eb-Qual

Customer Case Study

UNIVERSITÄT BERN

Transparency in real time

The University of Bern employs IBM's QRadar SIEM for monitoring data communication and network components.

Prioritized presentation of threats is needed to ensure the efficient and secure operation of the university's network – a requirement comfortably met by QRadar SIEM.

Initial situation

In the past, the University of Bern used a wide variety of independent tools to capture and archive log and NetFlow data. This made data capture and the later collation of all relevant information an extremely arduous task. Furthermore, the retrieval of recorded data archived to an external system on a daily basis was equally time consuming.

To resolve these issues, the University of Bern decided to evaluate a consolidated Security Intelligence Platform that securely archives all information – regardless of its type or origin – while granting various user groups access to that data via the web. The solution also had to enable forensic analyses and pro-actively generate alerts for problems and threats in the network and in end systems.

The solution

After closely assessing and extensively testing several products, the University of Bern chose the simple-to-use and intuitively designed QRadar Security Intelligence Platform from IBM. Stefan Zahnd at the University of Bern's IT services department stated that "we opted for QRadar for several reasons, the main ones being ease of installation, maintenance and administration. Equally important was the fact that all required logging formats are available out of the box, and that Net- and SFlow are supported. The incredible value for money and almost limitlessly scalable nature of this solution were also significant factors. The obvious competence of QRadar solution provider eb-Qual was also important. The company has already shown us that it is an enthusiastic and experienced partner and systems integrator. eb-Qual has been supporting our DNS/DHCP/IPAM systems from Infoblox and our Juniper Secure Access solutions at a consistent level of excellence for years."

“Ease of use, high reliability, top performance and flexibility as well as minimal administrative overheads – QRadar fully satisfies all of our requirements.”

Stefan Zahnd, IT services at the University of Bern, infrastructure group.

Minimal operation effort

QRadar is currently recording data from around 90 sources at the University of Bern. These include data from ASA, Checkpoint and Palo Alto firewalls, and from components and solutions such as routers, RADIUS, VPN, domain controllers, MPP, wireless controllers, Linux and Windows servers, and Infoblox DNS, Exchange and Squid proxies. It was only the connection with the open-source solution FreeRADIUS that required the development of a log source extension.

The systems at the University of Bern integrated into QRadar generate 60 million indexed events and over 80 million flows every day. However, the administrative overheads are at an absolute minimum despite this extraordinary amount of data. The time needed per week to administer the system tends to be around one hour, says Stefan Zahnd and adds that “some administrative work is needed, for example, when we connect new data sources or for tuning and optimizing the system.”

The heart of QRadar SIEM is a highly-scalable database that records real-time log and network transmission data to expose evidence of potential attacks. QRadar SIEM is an enterprise solution that records log event data from thousands of components distributed throughout the network. Each activity is documented in its original format then linked with other events to identify contexts and thus distinguish real threats from false positives. In addition to this, Deep Packet Inspection technology is used to record layer 4 network transmission data in real time and layer 7 application data – a feature which certainly demonstrates the quality of the solution.

QRadar SIEM from IBM

The QRadar security solution from IBM consolidates event data from the logs of thousands of end points and applications throughout the network. The solution carries out immediate normalization and correlation processes on raw data to distinguish between real threats and false positives. QRadar may optionally integrate the IBM Security X-Force Threat Intelligence function and therefore the list of potentially destructive IP addresses such as malware hosts, spam sources and other security threats. IBM Security QRadar SIEM also correlates system weak spots with event and network data to enable the prioritized identification of security-relevant breaches.

The University of Bern

The University of Bern is a full-scale university with eight faculties and around 160 institutions. Its roots stretch back to the 16th century. With 17,300 students, it is one of Switzerland’s largest universities (after the University of Zurich and ETH Zurich). The university therefore remains manageable in size and enjoys a personal atmosphere. The University of Bern is involved in several European and global research projects, one of which involves space exploration.

Business Partner IBM™

eb-Qual Simply Secure

Main Office: eb-Qual SA
Route André-Piller 33A
CH-1762 **Givisiez**
T +41 26 407 70 80
F +41 26 407 70 99

Swiss German Office: eb-Qual AG
Oberfeldstrasse 20
CH-8302 **Kloten**
T +41 43 211 47 20
F +41 43 211 47 29