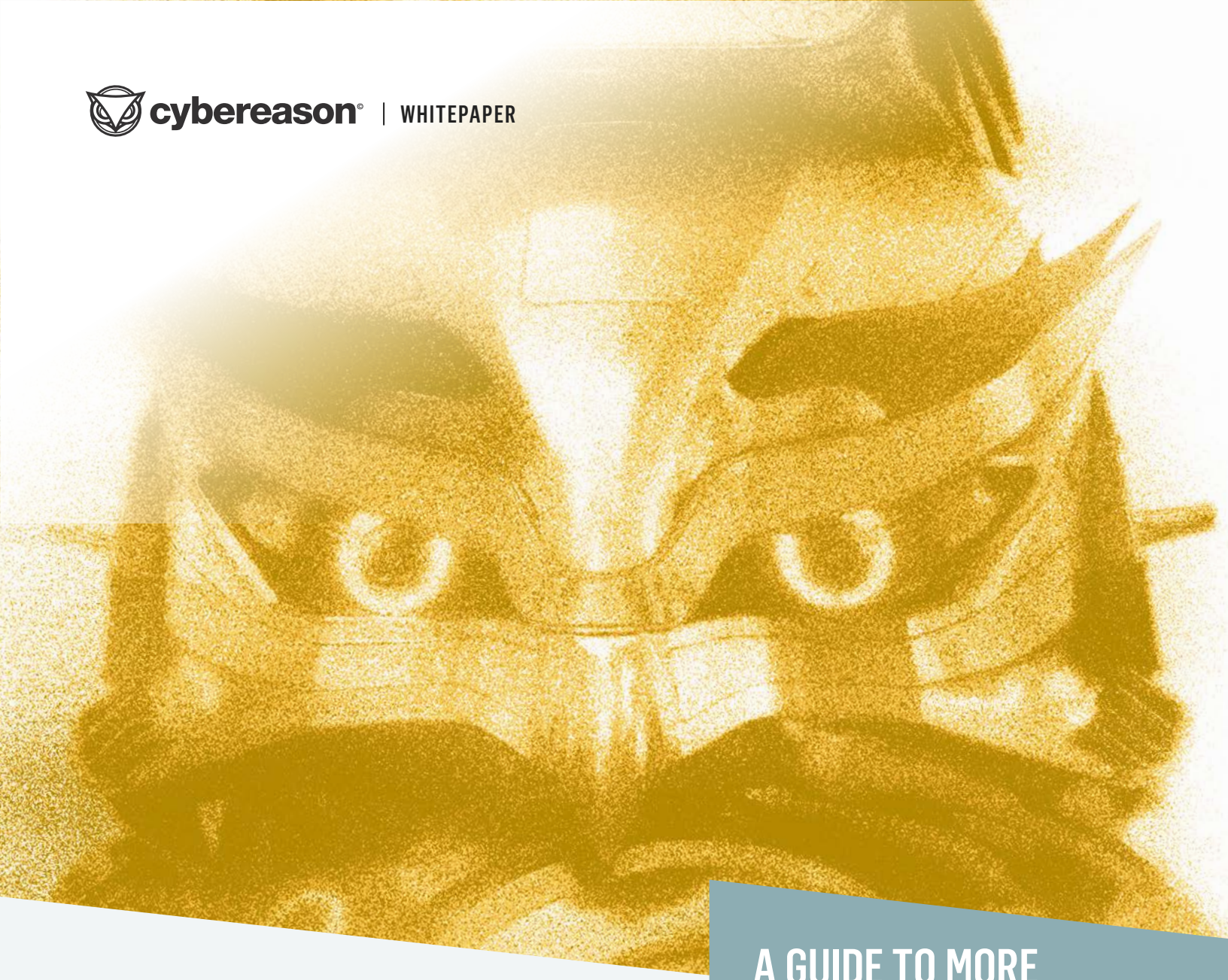
cybereason | WHITEPAPER



A GUIDE TO MORE EFFICIENT & EFFECTIVE SOC TEAMS

Eliminate Alert Fatigue

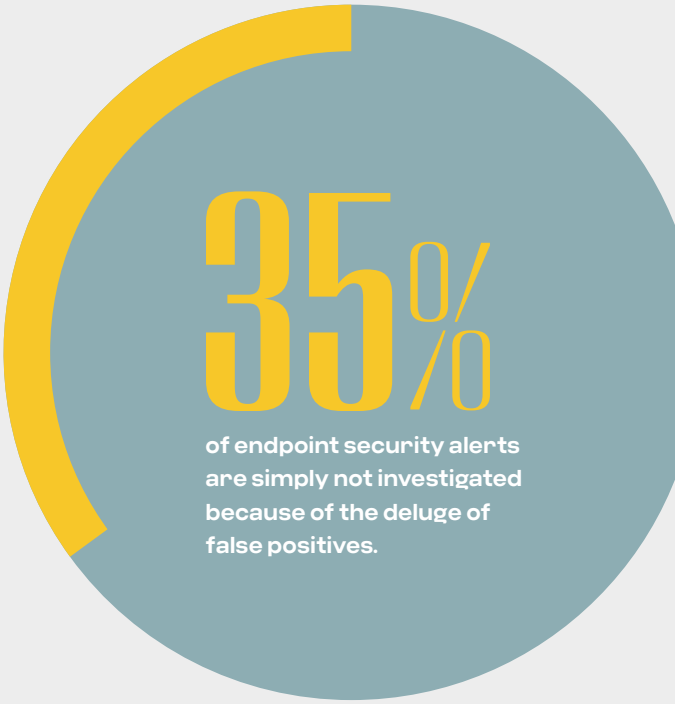
Introduction

Alert fatigue is more than an annoyance for your Security Operations Center (SOC) team, it's 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 the true 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% of their time. Making matters worse, security teams are under-resourced, understaffed, and plagued by manual processes.

These challenges are frustrating for SOC team members and can lead to stress, burnout and staff turnover, but the real impact is on the organization's overall security outcomes.

An operation-centric approach is needed to correlate alerts, identify the root cause, provide full visibility into an attack timeline, and at the same time automate as much of this work to deliver unparalleled analyst efficiency.



WHAT CREATES ALERT FATIGUE?

ALERT VOLUME

Information overload is the primary cause of alert fatigue. Security Information and Event Management (SIEM) platforms are designed to err on the side of too much visibility rather than miss an alert that later leads to a serious security event. An oversensitive SIEM will issue an alert for anything even closely resembling suspicious activity, leaving security analysts 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. Unsurprisingly, information overload and the pressure to detect malicious activity lead to burnout and high staff turnover.

MANUAL PROCESSES

An unsettling scenario for a security analyst is when they receive an alert without a straightforward indication of whether the detection is actually malicious. They must investigate and parse behaviors manually to find out. 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

- ANALYSTS HAVE LESS TIME TO FOCUS ON OTHER STRATEGIC OR MISSION-CRITICAL ACTIVITIES.
- TOO MANY DETECTIONS GO UNINVESTIGATED, MEANING ATTACKERS ARE UNDETECTED FOR LONGER, INCREASING THE DAMAGE INFLICTED.
- MANUAL REVIEW AND ANALYSIS MEAN SLOWER RESPONSE AND REMEDIATION TIMES.
- STAFF BURNOUT LEADS TO TURNOVER WHICH IS FURTHER COMPOUNDED BY A SHORTAGE OF EXPERIENCED TALENT.

INTRODUCING THE MALOP™ (MALICIOUS OPERATION) FROM CYBEREASON

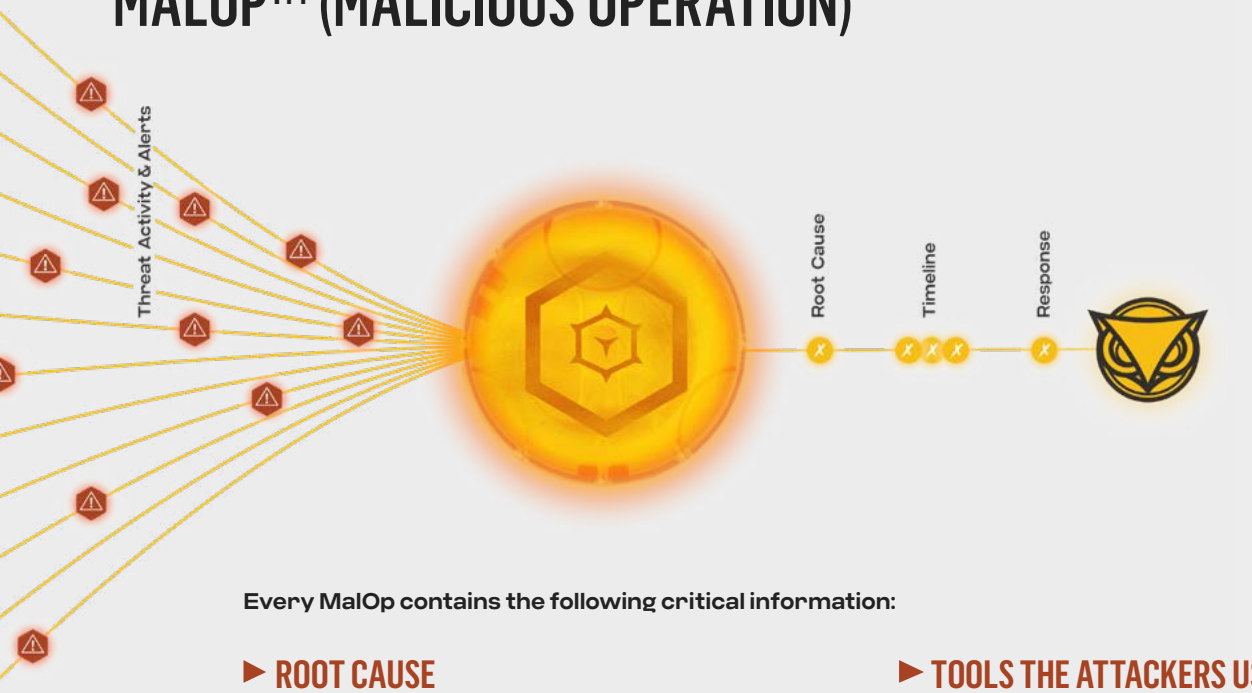
The Cybereason MalOp™, short for Malicious Operation Detection, is the realization of our operation-centric approach. In the background, the Cybereason Defense Platform uses AI-Powered analytics to automate the triage and investigation process across all impacted devices to present the complete, end-to-end picture of an attack rather than overwhelming analysts with piecemeal alerts.

Most security teams can relate to alert fatigue, and it's not uncommon for large enterprises to deal with alerts in extremely large and unmanageable quantities—up to tens of thousands per day.

These alerts are often reported individually and without a broader connection to related malicious activities. This is a scattered and chaotic approach with defenders becoming aware of a singular issue through multiple alert streams.

As an alternative approach to traditional alerts, the MalOp provides a contextualized view of the full narrative of an attack, correlated across all impacted endpoints, in a single screen. For security analysts, this transforms their approach from reacting to incidents from an alert-centric view to responding with an operation-centric view.

MALOP™ (MALICIOUS OPERATION)



Every MalOp contains the following critical information:

ROOT CAUSE

The malicious activity that caused Cybereason to suspect that a malicious operation might be taking place. The root cause is always mapped to the MITRE ATT&CK framework.

IMPACTED USERS AND MACHINES

Although a specific user or asset might be the ultimate target, attackers might leverage multiple systems along the path to their objective. All the users and machines involved 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 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

Moving from an alert-centric security model to an operation-centric model significantly improves SOC team operational effectiveness and efficiency.

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 one analyst to cover up to 200,000 endpoints.

WHAT SETS CYBEREASON APART?

Cybereason doesn't stop there. With Cybereason Managed XDR (Extended Detection and Response), defenders can extend their operation-centric approach beyond the endpoint to apply AI-driven analytics across telemetry from workspace, cloud, identity & access, and network areas of the IT Infrastructure to extend MalOp detections and deliver 10X performance improvements across the broader SOC remit.

It 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. This unlocks new powers of prediction that enable defenders to anticipate and end attacks before they begin.

Only Cybereason customers can take on the additional attack surface and move to a position of XDR, having first tackled the fundamentals of operation-centric EDR (Endpoint Detection & Response).

When Cybereason detects malicious activity and presents that detection to an analyst, it's a high-fidelity alert. Because the platform understands the full attack story, we orchestrate and automate your response to all impacted endpoints and users through tailored response playbooks, without the need for an outside SOAR solution.

HERE'S WHAT MAKES CYBEREASON UNIQUE:

- We are the only vendor to leverage a unique combination of multi-layered defense and Predictive Ransomware Protection to achieve a predictive response.
- We deliver 100% real-time detection by using more than 30 sources of telemetry to correlate all relevant data.
- Using artificial intelligence and machine learning, we build a comprehensive picture of the attack story, detecting threats as they happen.

When it comes to efficacy, Cybereason is one of the most effective solutions in the market, enabling analysts to drastically reduce their Mean Time to Respond (MTTR). Third-party testing from MITRE ATT&CK validates this claim, with Cybereason receiving excellent results.

LEARN MORE

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.**