exabeam

Solution Brief

External Threats: Dealing with Ransomware, Phishing Attacks, and Malware

Overview

Cyber threats are getting more sophisticated as more companies migrate to the cloud and remote work becomes a staple of a modern business. The changing dynamics of security threats and business processes have led to a fourfold increase in cybersecurity complaints and global losses from cybercrime exceeding $1 trillion in 2020.

Security operations teams not only manage internal threats but contend with software and security vulnerabilities that can expose intellectual property and financial data to external entities. Ransomware, social engineering, DDoS attacks, and phishing attacks are all common external threats most SOC teams have to contend with.

Changing dynamics of external threats

Cyberattacks are easier to implement than ever before; you can download the code for a ransomware attack on GitHub. Phishing attacks are another excellent example — hackers (bad actors) use fake email messages to obtain personal information, banking, or corporate credentials, while stealing important data or distributing malware, delivering additional vulnerabilities.

According to Verizon's 2020 Data Breach Investigations Report, 45% of breaches featured hacking, 17% involved malware, and 22% involved phishing. Cybersecurity teams are challenged across many fronts defending external attacks from hackers and bots, and delivering the necessary training and awareness so internal teams avoid being a victim of phishing or ransomware.

Reputational Impact of Security Breaches

- **71% of those who suffer a cyberattack** say there was some kind of negative impact on reputation — up from 62% in June 2020
- **90% of respondents had to report** to regulators or engage an IR firm to overcome the reputational problems caused by material breaches in the past 12 months

Source: VMware US Security Insights Report

Exabeam for external threats

Exabeam confronts external attacks head-on with packaged use case content that includes end-to-end workflows. Prepackaged content with detection rules, models, and workflows simplify addressing these fast-moving threats.

Nullify phishing attacks

Exabeam helps security teams outsmart adversaries committing phishing attacks with analytics, automation, and use case content across the full analyst workflow, from detection to response. Because most phishing attacks involve social engineering, where users are manipulated into divulging their credentials, many SOC teams struggle with detecting abnormal activity associated with phishing. With Exabeam, SOC teams gain complete visibility into abnormal user and asset activity to quickly mitigate phishing exploits before the bad actor accesses vital corporate information.

Behavioral analytics combined with Turnkey Playbooks help SOCs detect, triage, and investigate each incident. Investigation checklists provide analysts with recommended next steps for containment and remediation. Exabeam automatically enriches cases with contextual information to reduce false positives and increase alert fidelity, allowing analysts to focus on the most dangerous threats.

Mitigate malware attacks

Based on PurpleSec's 2021 Cyber Security Statistics, approximately 92% of malware is delivered by email; as a result, detection techniques used with phishing attacks also apply to malware. Organizations deal with a plethora of advanced attacks every day; proper detection and response to malware-based attacks is critical to preventing data exfiltration or the spread of a virus. Exabeam provides analysts with malware coverage across all their workflows — collection, detection, investigation, and response.

According to PurpleSec's 2021 Cyber Security Statistics, Trojans make up >50% of all malware attacks. Exabeam provides detection and investigation capabilities on top of endpoint detection and response (EDR) to prevent Trojan attacks. Specific rule-based alerts along with existing logs provide contextual information in chronological order so you can visualize how an entire incident plays out.

Exabeam detects abnormal activity often missed by endpoint solutions. Using behavioral analytics, Exabeam creates a baseline of normal activity for all users and assets, and as a result, SOC teams gain a deeper understanding of the anomalies in their environments. Rather than relying solely on indicators of compromise (IoC) for detection, Exabeam behavioral analytics provides additional detection support for external threats.

Detect ransomware activity

Similar to phishing and malware threats, the first level of defense against ransomware starts with email. Most ransomware attacks deploy via malicious links in email, but they can also come through chat or text. Exabeam detects and alerts analysts of recognized ransomware threats by looking for unique signatures for these types of threats. By using high-fidelity indicators, SOCs can better detect ransomware on endpoint devices. The rules used to detect ransomware derive from forensic analysis of how malware is installed and deployed, providing early ransomware detection. These rules look at common and known types of ransomware such as WannaCry, NotPetya, and their variants.

Exabeam provides vital capabilities to each workflow of collection, detection, investigation, and response for ransomware attacks. By combining anomalous behavior detection with behavioral analytics with a Threat Intelligence Service that tracks IPs, domains, and extensions known to be associated with ransomware attack rules, SOC teams can begin to investigate incidents before they become intrusions. Exabeam offers Turnkey Playbooks for ransomware work out of the box — no additional licenses to third-party tools or API token configuration is needed.

Conclusion

While external threats continue to evolve, Exabeam is making it easier to quickly respond to external threats. With a combination of analytics and automation, Exabeam combines the visibility and productivity to stay ahead of attackers.

When it comes to external attacks, training and endpoint solutions are only one piece of a broader solution. Exabeam combines the best of all worlds, IoCs, rules, Threat Intelligence, machine learning models, playbooks, and context to address external threats allowing SOC teams to quickly identify and remediate these evolving threats.

About Exabeam

As the leading Next-gen SIEM and XDR, the Exabeam Fusion SOC Platform is a modern, modular, and cloud-delivered solution for SIEM and XDR. Exabeam delivers advanced security analytics, automated threat detection and incident response (TDIR) with a use case-based approach focused on delivering outcomes.

For more information, visit exabeam.com.

Exabeam provides the following benefits:

Industry-leading behavioral analytics and automation to detect and respond to threats overlooked by other tools

- 51% reduction in the time it takes to detect, triage, investigate, and respond to threats
- 83% of analysts report triaging twice as many alerts than with their legacy SIEM
- 92% of customers report value in week one
- Advanced SOC capabilities with threat-centric, use-case packages

Want to learn more about Exabeam? Get a demo today.

exabeam