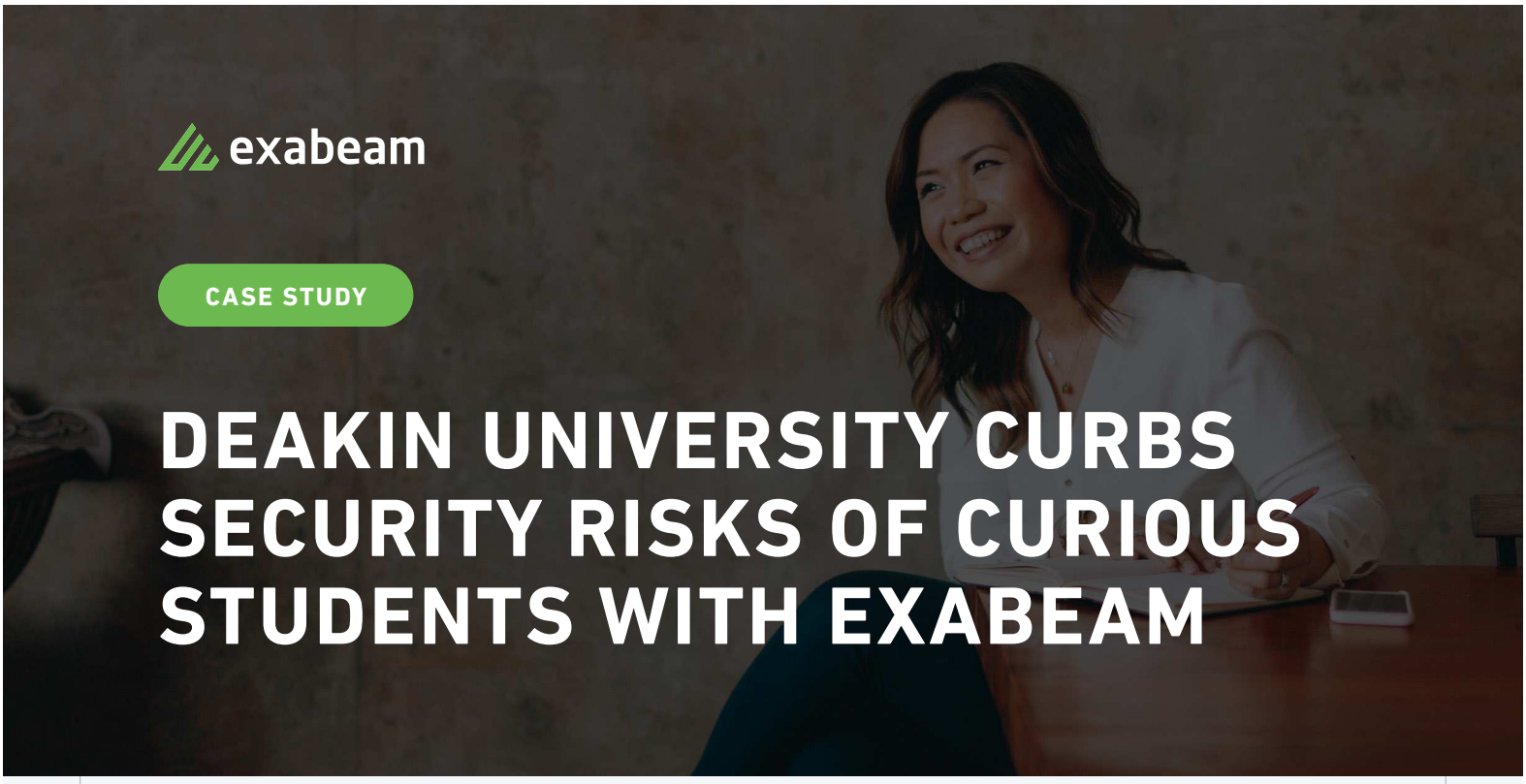

exabeam

CASE STUDY

DEAKIN UNIVERSITY CURBS SECURITY RISKS OF CURIOUS STUDENTS WITH EXABEAM

USER AND ENTITY BEHAVIOR ANALYTICS IMPROVES VISIBILITY AND PRODUCTIVITY

Deakin University is a 61,000-student educational institution based in Australia. Deakin aims to be Australia's premier university in driving the digital frontier. It aspires to enable globally connected education for the jobs of the future, and research that makes a difference to the communities it serves. As a dynamic, young university, Deakin has more than 500 active partnerships in 57 countries supporting academic and research collaboration. About 14,000 students come from international locations. Deakin ranks among the top 1% of universities worldwide and has earned the highest level of overall student satisfaction among universities in the Australian State of Victoria for eight years in a row.

BUSINESS CHALLENGE

Education is the mission of a university, but paradoxically, the curiosity that stimulates learning can have other consequences – particularly for cybersecurity. Australia-based Deakin University puts a priority on helping its students prepare for jobs of the digital future. Curriculum is presented in trimesters, so the institution deals with three major waves of change in student population annually. This is a different, fluid dynamic compared to Deakin's relatively stable community of 4,750 academic and administrative users. It also posed tricky detection challenges for Deakin's cybersecurity team.

> "We were drawn to the fact that out of the box, our security operations analysts can use Exabeam SIEM to respond to alerts without much customization."
>
> **FADI ALJA'FARI, INFORMATION SECURITY & RISK MANAGER, DEAKIN UNIVERSITY**

"Students typically use technology in an unusual way compared to staff, and this sometimes triggers indicators of compromise for their behaviors," says Fadi Alja'fari, Information Security and Risk Manager at Deakin University. "That was our big challenge and why we sought a solution with user behavior

and entity analytics (UEBA)," he says. "We needed a technical solution to help normalize these events and differentiate between what is a malicious indicator of compromise, or something that's benign or unexpected behavior." The cybersecurity team evaluated four of the top solutions surveyed by Gartner and chose the Exabeam Security Management Platform to meet its requirements.

VENDOR SELECTION AND PROOF OF CONCEPT

Addressing unique security challenges presented by students was a big requirement, but Deakin also faces a variety of cybersecurity threats that are shared by all large enterprises. In conjunction with UEBA, Deakin sought to upgrade the overall approach to protecting the university's operations with a security posture program called "Deakin Shield." This priority focused the team's search on the leading tools for security information and event management (SIEM). "We wanted a tool that brings security events from all the tools that Deakin has deployed and presents them in a digestible and actionable manner," says Alja'fari. Top criteria included better visibility via user- and device-based analytics, easy implementation, ease of use, and a good support model, according to Alja'fari.

"When we tested Exabeam's Advanced Analytics, we were drawn to the fact that out of the box, our security operations analysts can use Exabeam SIEM to respond to alerts without much customization," says Alja'fari. "This allows our security engineers to focus all of their time on improving our cyber defenses, instead of learning how to create anomaly detection and events correlation queries – which was incredibly time consuming."

Cost was another major selection factor. Compared to all of the other solutions in the market, they found the support and operational overhead associated with a SIEM solution were minimal with Exabeam.

UNIVERSITY USE CASES FOR USING EXABEAM

Deakin University's security operations team values opportunities to save time and resources. The team was painfully aware of being outgunned by data: its log aggregation solution generated massive amounts of feeds and alerts on the network. Deployment of Exabeam enabled automatic analysis of all the university's security data with notification to security operators of anomalies as they materialize. "Before Exabeam, operators had a delay of deciphering the data and attempting to understand which events might lead to an actual security incident," says Alja'fari.

"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 ALJA'FARI, INFORMATION SECURITY & RISK MANAGER, DEAKIN UNIVERSITY

For example, students might use a VPN service in different ways from a staff member, according to Alja'fari. "Students will use a VPN to try jumping through proxies, using the Tor network, or use one just to try it out and experiment." He notes these behaviors might ordinarily trigger security alerts by legacy tools. "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."

Some of Deakin's other use cases addressed by Exabeam include identifying legitimate network logins from multiple geolocations, leveraging email logs for data leak prevention, and implementing a more cost-efficient logging strategy. "Exabeam's threat hunting capability is something the security operations team looks at on a daily basis for anomaly analysis," says Alja'fari.

exabeam

PUTTING EXABEAM INTO THE CURRICULUM

Deakin University has also leveraged its use of Exabeam in the cybersecurity curriculum. Students who are working toward one of Deakin's cybersecurity degree programs are offered the opportunity to learn in a real-world environment by job shadowing the university's security team operators. These students are hired as interns to help augment capabilities of the team, according to Alja'fari. For purposes of safety and compliance, data and analytics exposed to interns are masked or anonymized. In this manner, students can gain hands-on security operations experience with the Exabeam Security Management Platform before graduation. Earning a real understanding of what it takes to ensure enterprise cybersecurity is a level of educational enhancement that makes these interns all-the-more attractive to employers after graduation from Deakin University.

Key Benefits

Deakin University has seen specific benefits from its Exabeam deployment:

- Stronger enterprise security with behavioral analytics by discovering unusual risks from student "experimentation"
- Deeper visibility on enterprise risks and a streamlined, proactive method of addressing security issues
- Augmenting cyber security education for student interns who shadow security team use of Exabeam

ABOUT EXABEAM

Exabeam is the Smarter SIEM™ company. We empower enterprises to detect, investigate, and respond to cyberattacks more efficiently so their security operations and insider threat teams can work smarter. Security organizations no longer have to live with excessive logging fees, missed distributed attacks and unknown threats, or manual investigations and remediation. With the modular Exabeam Security Management Platform, analysts can collect unlimited log data, use behavioral analytics to detect attacks, and automate incident response, both on-premises or in the cloud. Exabeam Smart Timelines™, sequences of user and device behavior created using machine learning, further reduce the time and specialization required to detect attacker tactics, techniques, and procedures.

TO LEARN MORE ABOUT HOW EXABEAM CAN HELP YOU, VISIT EXABEAM.COM TODAY.