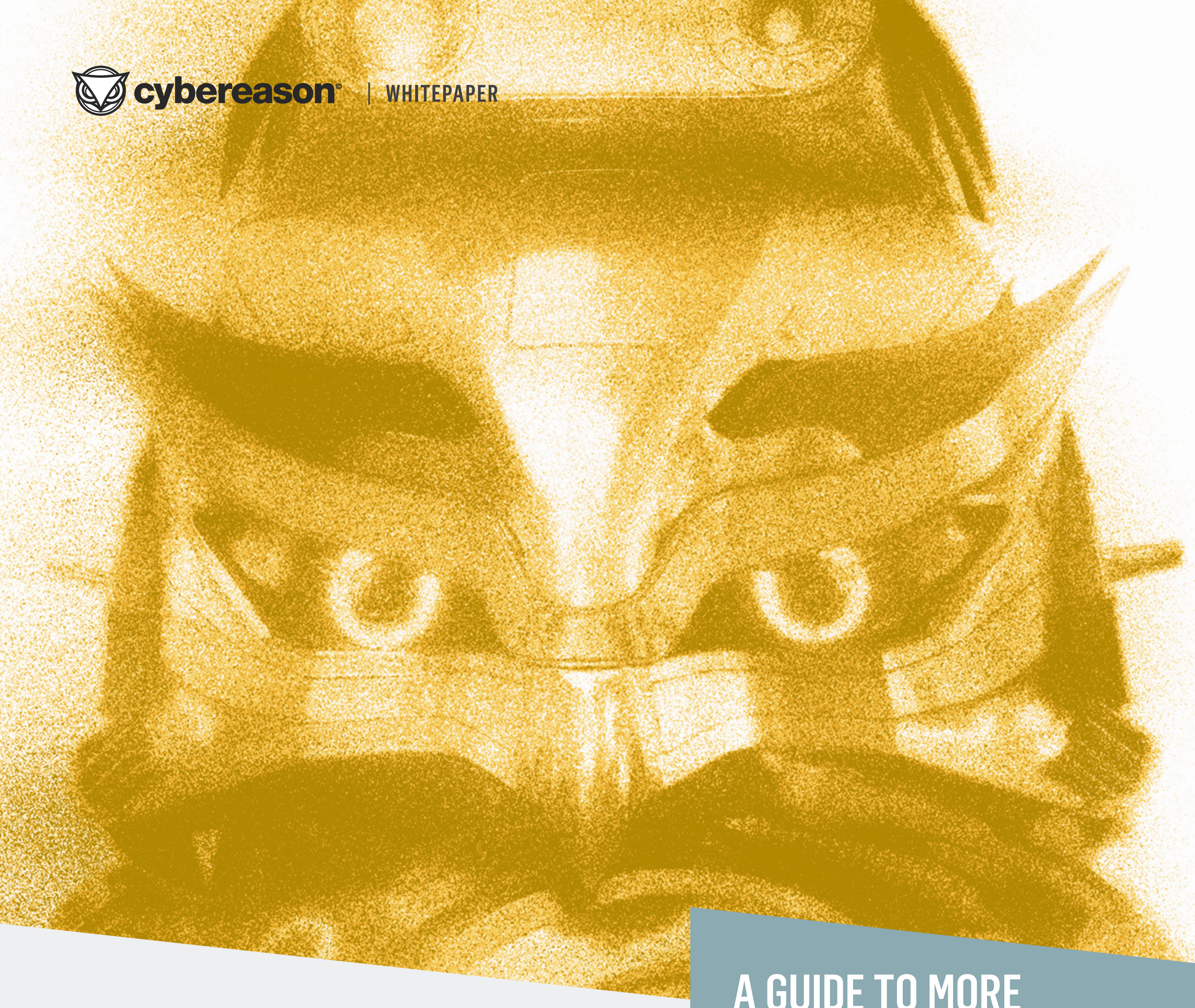
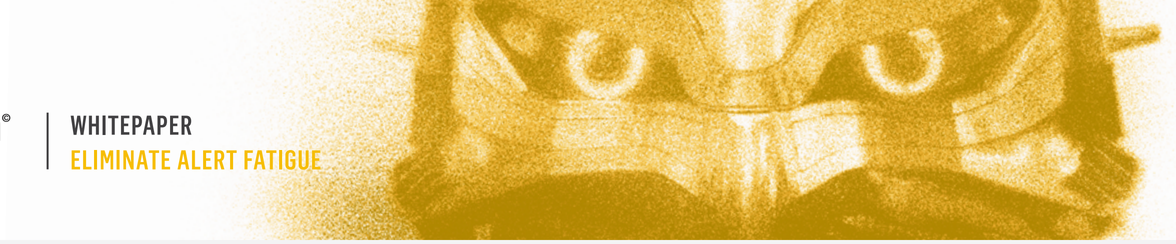
cybereason | WHITEPAPER



A GUIDE TO MORE EFFICIENT & EFFECTIVE SOC TEAMS

Eliminate Alert Fatigue



Introduction

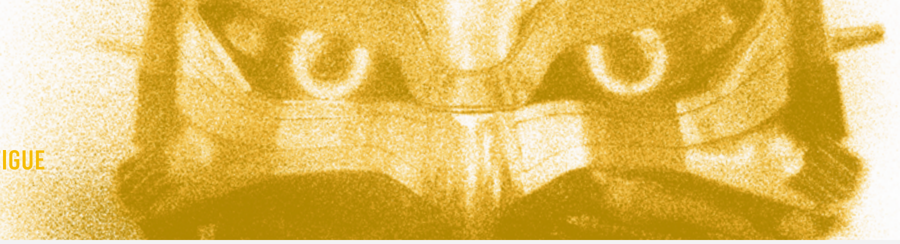
Alert fatigue is more than an annoyance for your security operations center (SOC) team, it is a real and present danger to your enterprise security. When analysts become overwhelmed by thousands of alerts per day, each of which must be triaged, investigated, and correlated, it becomes easy to spend critical time on false positives and miss actual indicators of an enterprise-wide data breach.

On average, SOC teams receive nearly 500 investigation-worthy endpoint security alerts per week, and the investigations that follow consume 65 percent of their time. Making matters worse, security teams are under-resourced, understaffed, and plagued by manual processes.

While these challenges can be frustrating for SOC team members and can lead to burnout and staff turnover, the real impact can be seen in an organization's overall security outcomes. Thirty-five percent of endpoint security alerts are simply not investigated because of the deluge of false positives. This also leads to investigation backlogs and low close rates for open investigations.

A different, operation-centric approach is needed to consolidate alerts, provide full visibility into an attack, and deliver unparalleled analyst efficiency.

of endpoint security alerts are simply not investigated because of the deluge of false positives.



2013 TARGET DATA BREACH

In December 2013, right in the middle of the holiday shopping season, cybercriminals executed a successful attack against Target, one of the largest retail companies in the United States. The attackers surreptitiously gained access to Target's computer network, stole the financial and personal information of as many as 110 million Target customers, and then removed this sensitive information from Target's network to a server in Eastern Europe.

The company's inability to detect the malicious activity wasn't for a want of resources. Target maintained a 300-strong security staff and operated two 24/7 SOCs, one in Minneapolis, Minnesota, and the other in Bangalore. Six months prior to the incident, the company had also deployed malware detection software from FireEye Inc.

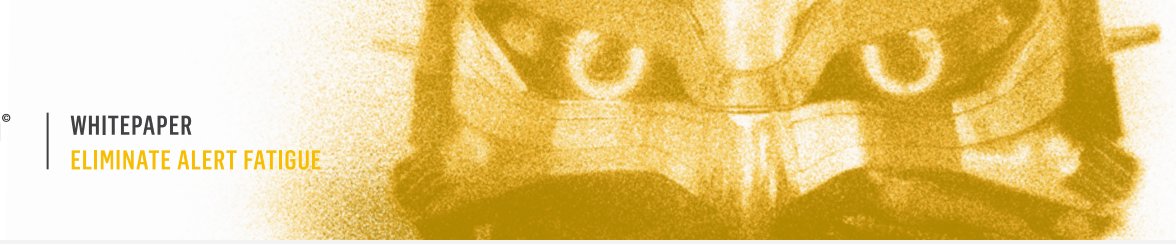
Target had given network access to a third-party vendor, a small Pennsylvania HVAC company. The vendor's weak security allowed the attackers to gain a foothold in Target's network. The attackers first installed their malware on a small number of point of sale (POS) terminals between November 15 and November 28, with the majority of Target's POS system infected by November 30. The company had no idea it had been hacked until the Department of Justice notified executives on December 12 that stolen data was appearing online.

Target's malware intrusion detection system triggered urgent alerts with each installation of the data exfiltration malware. However, Target's security team neither reacted to the alarms nor allowed the software to automatically delete the malware in question. Target's antivirus software also detected malicious behavior around November 28. According to a report by the Senate Committee on Commerce, Science and Transportation, "It is possible that Target staff could have viewed this alert as a false positive if the system was frequently alarming."

Despite multiple alerts and detections of well-known malware, the hackers were able to begin exfiltrating data on December 2 — a process that continued for nearly two weeks.

Target suffered almost irreparable damage to its brand, was forced to pay $300 million in settlements and legal fees, and the breach went down as one of the largest retail data breaches of all time — but they had multiple alerts that could have and should have stopped the attack before damage could be done.

> “Like any large company, each week at Target there are a vast number of technical events that take place and are logged. Through our investigation, we learned that after these criminals entered our network, a small amount of their activity was logged and surfaced to our team. That activity was evaluated and acted upon. Based on their interpretation and evaluation of that activity, the team determined that it did not warrant immediate follow-up.”
>
> MOLLY SNYDER,
> SPOKESWOMAN TARGET



ALERT FATIGUE & SOC PERFORMANCE: TWO PERSPECTIVES

A 2021 SOC Performance Report reveals a critical divergence of opinion between SOC leaders and analysts when it comes to SOC efficiency and effectiveness. When asked to rate how effective their SOC is on a 10-point scale, leaders scored it a 5 and staff a 3.9. The gap widens in response to the question of how effective their SOC is in its ability to gather evidence, investigate and find the source of threats, which earned a 5.5 from leaders and only a 3.3 from staff. Why such a disparity?

According to the report, SOC leaders tend to measure SOC performance based on avoidance of breaches and financial loss. SOC analysts, on the other hand, "tend to focus on how many events come across their screens that require some degree of action to determine which are innocuous and which require investigation and response."

Two areas where SOC leaders and staff find common agreement include lack of visibility into the attack surface and too many false positives.

As organizations grow and modernize their operations, their attack surface expands beyond the endpoint. To keep pace and stay secure, many organizations have simply added more security tools to defend more systems. According to a recent Security Response survey, organizations employed an average of 45 different security tools.

Ironically, this approach often has a negative impact on SOC efficiency and effectiveness. In fact, organizations using more than 50 tools ranked themselves 8% lower in their ability to detect an attack, and around 7% lower when it comes to responding to an attack.

TRUE CRIME PARALLEL

Criminals look for any opportunity to avoid being discovered. One of those options could be hiding in the noise.

Imagine a criminal collects hair trimmings from the trash can of dozens of hair salons and barber shops across the city, mixes those hair trimmings together, and then after committing a crime sprinkles those hair clippings all over the crime scene. The criminal would certainly have left DNA at the scene but could create a circumstance where forensics and DNA are useless in the investigation of that crime due to the sheer number of inputs. Hundreds, perhaps thousands of individuals would be within the dragnet of law enforcement investigators and create a circumstance where the adversary could hide amongst the noise.

The same applies to digital crime. Too many alerts mean adversaries can hide in the noise.

WHAT IS CREATING ALERT FATIGUE?

ALERT VOLUME

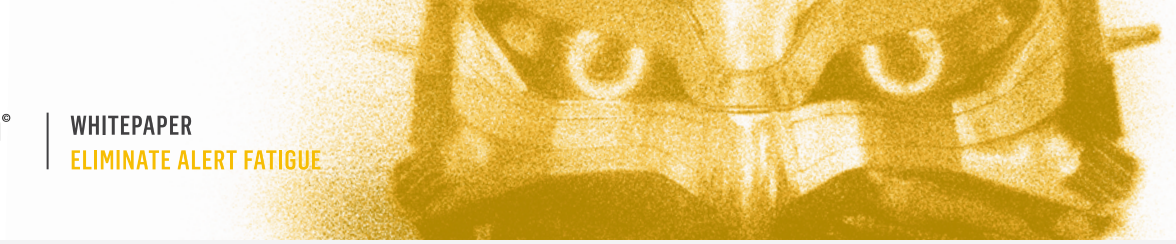
Information overload remains the primary contributor to the problem of alert fatigue. Security Information and Event Management (SIEM) platforms are set up by design to err on the side of too much visibility rather than miss an alert that later becomes critical and leads to a serious security event. This means that an oversensitive SIEM will issue an alert for anything even closely resembling suspicious activity, and security analysts are left to dig through the noise to find actual malicious activity.

TEAM SIZE

Security teams are notoriously understaffed. The most skilled Tier III analysts are extremely difficult to source, and even more of a challenge to retain. The cyber industry as a whole is dealing with a mass shortage of qualified staff, with negative employment and roughly 3.5 million unfilled cyber positions globally. Not surprisingly, information overload and the pressure analysts feel to ensure they detect malicious activity has led to burnout and high staff turnover. This workforce crisis impacts most SOC teams worldwide.

MANUAL PROCESSES

Investigating alerts the traditional way requires mostly manual processes. An unsettling scenario for a security analyst is when an alert comes across their desk but there isn't a straightforward indication that the detection is actually malicious. Unknown threats and zero days don't have the benefit of historical context, where they have been encountered before by other teams in other scenarios and added to threat intelligence databases. To confirm that a given threat is actually malicious, crossing the threshold from just merely suspicious, security analysts must investigate and parse behaviors manually to make a determination. A Tier I analyst often does some initial triage, and when an event warrants a deeper investigation, it is escalated to Tier II or Tier III for deeper analysis. But too many tools that generate too many alerts force analysts to work across silos. This only exacerbates the problem of alert fatigue.



ALERT FATIGUE CREATES UNACCEPTABLE OUTCOMES

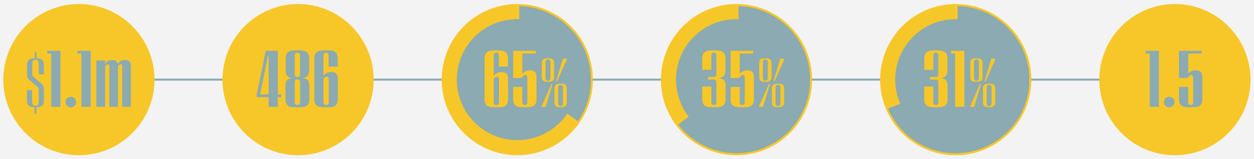
SLOWER RESPONSE AND LESS TIME FOCUSED ON OTHER MISSION-CRITICAL TASKS

TOO MANY DETECTIONS GO **UNINVESTIGATED**

MANUAL REVIEW AND ANALYSIS EXACERBATES ALERT FATIGUE

STAFF BURNOUT LEADS TO TURNOVER AND LACK OF EXPERIENCED TALENT

BY THE NUMBERS



U.S. Organizations with 2,500 or more employees spend, on average, $1.1 million annually on SOC payrolls

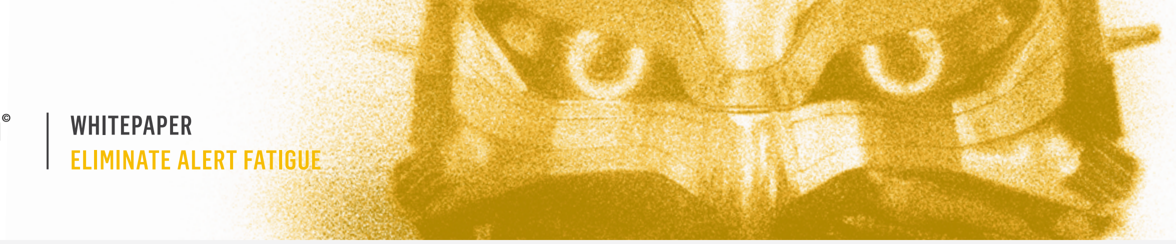
SOCs average 486 investigation-worthy endpoint security alerts each week

Investigations consume 65% of security analyst time

35% of endpoint security alerts are not investigated

31% of investigated endpoint security alerts are false positives

Each SOC member closes 1.5 security incidents daily



CYBEREASON IMPROVES EFFICACY & EFFICIENCY

Not all Endpoint Detection and Response (EDR) platforms are created equal. When it comes to efficacy, Cybereason is the most effective solution in the market today. Third-party testing like MITRE ATT&CK validates this claim, with Cybereason receiving the highest visibility scores in the history of the evaluation and consistent top performance in all other aspects of MITRE's evaluations.

Prevention testing determines a solution's ability to stop threats from executing before a foothold can be gained or damage can be inflicted. Stopping attacks early drastically reduces the number of alerts that the security team has to triage downstream, improving the team's ability to uncover sophisticated threats and reducing burnout.

in real-time. Finally, using artificial intelligence and machine learning, Cybereason builds a comprehensive picture of the attack story, detecting threats in real-time as they are happening.

When Cybereason detects malicious activity and presents that detection to an analyst, it's a high-fidelity alert. Analysts are only brought into the triage, investigation, and response workflows when a verified alert is active in an environment. This creates massive savings in investigation time by avoiding repeat issues and only fielding true positive detections that warrant human eyes on a screen.

Cybereason's primary differentiator is the ability to consolidate alerts into a single malicious operation — what Cybereason calls a MalOp^{tm}. Whereas other vendors alert dozens of times for a single intrusion, **the Cybereason MalOp Detection Engine stitches together the separate components of an attack**, including all users, devices, identities, and network connections **into a comprehensive, contextualized attack story.**

Cybereason is the only vendor to leverage a unique combination of multi-layered defense and Predictive Ransomware Protection to achieve predictive response. These prevention capabilities help security professionals stay one step ahead of the attacker at every move and prevent attacks before they start. The more threats that are prevented at the onset without manual analyst intervention means more bandwidth for security teams is preserved for detection and investigation of more complex issues.

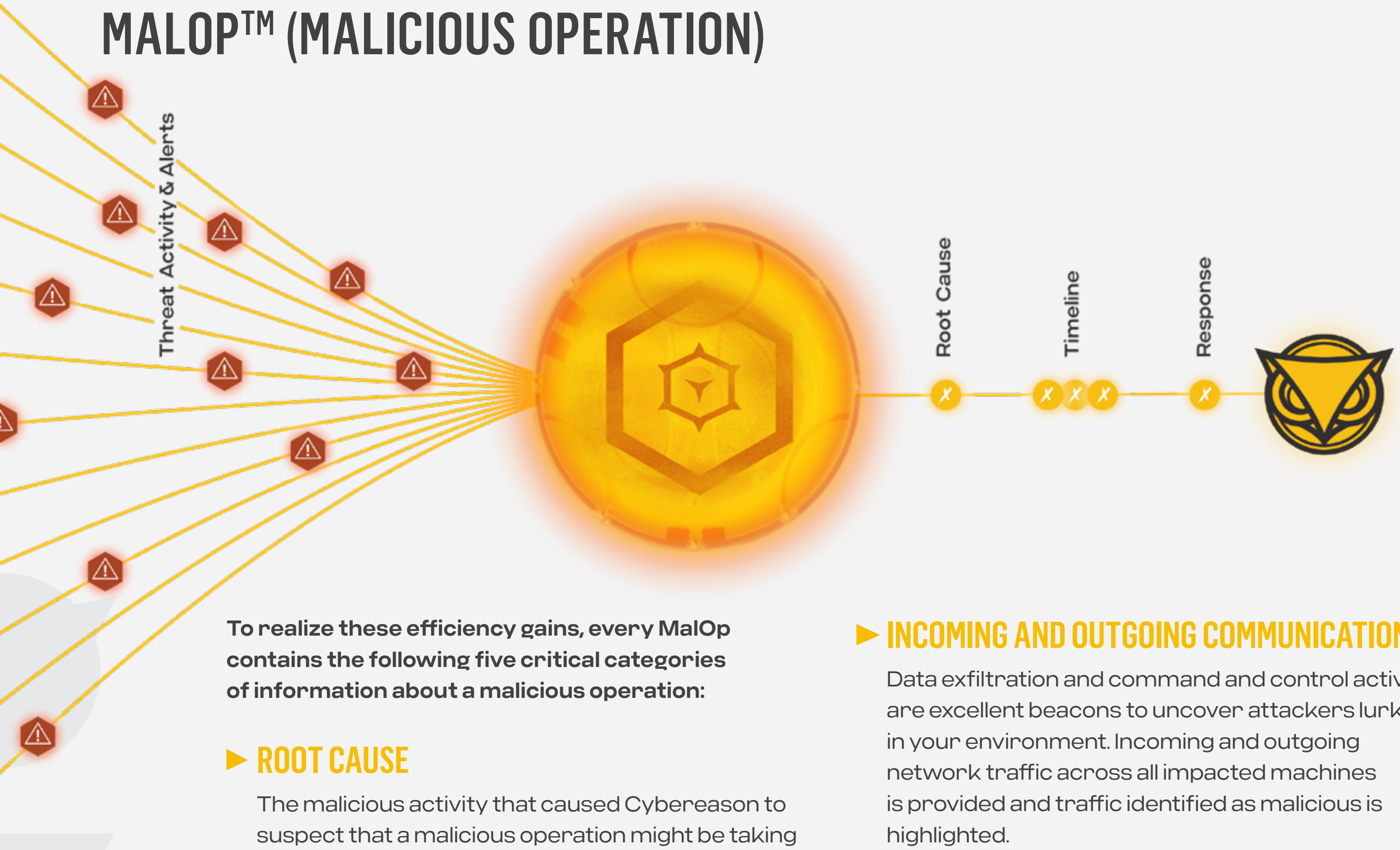
Solutions that are highly effective against today's threats—especially sophisticated threats like ransomware—must be able to detect malicious activity immediately without waiting for additional processing time or human analyst intervention.

Cybereason delivers 100% real-time detection by leveraging all of your data. While other solutions filter valuable event data, Cybereason uses more than 30 sources of telemetry to correlate all relevant data.

Cybereason's primary differentiator is the ability to consolidate alerts into a single malicious operation — what Cybereason calls a MalOp^{tm}. Whereas other vendors alert dozens of times for a single intrusion, the Cybereason MalOp Detection Engine stitches together the separate components of an attack, including all users, devices, identities, and network connections into a comprehensive, contextualized attack story. Because the Cybereason Defense Platform understands the full attack story, we orchestrate and automate response to all impacted endpoints and users through tailored response playbooks without the need for an outside SOAR solution.

This advanced and automatic analysis increases analyst speed and accuracy by reducing the noise of alerts with a focused deconstruction of the overall operation. With all the information an analyst needs to scope and respond to a malicious operation concisely presented, analysts are able to drastically reduce their Mean Time to Respond (MTTR).

MALOP™ (MALICIOUS OPERATION)



To realize these efficiency gains, every MalOp contains the following five critical categories of information about a malicious operation:

► ROOT CAUSE

The malicious activity that caused Cybereason to suspect that a malicious operation might be taking place. Whether through a well-crafted spear-phishing email or another entry vector, cyber adversaries must first establish a foothold in the environment to build on and escalate the intrusion. The root cause (along with any other suspicious behavior and ultimately evidence) is always mapped to the MITRE ATT&CK framework. For example, a common root cause observed by Cybereason technology is the use of domain generation algorithms.

► IMPACTED USERS AND MACHINES

Today's attackers almost never focus their malicious operation on a single user or machine. Although a specific user or asset might be the ultimate target, multiple systems will be leveraged along the path to their objective. All of the users and machines that are part of this larger operation are correlated into this single, full-scope view.

► INCOMING AND OUTGOING COMMUNICATIONS

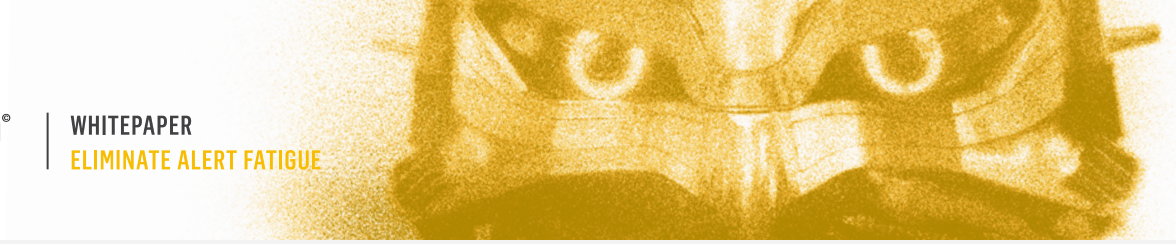
Data exfiltration and command and control activity are excellent beacons to uncover attackers lurking in your environment. Incoming and outgoing network traffic across all impacted machines is provided and traffic identified as malicious is highlighted.

► TOOLS THE ATTACKERS USED

What is the attacker using to execute their malicious code and traverse the environment? Metasploit Meterpreter? Or perhaps they are stealthy and leveraging components built into the operating system to avoid detection—commonly called Living Off The Land (LOL). Cybereason users see a lot of signed Microsoft Windows binaries being abused such as regsvr32.exe.

► TIMELINE OF THE ATTACK

Automatically analyzing the activity across the vast environment and presenting the full timeline of the attack in a straightforward and visual way saves your SOC analysts untold amounts of time. Gone are the painful hours of examining alert time stamps to try and determine what happened, and when, during a malicious operation.



The key to getting ahead of the alert fatigue crisis is to automate as many of the mundane and repetitive tasks as possible. Because the MalOp understands the full narrative of the attack, Cybereason populates tailored response playbooks to all impacted endpoints and users, and the remediation of the full operation takes place with a single click. Cybereason is careful to not over-automate, as human intervention will always be needed in the response process.

FROM-THE-FIELD SUCCESS STORY

Multinational Financial Services Firm	
CYBEREASON	CROWDSTRIKE
27,000+ endpoints	**27,000+** endpoints
721 consolidated alerts (MalOps) generated	**12,930** alerts generated

18x

Cybereason was 18x more precise than Crowdstrike

5x

Cybereason delivered a 5x detection rate over Crowdstrike

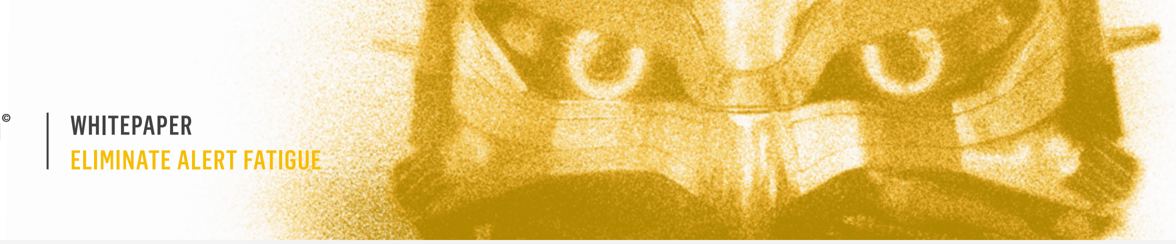
200,000

Cybereason enables 1 analyst to cover up to 200,000 endpoints

CYBEREASON CREATES BETTER SECURITY OUTCOMES

Moving from an alert-centric security model to an operation-centric model significantly improves SOC team operational effectiveness and efficiency. Small teams can do the work of larger teams, less experienced teams are immediately more effective, and your SOC's ability to mitigate risk improves exponentially.

When a team has more bandwidth, this creates extra cycles. An operation-centric approach means that the additional bandwidth created can be used on projects that were out of reach before (like threat hunting), and teams can finally get ahead of the curve.



What sets the Cybereason Defense Platform apart from other cybersecurity tools?

▶ COMPLETE DATA COLLECTION

Detection of the most advanced and elusive attackers requires exhaustive and correlated data collection from the endpoint. Our platform processes 80 million events per second leaving adversaries nowhere to hide.

▶ INDICATORS OF BEHAVIOR (IOBS)

Traditional Indicators of Compromise (IOCs) and signatures are useful for catching known malware. To stop even the most sophisticated attacks and catch never-before-seen malware Cybereason leverages Indicators of Behavior, the more subtle chains of behavior that can surface an attack earlier and more reliably.

▶ AUTOMATED RESPONSE

Analysts can take remote remediation actions including machine isolation, killing processes, and opening remote shells, all from within an intuitive point-and-click interface—stopping attackers in their tracks.

▶ RANSOMWARE PREVENTION AND DECEPTION

Cybereason uses a combination of behavioral detections and proprietary deception techniques to surface the most complex ransomware threats and end the attack before any critical data can be encrypted.

▶ FUTURE-READY

The flexibility of our product and the new innovations being added every day, make Cybereason future-ready for wherever the fight takes us.

Defenders can take on more of the attack surface and mature their strategy to include XDR. Cybereason XDR creates a single point of visibility, detection, and response across the breadth of the enterprise, and our prowess and expertise on the endpoint create the foundation for extensible XDR that incorporates all of the necessary data sources.

AI-driven XDR from Cybereason is the only XDR platform capable of gathering telemetry across the planetary attack surface and delivering 10X performance improvements for defenders. AI-driven XDR from Cybereason breaks down the data silos that attackers rely on to remain undetected by unifying device and identity correlations for 10X faster and 10X more effective threat detection and response while unlocking new powers of prediction that enable defenders to anticipate and end future attacks before they begin.

Only Cybereason customers have the capacity to take on the additional attack surface and move to a position of XDR, having first tackled the fundamentals of operation-centric EDR.

Cybereason is dedicated to teaming with defenders to end attacks on the endpoint, across the enterprise, to everywhere the battle is taking place.

Learn more about Cybereason here or schedule a demo today to learn how your organization can benefit from an operation-centric approach to security for increased efficiency and efficacy.

ABOUT CYBEREASON

Cybereason is the champion for today's cyber defenders with future-ready attack protection that extends from the endpoint to the enterprise, to everywhere. While every other security solution is alert-centric, Cybereason is operation-centric. We empower defenders to instantly visualize MalOps from root cause to every affected endpoint with real-time, multi-stage displays of all attack details. This gives you the power to end attacks with a single click.

Learn more at cybereason.com/why-cybereason.