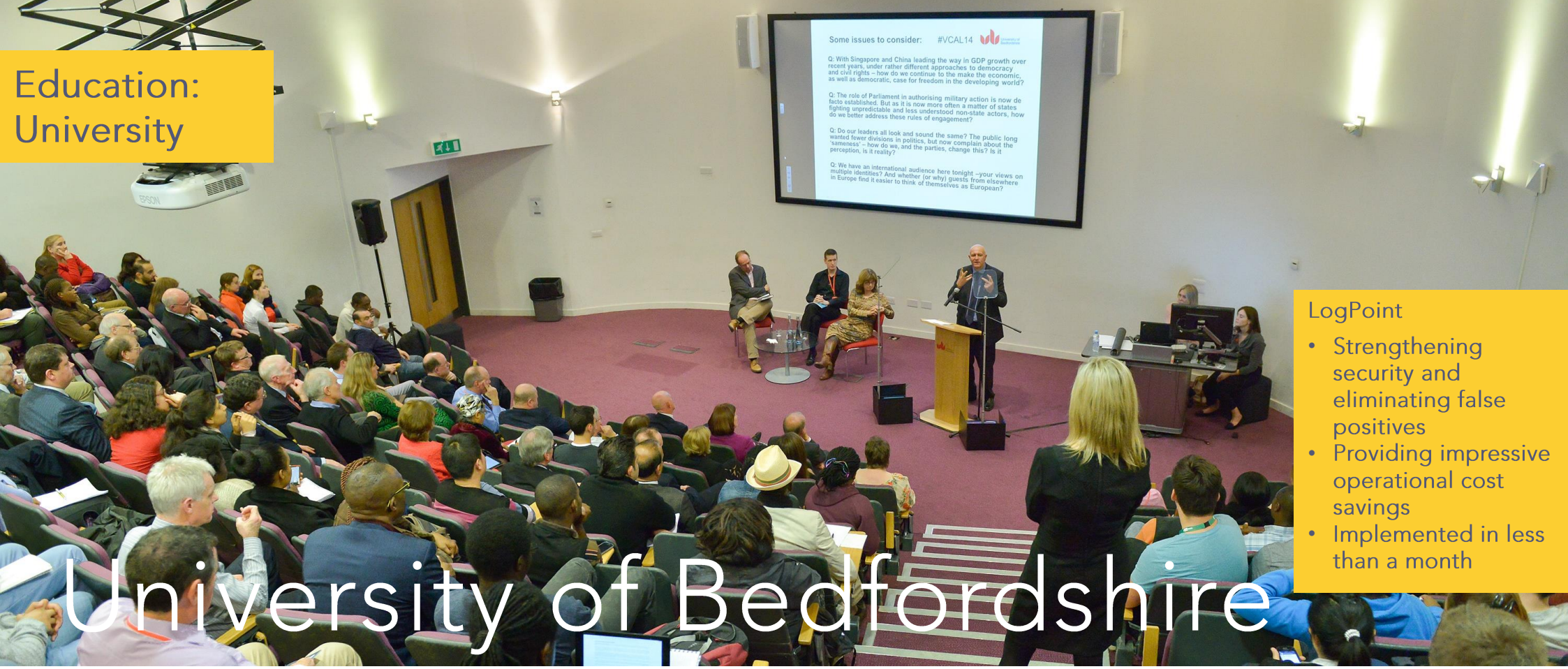
Education: University




LogPoint

- Strengthening security and eliminating false positives
- Providing impressive operational cost savings
- Implemented in less than a month

# University of Bedfordshire

## How LogPoint is helping the University of Bedfordshire strengthen security and eliminate false positives

With LogPoint, the University of Bedfordshire's IT team has simplified management of network alerts and improved their ability to identify incidents requiring action. By converting data into actionable intelligence and improving their cybersecurity posture, LogPoint has reduced time-consuming analyses of security logs while eliminating the majority of false positives.

LOGPOINT

# Education

University of Bedfordshire

## Background

For the University of Bedfordshire, protecting IT infrastructure is a round-the-clock responsibility. With campuses in Luton, Bedford, Milton Keynes and Aylesbury, the university welcomes more than 14,000 students each year from over 120 countries. It serves international learning communities via education partners in China, the Middle East, Europe and South East Asia.

In a sector where IT budgets can be limited but intellectual freedom and information accessibility are key, identifying potential breaches and knowing which of them require action is essential. Many universities are challenged to find the resources to be able to accomplish this in an effective way.

As the cyber threat environment becomes more heated and complex, it can be easy for security teams to feel overwhelmed by network monitoring. That's particularly true in the open environment of a university, where large numbers of visitors jump on and off public WiFi on a daily basis; while students and staff increasingly bring their own devices on campus to access network resources.

"The operational cost savings we've seen have been impressive, and the support we've received from LogPoint before, during, and after implementation has really been fantastic. We're now upgrading to the latest version of LogPoint and looking to leverage its analytics to assess other areas such as asset utilization and more detailed profiling of the devices, applications and operating systems users bring to the network."

Chris Newby, Systems Infrastructure Manager at University of Bedfordshire

Bedford Campus Gateway Building

## The challenge

For the university to continue to attract the best and brightest, it has to meet the highest levels of cyber security across its infrastructure. Policies need to be up-to-date and not impinge on learning and innovation. They also need to be future-proofed as user demands scale and evolve. Ensuring regulatory compliance and having the ability to respond quickly and accurately to legal requirements such as the government's Prevent programme, are necessary to ensure that the University can meet

LOGPOINT

# Education

all of its legal, regulatory and strategic obligations.

With the trend toward BYOD and expansive public WiFi access, the university's relatively open environment provides an exposed surface for cyber-attack. Ethical hacking courses are also offered, and IT managers needs to understand if internal breaches are benign and course-related, or malicious and potentially damaging.  Total security is impossible and as such breaches have to be expected. The issue for Bedfordshire and other universities is knowing how early a breach can be detected, and how quickly end points can be locked down before real damage occurs.

With growing complexity and increasing security demands, the University of Bedfordshire IT team felt that its open source solution for detecting and responding to security threats had reached the limit of its capabilities.

## The Solution

Recognizing that its legacy network monitoring systems were no longer up to the job; the University began evaluating Security Information and Event Management (SIEM) solutions to improve their ability to sift through information and highlight difficult to detect security issues.

"With so many users spread across locations, devices and access points, managing all the alerts around authentications has been our main pre-occupation. We were seeing more and more compromise attempts, but they were fragmented across logs," said Chris Newby, Systems Infrastructure Manager at University of Bedfordshire. "We set a straightforward scope for the new system initially to help us better capture and analyze authentication events."

Bedfordshire settled on LogPoint's solution for ingesting log data from its numerous IT systems and then correlating it to find indicators of compromise/attack, or patterns of threatening behavior. LogPoint's system is designed to be simple, flexible, and scalable, providing modular design, streamlined deployment, and integration tools that make it easy for enterprises of all sizes and budgets to adopt SIEM. Smaller networks can emphasize simplicity and deploy components within a single virtual appliance. Larger networks can split components across various network zones

## Facts

| | |
|---|---|
| Customer | University of Bedfordshire |
| Industry | Education, University |
| Location | Bedfordshire, United Kingdom |
| Objectives | Strengthen security and eliminate false positives |

# Education

to reduce potential load on the network.

"By addressing the issue with a more effective solution we hoped to save time and free up team resources to focus on only the events with high risk potential for loss or damage," said Chris Newby.

**Results:**

With expert support from LogPoint and best practice guidance from the SANS Institute, Chris and his team implemented LogPoint in less than a month. He and his team have been able to significantly reduce the workload associated with correlating security logs.

LogPoint's SIEM has given University of Bedfordshire the ability to be alerted on and assess the seriousness of a number of issues around authentications, such as failed authentications due to bad username /password combinations, concurrency, user access time limits, or too many failed password attempts.


Graduation at University of Bedfordshire

"The operational cost savings we've seen have been impressive, and the support we've received from LogPoint before, during, and after implementation has really been fantastic," said Chris Newby. "We're now upgrading to the latest version of LogPoint and looking to leverage its analytics to assess other areas such as asset utilization and more detailed profiling of the devices, applications and operating systems users bring to the network."

## Contact LogPoint

If you have any questions or want to learn more about LogPoint and our next-gen SIEM solution visit www.logpoint.com or contact us at sales@logpoint.com

LOGPOINT