Cybersecurity for Higher Education

Use cases for the higher education industry relating to: data exfiltration, unauthorized access, detecting anonymous traffic, and nation-state cyber espionage.

LogRhythm®

Introduction

The high volume of personal information and research data stored by higher education institutions, coupled with limited security budgets and headcount, makes this industry a prime target for cybercrime.

In April 2020, the education sector was the most popular target of hackers, when hundreds of thousands of students and teachers had to access online resources daily for remote learning. Recent research highlighted that education institutions faced 16 times more attacks than other often-targeted organizations in the healthcare and retail sectors.[1]

With education institutes switching to remote learning amid COVID-19, the need to protect, defend, and respond to threats — regardless of where the user, data, systems, and applications sit — is more apparent than ever. Recently Australian Prime Minister, Scott Morrison, announced targeted cyberattacks to Australian Governments and businesses, highlighting the enhanced need for organizations to protect themselves from being targeted.

In this document, we look at several use cases that outline how LogRhythm's security offerings provide industry-leading automation, compliance, auditing support, comprehensive reporting, and protection against advanced threats. Getting educated with LogRhythm will prevent higher education facilities from getting schooled by hackers.

Why education institutions are a target:

Cyberattacks against educational institutions are a threat because of the diverse and valuable data stored in educational networks, including:

- **Student information:** Educational institutions store a great deal of personal data, such as name, date of birth, and diversity information. This can be a prime target for identity theft.
- **Financial information:** Whether it belongs to students, staff, or the institution, educational organizations store banking and credit information. Compromising this information could allow criminals to transfer funds, take over bank accounts, or commit credit fraud.
- **Research:** Educational institutions could be at risk of losing research accumulated over years in a cyberattack. In addition to damaging the school's reputation, lost data could lead to legal action, the withdrawal of research funding, or loss of security clearances for sensitive material.
- **Email access:** Gaining access to an institution's email servers offers cybercriminals a vector for further attacks on the network.
- **Disruption:** Distributed DDoS attacks aim to disrupt or crash an organization's servers by overwhelming them with more data than they can handle. Such attacks, in addition to shutting down access, can also be used as part of an attack to infect systems with malware that does further damage.

[1] Surge in cyber attacks in Singapore's education sector in April

Data Exfiltration

What is Data Exfiltration?

Data exfiltration is the loss of data due to unauthorized copying, transfer, or retrieval of data from a computer or server. Data loss can occur unintentionally through user error or when a threat actor intentionally steals data for malicious purposes.

Challenge:

Data loss remains a growing threat for organizations of any size. In 2019, there were more than 3,800 reported data breaches, with 52 percent more records exposed than in 2018. And the outlook appears bleak for the remainder of 2020. There have already been several high-profile breaches in the first half of 2020, and the estimated cost of a data breach in 2020 is over $150 million.[2]

Solution:

The LogRhythm XDR Stack enables organizations to detect, qualify, and remediate data exfiltration attempts. NetworkXDR goes beyond network traffic analysis with an integrated set of capabilities and workflows for detecting, qualifying, investigating, and responding to advanced threats hidden in network traffic data. LogRhythm NetworkXDR can help detect unknown network-borne threats like data exfiltration and help teams remediate and contain an issue quickly with automated response features.

Additionally, UserXDR, LogRhythm's user and entity behavioral analytics (UEBA) solution, tracks unauthorized data access and exfiltration, e.g., when a compromised user account or a rogue insider finds sensitive data on your network. Our full-spectrum analytics and file integrity monitoring (FIM) can help you detect when a user inappropriately accesses protected data — in real time.

[2] Prevent Data Exfiltration with Network Traffic Analytics

Typical Approach to Data Exfiltration

- Get to the data (discovery)
- Move the data by coordinating with their foothold (command and control)
- Exfiltrate the data (lateral movement)

Sample Log Types Needed to Detect Data Exfiltration

- DNS logs
- Email servers (e.g., Exchange)
- Proxy logs
- Network logs

Types of Detection

- **Suspicious port activity:** Suspicious port activity refers to the process of learning details about potential vulnerabilities or services that are running on a host by sending packets to specific ports.
- **Email activity to non-corporate domains:** Given the ability, many users would like to access third-party email accounts from a corporate network. Detecting non-corporate email activity will prevent corporate data leaving the network through a non-corporate service and maintain records of official correspondence by ensuring the use of the corporate email service.
- **Excessive email by a specific host**
- **Suspicious, large volume of DNS queries:** One of the ways criminals exploit individuals or organizations is by trying to register disposable domain names for spam campaigns and botnet administration, and utilizing compromised domains to host phishing or malware downloads, etc.
- **Web uploads to non-corporate sites by users:** Bad actors can use multiple entry points like phishing emails, botnets, or customized executables to trick users into uploading data to non-corporate sites leading to data leakage.

Use Case:

An attacker is looking for sensitive financial information. The attacker successfully compromises a host and is able to copy the information to a different external server.

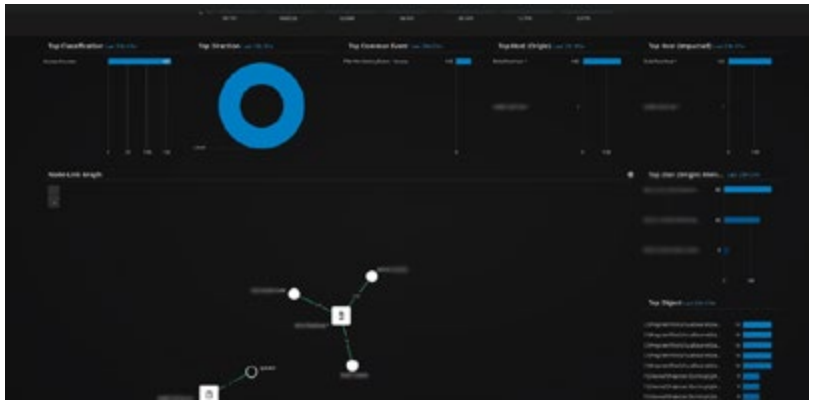


Figure 2: Detecting data exfiltration in the LogRhythm Web Console

Figure 3: MITRE ATT&CK Module implementation for detecting data exfiltration

Unauthorized Access to Critical Data

Challenge:

For universities, information about assessment criteria, research data, student information, etc., is critical to daily operations. It is very common to see unauthorized access instances due to lack of safeguard mechanisms to information and IT resources. Sometimes, this will result in the loss of confidentiality, integrity, and availability of the technology assets.

Solution:

Universities should implement an effective IT security strategy to protect critical data and assets. The strategy will help ensure the confidentiality, integrity, and availability of systems — intellectual property vital to universities. Additionally, they help protect a universities reputation and employee and student privacy.

Types of Logs Needed to Detect Unauthorized Access

- Windows security logs
- Windows application logs
- File integrity monitoring logs

Types of Detection

- Anomalous data access
- Unauthorized file access

Use Case:

Suspected access to a folder shared by lecturers containing confidential data by an individual outside the lecturer department.

Figure 4: The LogRhythm dashboard highlights unusual user behavior

Figure 5: Detecting unauthorized file access

Detecting Anonymous Network Traffic

Challenge:

Anonymous browsers act as a medium for cyberthreats such as malware, botnet, and DDoS attacks, as well as methods of information theft.

It's common to see new browsers developed to hide user identity on the internet. For example, the Tor browser was built primarily for anonymous browsing without cybersecurity needs or security requirements in mind.

The Tor browser works by employing a technique called "onion routing." Onion routing works by encapsulating messages in layers of encryptions that are then transmitted through a series of nodes called "onion routing."

Universities need to consider implementing various tools to detect threats hidden in anonymous traffic and automate actions to remediate threats.

Solution:

LogRhythm provides detection, alert and automation capabilities for anonymous traffic.

Organizations can leverage LogRhythm to detect anonymous traffic in multiple ways as below:

a) Threat intelligence feeds

b) Threat detection modules

c) LogRhythm Labs list updates

d) User and entity behavior analytics

e) LogRhythm NetMon

LogRhythm Labs

You may not be an expert in every area of security — which is why we built a team of dedicated security experts. Our LogRhythm Labs team delivers unparalleled security research, analytics, and threat intelligence services. By delivering actionable intelligence and advanced analytics, your team is empowered to greatly reduce its time to detect and remediate the latest security threats.

Learn more about LogRhythm Labs ›

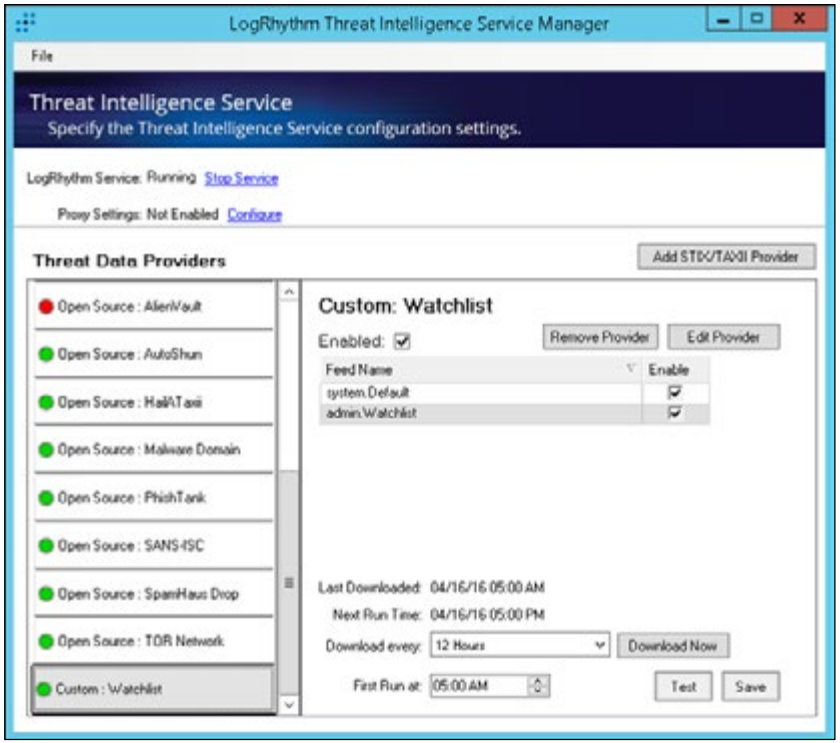


Figure 6: LogRhythm Threat Intelligence Service Manager

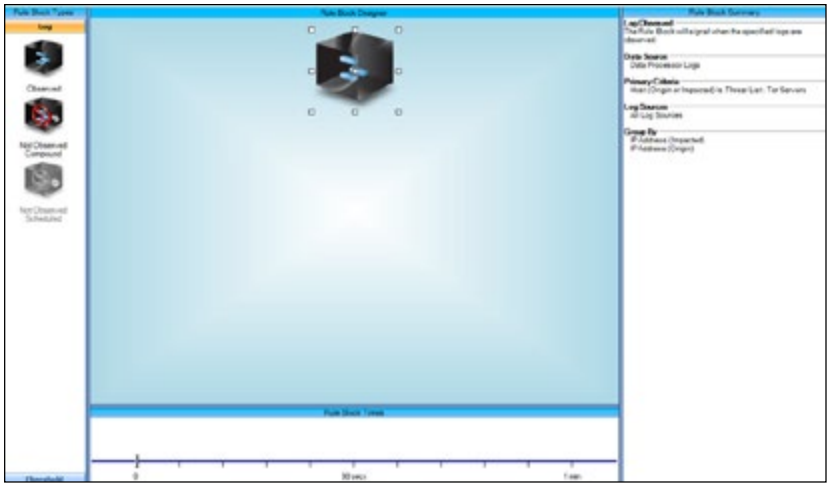


Figure 7: A sample use case from the LogRhythm Threat Detection Module to identify Tor traffic

Nation-State Cyber Espionage, a Worrying Trend

Challenge:

There is increasing risk from cyber espionage targeting countries and organizations. Recently, Australian Prime Minister, Scott Morrison went live on various media outlets and announced targeted cyberattacks to Australian Governments and businesses and a need for organizations to protect themselves from being targeted.

When reviewing the government advisories there were multiple references to the tactics, techniques, and procedures listed in the MITRE ATT&CK framework.

Solution:

LogRhythm has published several modules to help organizations achieve rapid deployment with minimal configuration. These modules not only cover security best practices, but also cover key areas where organizations need to focus. The modules have references to use cases and its prerequisites, thus helping organizations focus on implementation, gain visibility, and remediate based on findings.

Reference Links:

Main advisory | 18th June 2020:

https://www.cyber.gov.au/threats/advisory-2020-008-copy-paste-compromises-tactics-techniques-and-procedures-used-target-multiple-australian-networks

Linked advisories | 22nd May 2020:

https://www.cyber.gov.au/threats/advisory-2020-004-telerik

https://www.cyber.gov.au/threats/advisory-2020-006-active-exploitation-vulnerability-microsoft-internet-information-services

Core Threat Detection Module:

This module is a collection of fundamental AI Engine (AIE) rules that can be utilized to provide a balanced and basic level of security coverage with minimal configuration. Additionally, this rule set can be used as an introduction to AIE rules before an organization begins moving on to more complex and customizable rules.

Download the Core Threat Detection Module Guide >>

MITRE ATT&CK Module:

MITRE ATT&CK™ is an open knowledge base of observed adversary tactics and techniques based on real-world observations. This framework enables broad sharing of adversarial behaviors across the attack lifecycle and provides a common taxonomy for threat analysis and research. The LogRhythm MITRE ATT&CK Module provides prebuilt content mapped to ATT&CK within the LogRhythm NextGen SIEM Platform, including analytics, dashboard views, and threat hunting tools. This content enables you to detect adversaries and improve your security program as prescribed by the MITRE ATT&CK framework.

Download the MITRE ATT&CK Module Guide >>

Network Detection and Response Module:

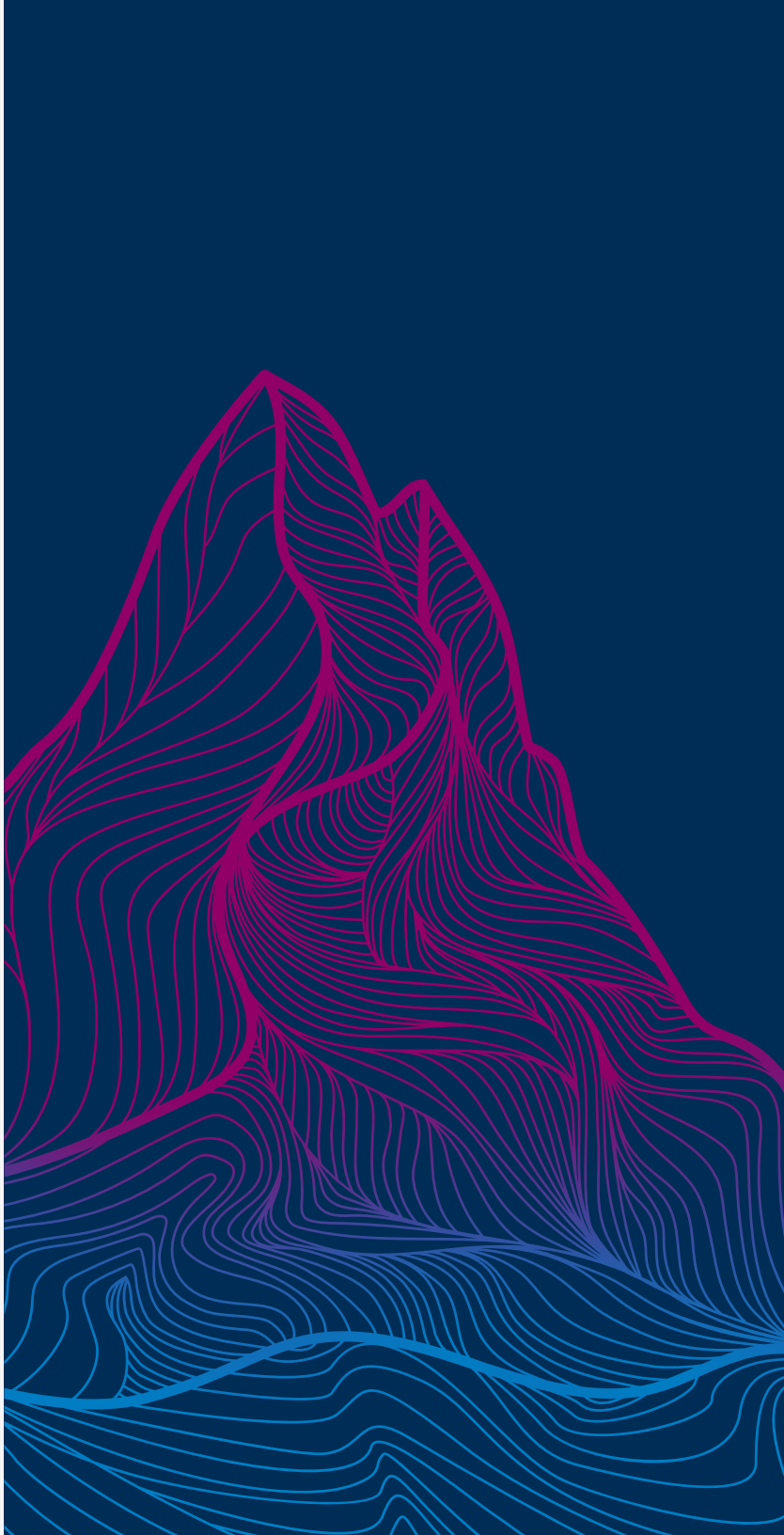
The LogRhythm Network Threat Detection Module delivers comprehensive analytics beyond what legacy Network Behavior Anomaly Detection (NBAD) and flow analysis tools can provide. This module empowers your organization to understand the network activity occurring in your environment by delivering automated, preconfigured rules, dashboards, investigations, and reports that reduce the time it takes to detect and respond to a broad range of cyberthreats.

Download the Network Detection and Response Module Guide >>

About LogRhythm

LogRhythm's award-winning NextGen SIEM Platform delivers comprehensive security analytics; user and entity behavior analytics (UEBA); network detection and response (NDR); and security orchestration, automation, and response (SOAR) within a single, integrated platform for rapid detection, response, and neutralization of threats. Built by security professionals for security professionals, LogRhythm enables security professionals at leading organizations NASA, Xcel Energy, and Temple University to promote visibility for their cybersecurity program and reduce risk to their organization each and every day. LogRhythm is the highest-ranked provider for customer satisfaction in G2 Research's grid report for SIEM.

To learn more, please visit: www.logrhythm.com.



LogRhythm®

1.866.384.0713 // info@logrhythm.com // 4780 Pearl East Circle, Boulder CO, 80301