exabeam

Solution Brief

Higher Education

Empower small teams with analytics and automation for faster, more accurate, and cost-effective threat detection, and response

Decentralized, revenue-challenged operations and ever-changing student populations of higher education make this sector a prime target for cyberattacks.

Higher education institutions are besieged by cybersecurity threats due to many challenges. As a byproduct of the global pandemic, enrollments at U.S. colleges and universities have dropped sharply – almost a half-million fewer undergraduate students based on recent estimates. Fewer students mean less revenue, which adds pressure to already challenged IT and security budgets in private and public institutions alike. Higher education also faces a dearth of cybersecurity talent, which weakens the ability to detect advanced threats, investigate potential vulnerabilities, and respond to ransomware and other costly attacks.

A unique challenge for cybersecurity in higher education stems from decentralized operations and security oversight – plus the siloed nature of administrative versus academic systems and users. And unlike a business, which has a relatively stable body of users, higher education also sees continuous new waves of users as students graduate and others take their place. Students often use technology in unusual ways compared to faculty and staff, which poses exceptional detection challenges despite the typical use of dozens of security tools.

> We were drawn to the fact that out of the box, our security operations analysts can use Exabeam to respond to alerts without much customization. Now, with Exabeam, we can tell when a student's VPN behavior is legitimate and not an indicator of compromise. This saves our security team an enormous amount of time."
>
> **Fadi Al Ja'Fari, Information Security & Risk Manager, Deakin University**

Exabeam brings higher education a new, simpler, and more effective way to ensure cybersecurity with existing small teams and within budget constraints.

Mitigating cybersecurity risk

Security teams at many universities and colleges are burdened with unwieldy SIEMs and other legacy tools as they struggle to understand security and network data. Effectively retrieving data from such tools is time-consuming, often requiring specialist coding skills, and resulting in cumbersome investigations. These issues inhibit the early detection of threats like ransomware attacks, and visibility for distinguishing true threats versus odd, otherwise innocuous student behavior online.

Exabeam solutions use behavioral analytics to accurately detect high-risk, anomalous user and entity activity across your network, including on-premises administrative systems, academic research projects, and cloud applications.

By analyzing user behavior your security team is directed, in near real time, to instances of a potentially malicious student or employee, or indicators of compromise such as early signs of a potential ransomware attack.

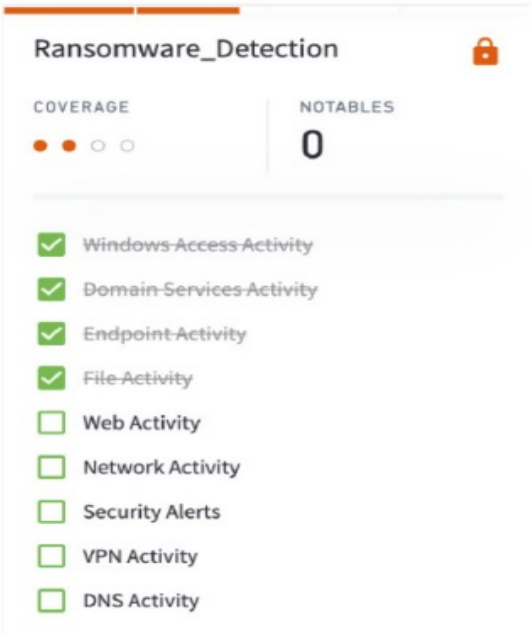

Figure 1 – Exabeam provides guidance on which logs are needed to ensure you have coverage where it matters most.

Ransomware is a huge current risk to higher education institutions. While unique from other malware, ransomware still exhibits several tell-tale signs that can point out an infection is underway. By using machine learning to analyze users' day-to-day behavior in real-time for specific anomalies, it is possible to detect these early warning signs with Exabeam and stop a ransomware infection before it takes hold across your network.

Your security team would view this analysis as an investigation attack chain or 'smart timeline' as shown in Figure 2. Exabeam Smart Timelines provide all the information your analysts need to perform rapid investigations and responses. They include every action a user (or an attacker who has compromised a user's credentials) took during a specific session, including access to personally identifiable information or intellectual property. Your team can see what preceded the security represented in the timeline with a risk score and includes surrounding context such as if the alert maps to the MITRE ATT&CK framework.

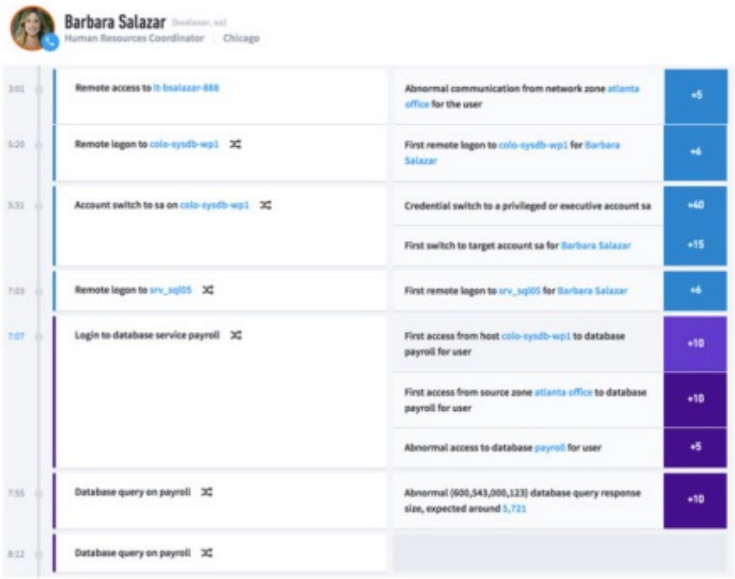

Figure 2 – Exabeam Smart Timelines shows how each action taken by the user is attributed with a risk score, denoting how risky an individual's activity is to the organization.

Addressing the skills shortage

Legacy security solutions are renowned for being resource-intensive, requiring skilled analysts to run manual investigations that consume huge amounts of time and are prone to human error. Your ability to source, train, and retain proficient talent to run such solutions is expensive and hard to fulfill in a market that already suffers from a significant skills gap.

Exabeam's solutions improve analyst productivity through natural language querying, context-enhanced parsing, and data presentation, providing security analysts the ability to quickly create new rules without the need for copious amounts of training.

Exabeam enables you to improve the operational efficiency of a small security team with automation throughout your workflow.

- Behavior-based detection reduces the reliance on static correlation rules.
- Dynamic risk scoring identifies users and assets that may be compromised based on their actions.
- Automated investigations, visualized through Smart Timelines, help analysts accurately detect threats faster.
- Automated response rounds out the workflow with pre-configured playbooks.

By automating the end-to-end workflow, Exabeam cuts the time spent on security tasks by 51% and further supports your compliance requirements by removing the potential for human error borne out of historically manual processes.

Key benefits

- **Plug and play solution offers immediate results**
- **Quickly gain visibility into potential threats and indicators of compromise**
- **Monitor online student activity for unusual behavior**
- **Secure intellectual property and personally identifiable information**
- **Meet data regulatory requirements**
- **Boost productivity by reducing time spent on security tasks by 51%**

> Exabeam has had a significant and positive impact on our security operations. Since deploying Exabeam our time to respond to security incidents has reduced by nearly 80%. The analysts can now stay focused on proactive security monitoring and threat hunting."
>
> **Gartner Peer Review, Education, for Exabeam Fusion**

About Exabeam

Exabeam is a global cybersecurity leader that adds intelligence to every IT and security stack. The leader in Next-Gen SIEM and XDR, Exabeam is reinventing the way security teams use analytics and automation to solve Threat Detection, Investigation, and Response (TDIR), from common security threats to the most critical that are difficult to identify. Exabeam offers a comprehensive cloud-delivered solution that leverages machine learning and automation using a prescriptive, outcomes-based approach to TDIR. We design and build products to help security teams detect external threats, compromised users and malicious adversaries, minimize false positives, and best protect their organizations.

For more information, visit exabeam.com

exabeam