CASE STUDY KAREL ENGLIŠ COLLEGE

Karel Engliš College, a private Czech college offering bachelor's degrees, administers a complex network infrastructure in two locations with more than 400 students and 60 employees. The college deployed GREYCORTEX MENDEL.

Challenges

The college identified the following main challenges for GREYCORTEX MENDEL:

- Deployment on a university environment with open and benevolent policies
- A range of threats related to student behavior
- Integration with IBM QRadar SIEM
- Network running mostly on IPv6
- A combination of network traffic analysis and Netflow analysis, at the same time

Before GREYCORTEX MENDEL's deployment, Karel Engliš College had implemented a SIEM solution to improve the security and visibility of its IT operations. Because SIEM requires various inputs, GREYCORTEX MENDEL provided valuable outputs for further analysis.

Challenges

- Deployment on a university environment
- Installation on non-standard hardware
- Threats related to student behavior
- Integration with IBM QRadar SIEM
- IPv6 Network
- ASNM + Netflow processing

Advantages

GREYCORTEX MENDEL is based on a combination of various types of detection technologies:

- An Intrusion Detection System, including deep packet inspection which provides detection of unwanted applications like torrents, P2P clients, and malware
- Network Behavior Analysis based on the principles of artificial intelligence and machine behavior, this analysis provides an overview of network attacks like brute-force or trojans which engage in periodic communication
- Network Performance Monitoring (NPM) and Application Performance Monitoring (APM) detect performance issues of the network traffic and network applications
- Event correlation and risk assessment highlight the most critical issues
- A detailed description of network flows through Advanced Security Network Metrics protocol

GREYCORTEX MENDEL focuses on symptoms of attack, irrespective of the attack vector or method. Artificial intelligence, machine learning, big data analysis, and unique algorithms help detect security breaches and other behavioral anomalies in early stages.

Advantages

- Intrusion detection system including deep packet inspection
- Network Behavior Analysis
- Network Performance Monitoring & Application Performance Monitoring
- Event correlation and risk assessment
- ASNM protocol

Results

GREYCORTEX MENDEL helped achieve the following:

- Faster detection of security breaches
- Effective enforcement of policies across the network
- Alerts about inbound attacks on the college's infrastructure
- Identification of weak points in the IT security

Results

- Accelerated detection of security breaches
- Enforcement of network policies
- Early alerts for inbound attacks
- Identification of weak points

Most Beneficial Features of MENDEL

Karel Engliš College found the following capabilities to be the most beneficial:

- MENDEL was easy to use
- Especially wide filtering options
- User-configurable views were greatly appreciated by the staff
- Integration with SIEM
- Elimination of false positive alarms
- The ability to detect both known and unknown threats