Higher Education

Empower your team with security analytics and automation for faster, more accurate, and cost-effective threat detection and incident response across your institution.

The decentralized, revenue-challenged operations and ever-changing student populations of your institution make you a prime target for cyberattacks.

Colleges and universities like yours are flooded with cybersecurity threats. Due to complex budgeting processes, fluctuating user activity, and lack of security resources, most higher learning institutions find themselves living on the razor’s edge, hoping to avoid a devastating cyberattack. But hope, unfortunately, is not enough. With the school’s reputation and livelihood at stake, it is critical to deploy a solution to protect against growing threats from outside and inside your environments.

So how do you meet these challenges?
The answer is Exabeam.

Exabeam brings higher education institutions a simpler, more effective way to ensure cybersecurity without adding resources or budget.

“... 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
Mitigating cybersecurity risk

Exabeam accurately detects high-risk, anomalous activity on a network, and across cloud instances.

Security teams at many universities and colleges are burdened with unwieldy SIEMs and other legacy tools as they struggle to secure their environment. Effectively retrieving data from such tools is time-consuming, often requiring specialist coding skills (when available), and results in cumbersome investigations. These issues inhibit the early detection of threats like ransomware attacks, and visibility for distinguishing true threats versus odd, otherwise innocuous user 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 potentially compromised credentials, or indicators of compromise such as early signs of a potential ransomware attack.

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

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 (PII) or intellectual property. Your team can see what preceded the activity represented in the timeline with a risk score and surrounding context, such as if the alert maps to the MITRE ATT&CK framework.

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 with the mission to add actionable 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 and incident response (TDIR). Exabeam offers a comprehensive cloud-delivered solution that uses machine learning and automation focused on a prescriptive, outcomes-based approach. We design and build products to help security teams detect external threats, compromised users, and malicious adversaries while minimizing false positives to protect their organizations.

For more information, visit exabeam.com.