# Enhancing a University's Campus Wireless Security with LogRhythm SIEM

A public university in the United States is comprised of over 30,000 students and 11,000 faculty and staff. The university's campus wireless network is used by students, faculty, and staff to access the internet, email, and other online resources. Due to this, it faced challenges in efficiently managing and detecting stolen devices on its campus wireless network. The university addressed these issues and collaborated with LogRhythm to enhance the stolen device detection process.

## The Challenge

Prior to implementing LogRhythm SIEM, the university relied on a manual approach to handle stolen device incidents. When a device was reported as stolen, the university police department provided whatever information it had on the device, and the security team manually searched through logs to identify any suspicious activity. This process was time-consuming and lacked the efficiency needed to address the increasing incidents of stolen devices on campus.

Another significant challenge was the difficulty in obtaining logs from the Aruba wireless infrastructure used across the campus. Aruba's system required aggregating logs from individual controllers, and the centralization process posed complications in extracting the necessary information for investigation. The university recognized the need for a more streamlined and automated solution to enhance its stolen device detection capabilities.

## The Solution

The university implemented LogRhythm SIEM, a self-hosted security information and event management (SIEM) platform, to enhance campus security and help automate and streamline the detection of stolen devices on its campus wireless network. LogRhythm SIEM collects and analyzes logs from various sources, including wireless controllers, network firewalls, and security appliances. This allows customers to have a centralized view of their network activity, making it easier to detect suspicious activity.

## US University

**Organization:**

University

**Industry:**

Education

**Company Size:**

11,000

**Key Impacts:**

- Streamlined and automated stolen device detection saving SOC team time
- Seamless integration into existing security infrastructure
- Expert support to enhance and optimize the university's cybersecurity strategy

LogRhythm SIEM also generates alerts when a device reported as stolen connects to the network. This allows the university to quickly respond to stolen device incidents and take steps to mitigate the risks.

## Customized Incident Detection, Rapid Response, and Seamless Integration for Wireless Stolen Devices

LogRhythm SIEM proved to be instrumental in automating the detection process of stolen devices on the university's campus. By leveraging SmartResponse™, the university could quickly identify and respond to security incidents. SmartResponse™ is part of the LogRhythm SIEM security orchestration, automation, and response (SOAR) solution. SmartResponse™ accelerates response to suspicious or unauthorized authentication requests to minimize damage, eliminating manual intervention by security analysts.

LogRhythm SIEM is a customizable solution and enables the integration of PowerShell scripts in response to specific log events that facilitate swift and precise response to potential security threats. The ease of deployment further benefited the university, as LogRhythm SIEM is seamlessly integrated into its existing infrastructure, ensuring a quick implementation with minimal disruption to ongoing operations.

> **"LogRhythm SIEM has provided us with a powerful and easy-to-deploy solution,** enhancing our ability to safeguard our campus and respond effectively to security incidents," said the Senior Security Analyst at the university.
>
> **"This partnership has reinforced our commitment to maintaining a secure and responsive campus environment,** showcasing the value of innovative security solutions in the education sector."

## About Exabeam

Exabeam is a leader in intelligence and automation that powers security operations for the world's smartest companies. As a global cybersecurity innovator, Exabeam provides industry-proven, security-focused, and flexible solutions for faster, more accurate threat detection, investigation, and response (TDIR).

exabeam

**Learn more at www.exabeam.com** →