NXLog

NXLog Helps the University of East Angila Meet PCI Compliance and Minimize SIEM Migration Costs

NXLog Helps the University of East Angila Meet PCI Compliance and Minimize SIEM Migration Costs

CUSTOMER PROFILE

The University of East Anglia is a public research university in Norwich, England. Established in 1963, its campus has a 16,872 students population as of 2023.

According to **Research Excellence Framework (REF)**, UEA is positioned as a Top 20 research-intensive university and **Top 100 Times Higher Education World University Rankings 2023** for research citations. The University displays a Top 30 performance in two main UK charts for 2023: **The Times/Sunday Times Good University Guide** and the **Complete University Guide**.

UEA alums and faculty include 3 Nobel Prize winners, a discoverer of the Hepatitis C and Hepatitis D genomes, a co-inventor of the Oxford–AstraZeneca COVID-19 vaccine, a discoverer of the small interfering RNA, President of the Royal Society, 3 Fellows of the Academy of Medical Sciences and 48 Fellows of the Royal Society.

RELATED INDUSTRIES

- Education
- Public Research and Science
- Business School

BUSINESS DEMANDS

- Improve security posture
- PCI DSS compliance

CHALLENGES

Establish a unified log collection pipeline to aggregate events from various sources, including Windows, Linux, and network appliances. Enable ongoing security monitoring and longterm retention of security events.

SOLUTION

- NXLog Platform
- NXLog Professional Services

BUSINESS RESULTS

- Improved security posture with centralized log collection
- Achieved PCI DSS compliance
- Reduced SIEM migration costs

BACKGROUND

Modern academic institutions are susceptible to data breaches and cyber-attacks due to their open and collaborative IT environment with thousands of disparate users and widely adopted BYOD (bring your own devices) practices. Vast volumes of personal and research data make universities ideal targets for cybercriminals.

UEA offers a blended approach to learning and teaching with cutting-edge digital services that enable studying and coaching from anywhere. This includes a remote desktop service to access a campus-based computer and a virtual learning environment to access course materials, submit assignments, and attend online lectures.

With over 700 computers and 6,000 wireless access points across the entire campus, the UEA network provides resilient, fast connections for offices, student residences, and teaching spaces. The network links to an on-site data center, cloud services, and the wider internet. The UEA IT team aims to maintain campus network availability 24 hours a day, seven days a week.

The main focus of the UEA security team is to establish university-wide security policies and maintain a strong security posture that includes balanced endpoint protection, multi-factor authentication, security monitoring, and proactive threat hunting to mitigate cyber-attacks.

PROJECT & SOLUTION

UEA is subject to PCI-DSS compliance and, according to “Requirement 10. Log and Monitor All Access to System Components and Cardholder Data”, it was necessary to implement centralized log collection for ongoing monitoring and long-term security logs retention.

The network infrastructure of UEA represents a very diverse set of endpoints, including hundreds of Windows and Linux servers and network appliances such as routers and firewalls. Collecting the necessary security logs from these systems, with their different log formats and output methods, poses a tremendous technical challenge.

UAE chose to roll out agent-based log data collection and smoothly deployed NXLog Agent across its infrastructure. Centralized agent fleet management provided by NXLog Platform allows for ongoing performance health-checks and convenient configuration of installed agents via visual tools. UAE team opted to configure NXLog to forward logs to two destinations: the first filters security events from critical systems and forwards them to a SIEM, and the second saves all unfiltered logs to network-attached storage (NAS, cold storage) for long-term retention.

NXLog supports both agent-based and agentless log shipping with robust High-Availability/Failover options. UEA security team is now looking forward enhancing its telemetry pipeline architecture with agentless configurations for better scalability and reliability.

NXLog has been chosen among competitors due to its wide integration list, flexible deployment schema, and a solid reputation across the log management market.

Cybersecurity is an evolving thing, and facing the need to migrate from one SIEM solution to another, we found it very easy to accomplish with NXLog. Autonomous telemetry pipeline powered by NXLog allowed us to switch between security monitoring platforms without much reconfiguration and save costs.

At UEA, we are really impressed with the product. It’s absolutely reliable and does pretty much everything we expect from the log collection software. Also, customer service is excellent. We definitely got the value out of NXLog Professional Services while planning and during deployment.

Andrew Dixon,
Operational IT Security Manager.

For more information about NXLog products and services, visit our website,contact us via the web form, or schedule a meeting.

Start free with the NXLog Platform now!