Securing free and easy access to knowledge

Providing free and easy access to digital resources is a key issue for education institutions across the world. Expectations of free and easy access among new generations of students and researchers are high, but increasing cybersecurity by building new and higher digital walls and safety barriers contradicts the concept of free and easy access. SIEM allows education institutions to immediately detect cyberthreats without severely restricting access to digital resources and also supports Safeguarding of students in education institutions.

/logpoint

Cybersecurity challenges at education institutions

Providing free and easy access to digital resources is a key issue for education institutions across the world. Allowing students and researchers free and unlimited access to wealth of information on the internet, in digital libraries and databases, providing state-of-the-art tools for processing and analyzing information and supporting efficient online collaboration is essential in this day and age.

For education institutions to continue to attract the best and brightest, educating the thought leaders of tomorrow and providing research results supporting the growth and prosperity of society, providing free and easy access is paramount. At the same education institutions has to maintain the highest levels of cybersecurity protecting students, staff, research data and their reputation.

But education institutions are facing a number of challenges:

- With the trend towards Bring-Your-Own-Device (BYOD) and expansive public WiFi access, education institutions with their relatively open environments provides a large exposed surface for cyberattacks.
- Keeping networks and IP safe against cyberattacks while allowing access to systems to very technically adapt individuals
- Keeping Cybersecurity policies up to date, but not impinge on learning and innovation. They also need to be future-proof as user demand scale and evolve.
- To effectively safeguard students online, education institutions needs to be able to monitor student and staff online activity, while protecting the privacy of the individual
- Identifying the difference between academic research like ethical hackers and malicious activity, strengthening security and eliminating false positives.
- Quickly and efficiently identifying students, that are putting the education institutions' reputation at risk by illegally downloading copyrighted material or mining Bitcoin using education institutions' resources
- Operating large and often complicated network infrastructures with reduced IT Budgets and resources compared to commercial organizations.

Expectations of free and easy access among new generations of students and researchers are high, while concerns about safety and privacy are growing. Increasing cybersecurity by building new and higher digital walls and safety barriers contradicts the concept of free and easy access. Consequently, education institutions have to look towards cybersecurity solutions such as SIEM (Security Incident and Event Management), to be able to address their Cybersecurity challenges.

SIEM for education institutions

SIEM allows education institutions to immediately detect cyberthreats without severely restricting access to digital resources. The Logpoint SIEM solution provides monitoring, detection and alerting of security events or incidents within the education institution's IT environment. It provides a comprehensive and centralized view of the security posture of the infrastructure and gives Cybersecurity professionals detailed insight into the activities within their IT environment.

SIEM software collects and aggregates log data generated throughout the education institution's infrastructure, from host systems and applications to network and security devices, such as firewalls and routers. The SIEM then identifies, categorizes and analyzes incidents and events and delivers real time alerts, dashboards or reports to the cybersecurity team.

With User Entity Behavior Analytics (UEBA) Logpoint provide extensive machine learning and anomaly detection capabilities, for advanced threat detection. Leveraging advanced Machine Learning, it enables you to detect cyberattacks immediately by spotting unusual patterns of activity and eliminate false positives. This ultimately can assist education institution security teams to increase their effectiveness and reduce the resources required to run security operations – which is important in a time where there's a shortage of security skills and an ever-increasing number of alerts.

In a nutshell, SIEM allows Cybersecurity teams to see the bigger picture by collecting security event data from applications, the cloud and core infrastructure to learn exactly what goes on within the network – creating value from the sum of data which is worth much more than the individual pieces. A single alert from an antivirus filter may not be a cause of alarm on its own, but if it correlates with other anomalies, e.g. from the firewall at the same time, this could signify that a Cybersecurity threat is developing.

With User Entity Behavior Analytics (UEBA) Logpoint provide extensive machine learning and anomaly detection capabilities

Safeguarding using SIEM

In addition to the technical challenges, education institutions are facing a separate issue in Safeguarding students. Essentially it is preventing and protecting students from exposure to materials that may cause themselves or other individuals to come to harm, like forums on self-harming or websites know to propagate extremist views.

The safeguarding approach many education institutions take is to block specific websites entirely, limit internet usage on public networks, and closely monitor the activity taking place there. As a baseline control mechanism, these measures can help raise a red flag if a student or staff member is using the network in a way likely to cause harm to themselves or others.

On their own however, these measures are blunt instruments. With the right tools in place and a clear understanding of safeguarding's aims, education institutions can implement more sophisticated measures that go beyond blocking, while remaining mindful of privacy. It is possible to safeguard students' well-being without restricting academic endeavor, informed discussion, or debate around controversial topics.

What is needed is context, and that's where the analytics power of the Logpoint SIEM and UEBA based on Machine Learning, can help education institutions correlate activity with what we might know about the individuals engaging in it. Someone accessing self-harm forums could be a potential flag, but what is the context?

By understanding who that individual is, are they the welfare officer or are they a student, a SIEM solution can provide context. Adding other key metrics like how many times have they tried to access that type of information, what key words are they searching for, we can make informed decision – quickly and efficiently.

How is Logpoint working with education institutions

Logpoint is working with a number of education institutions across Europe and the US on overcoming these challenges by utilizing Logpoint's next-gen SIEM and UEBA, providing a unified solution for management, correlation and analysis of machine and entity data. Engineered with a simplified taxonomy and advanced analytics Logpoint translates data into valuable intelligence enabling education institutions to make informed decisions.

Cyber Security and Compliance

Computerome, the Supercomputer for Life Science is a collaboration between Technical University of Denmark (DTU) and University of Copenhagen (UCPH). Logpoint was chosen by Computerome as a key security platform to ensure the highest level of security and compliance. This was done by:

- Offering a full custom integration services – Logpoint's single taxonomy allowed for easy integration with the Computerome systems
- Enabled real time monitoring of security controls, providing real time data analysis.
- Early detection of possible data breaches, data collection, data storage and accurate data reporting.
- Built in log analysis is configured to automatically detect and notify all critical events in the Computerome system before the happen.

"Logpoint allows Computerome administrators to quickly detect unusual behavior in the system and to prevent misuse and data breaches. It provides that extra layer of security on top of the established security controls, which is required when handling vast amounts of data. It also allows us to provide our users with full insight and transparency"

Peter Løngreen, National Life Science
Supercomputing Center

Dramatic improvements in cybersecurity efficiency

Logpoint was chosen by Columbia College in Missouri as a replacement to their existing SIEM which was no longer meeting requirements. As the amount of users, data and cybersecurity threats grew, Columbia College wanted a SIEM solution with a powerful search capability and the ability to ingest and store large amounts of data. By implementing Logpoint, Columbia College can now

- Have customizable dashboards that provide instant overviews, pre-built customizable alerts and normalized log format
- Run a query for 30 days of data in less than 2 minutes
- Have a real time overview of their cyber security posture, making determination of incidents quickly and efficiency.

How is Logpoint working with education institutions

Strengthening Security and Eliminating False Positives

Logpoint has worked with University of Bedfordshire, a UK university with over 14,000 students to convert data into actionable intelligence, greatly improving their cyber security posture. This is done by:

- Simplifying management of network alerts
- Improving ability to identify incidents requiring actions
- Ingesting logs from its numerous IT Systems and then correlating to find indicators or compromise/attack or patterns of threatening behavior.
- Significantly reduced workload associating with correlating security logs.

> "Having central visibility and the ability to enrich logs in Logpoint is incredibly useful from a security perspective. Having identity -enriched logs means that we can spot privilege misuse, observe trends, investigate effectively and pick out issues preemptively before they become an actual problem,"
>
> John Couzins, IT Security Manager,
> Lancaster University

Achieving cybersecurity visibility

With Logpoint, Lancaster University has taken cybersecurity to a new level. The Logpoint SIEM solution allows the IT security team to identify privilege misuse, observe trends, and investigate effectively, while also providing a valuable tool to optimize operations. The Logpoint node-based license model allows Lancaster University to process massive amounts of data, without fear of tipping the budget.

Working with Logpoint has enabled Lancaster University to

- Enable 80-90% quicker response time to cyberthreats
- Have the ability to throw a large amount of data into Logpoint which would be impossible to capture in a volume base license model
- Use identity enriched logs that means Lancaster University can investigate effectively and pick out issues pre-emptively before they become an actual problem
- Use the Logpoint API to create custom functionalities supporting the IT Security team

Why education institutions choose Logpoint

1. **Education institutions prefer Logpoint's intuitive analytics and advanced threat hunting capabilities**

   Logpoint's unique taxonomy harmonizes data from cloud applications, core infrastructure, security products and proprietary applications, among other sources. By leveraging this taxonomy, analytics is consistent across all data sources and use cases, enabling analysts to focus on the output of behavioral analytics, machine learning and correlations use cases.The taxonomy extends to the integration layer, allowing easy consumption of threat intelligence, adding business context to events and integration with the rest of the infrastructure.

2. **A flexible security analytics platform to fit the education institutions' technology strategy**

   Logpoint supports education institutions, colleges and other educational institutions with security strategies that are on-premises, in the public cloud and through a managed security service provider. By supporting more than 400 of the most critical security data sources, education institutions can ingest data from virtually any source – from databases to cloud applications.

3. **Unmatched time-to-value makes it resource efficient to implement and expand Logpoint**

   Our customers tell us that time-to-value is a huge factor for why they choose our solution. Logpoint gives you a full SIEM solution that provides valuable analytics within a matter of days. Adding UEBA capabilities to enhance the SIEM takes no more than 6 hours, which brings customers unmatched time-to-value.

Why education institutions choose Logpoint

4. Predictable and transparent total cost of ownership

Logpoint works with your infrastructure, and we believe that the licensing model should not be a limiting factor when planning how and which data sources you would like to ingest data from. Our node-based pricing for SIEM is straightforward, and unlike other SIEM vendors, it covers all servers and data ingested – giving you the control and predictability to know exactly what the total cost of ownership will be.

5. Large partner community enables maintenance-free security operations

Logpoint takes a 100 percent customer-centric approach. You can join an ecosystem of some of the best global integration and technology partners, as well as hundreds of customers including numerous education institutions across Europe and the US. We provide 24/7 service and enjoy a consistent 97 percent satisfactions among customers for our support.

> Our customers tell us that time-to-value is a huge factor for why they choose our solution

About Logpoint

Logpoint is the creator of a reliable, innovative cybersecurity operations platform — empowering organizations worldwide to thrive in a world of evolving threats.

By combining sophisticated technology and a profound understanding of customer challenges, Logpoint bolsters security teams' capabilities while helping them combat current and future threats.

Logpoint offers SIEM, UEBA, and SOAR technologies in a complete platform that efficiently detects threats, minimizes false positives, autonomously prioritizes risks, responds to incidents, and much more.

Headquartered in Copenhagen, Denmark, with offices around the world, Logpoint is a multinational, multicultural, and inclusive company.

For more information, visit www.logpoint.com

Trusted by more than 1,000 enterprises

KONICA MINOLTA CAPTIVATE

BOEING

GOSECURE RÉMY COINTREAU

Awards and honors

Gartner peerinsights customers' choice 2021

Gartner Peer Insights

Gartner

Gartner Magic Quadrant

Software Reviews GOLD MEDAL 2021 SECURITY INCIDENT AND EVENT MANAGEMENT

/logpoint