CASE STUDY EU FINANCIAL CORPORATION

The client is a European-based financial corporation providing multiple financial products for almost 10 million individual clients in more than 10 countries in Europe and Asia. The company administers a complex and diversified network infrastructure serving more than 50,000 employees in more than 1000 physical locations.

Advanced Security Monitoring in a Complex Network

Prior to the implementation of GREYCORTEX MENDEL the Corporation identified its main challenges:

- Insufficient network threat detection inside the network perimeter
- Insufficient monitoring of internal security policies and detection of suspicious network behavior
- Lack of forensic analysis tools

The network is highly diversified in terms of the types of devices and the number of network segments. It is rapidly expanding and there is high fluctuation in the number of users, with hundreds of new devices owned and administered by corporate subsidiaries, and more importantly, a very diverse portfolio of business partners (from sole entrepreneurs to corporations).

The Corporation had previously implemented a relatively **robust IT security infrastructure** that proved to be incapable of providing optimal answers to these challenges.

- The **firewalls** and signature-based **intrusion detection** at the perimeter could not detect internal threats and threats that entered the network via devices infected outside of the network perimeter. Moreover, the signature-based detection was limited to detection of known threats.
- Simple **NetFlow collection and analysis** had been implemented, but it provided limited anomaly detection capabilities that were sufficient for the network administration, but not for the IT department (e.g. detection of abnormal user behavior and breaches of security policies).
- Together with **SIEM** and flow processors, these technologies provided a very powerful security insights into the network (e.g. what data are flowing, what apps are used). However, the network was missing a robust network behavioral analysis capability which would boost the SIEM capabilities was missing.
- The Corporation was challenged by uncertainty as to whether the NetFlow collection or the SIEM provided sufficient context and contextual data for forensic analysis, and by security incident investigation, which proved to be inflexible and time-consuming.

The Corporation Considered, then **Rejected Several Technologies**

- Network threat detection based on behavioral analysis in **sandboxes** was considered. Given the Corporation's demands for network bandwidth, and its complicated network topology, this option would have seen overly expensive.
- A dedicated **tool for forensic analysis** based on recording all network packets (TCP dump) was ruled out because it would not meet EU traffic interception rules.
- Several other dedicated tools for forensic analysis were considered but proved to provide a low added value.

Robust Behavioral Analysis and Other Advantages

GREYCORTEX MENDEL provided an optimal answer to the Corporation's challenges:

- MENDEL's behavioral analysis engine is particularly effective against advanced unknown threats and for the detection of suspicious network behavior, while keeping operational costs down. In contrast to the vast majority of other behavioral analysis tools, it is not dependent on manual rules set (thresholds). A set of specific rules is automatically generated and continuously adapted based on normal network behavior (of the entire network, each subnetwork, host, and service).
- Several unique specialized detection algorithms are used to detect remote access trojans (RATs) and several other advanced threats. This detection is based on similar behavior profiles (e.g. machine-like behavior that is different from human behavior).
- MENDEL's signature-based engine detects threats inside the network, at the network perimeter, providing additional layers of security to the primary IDS.
- Apart from NetFlow, MENDEL also analyzes network communication metadata and stores it for six to nine months (more with additional storage). This provides contextual

Challenges

- Insufficient detection of network threats inside the network perimeter
- Insufficient monitoring of internal security policies and detection of suspicious network behavior
- Lack of tools for forensic analysis
- A highly diversified and complex network

Inability to address the challenges with present IT security infrastructure:

- Firewalls and an intrusion detection system at the perimeter
- Simple NetFlow collection and analysis
- SIEM and flow processor

Several technologies considered proved to be too costly or with little value added:

- Behavioral analysis in sandboxes
- Dedicated forensic tools

Implementation

- Behavioral analysis engine with automatic generation and adaptation of rules based on normal network behavior
- Unique algorithms for the detection of RATs
- Signature-based detection engine provides an additional layer of security both inside the network and at its perimeter
- NetFlow and metadata of network traffic stored for forensic analysis

and content awareness that is crucial for forensic analysis (while avoiding the legal problems associated with unlawful surveillance and making relatively low demands on storage capacity).

GREYCORTEX MENDEL was deployed in order to analyze all available traffic from network segments at the headquarters layer and at the perimeter (three probes and one collector were deployed). Additionally, the security department utilized the opportunity for role-based access control for network administrators of corporate subsidiaries and business partners. This gave administrators have more security awareness of their network segments.

Better Detection and Faster Incident Response

GREYCORTEX MENDEL provided high added value in several aspects.

- The risk assessment capabilities of MENDEL helped the department stay more focused and greatly improved its operation, both in time savings while executing a range of important tasks, and in producing better and faster incident responses.
- With its robust and easy browsing and filtering, security incidents were analyzed with little time investment.
- GREYCORTEX MENDEL quickly proved its effectiveness and capability. It reported several serious security incidents (see table below), both at the network perimeter and inside the network which were easily investigated which received quick responses from the Corporation's IT team.

In addition to the main needs of the client, access to the MENDEL user interface for lower level administrators helped to greatly to improve communication between network administrators and the security department both within the Corporation, and in its subsidiaries and business partners. These network administrators could be included in the investigation and response of incidents with greatly improved work efficiency as a result.

Results

MENDEL's Added Value:

- More focused and efficient work in the IT security department
- Early detection and easy investigation of serious security incidents (see table below)
- Improved investigation and incident response due to easier communication with lower-level network admins

Summary of Detected Threats by Method

Security Incident	Signature-based Detection (IDS)	Detection Using Behavior Analysis (NBA)
Unknown malware Remote access trojan	--	Machine-like behavior Predictable communication patterns
Breach of an internal security policy P2P data sharing	--	Behavioral anomaly Higher than usual number of communication peers and higher than usual data volume at a port
Network reconnaissance Aimed at an HTTPS application	--	Web attack algorithms More factors
Breach of an internal security policy (3rd party app. sending data to an ext. network	--	Behavioral anomaly Anomalous communication with external hosts
Variant of known malware Conficker	Known data signature (A signature different to those used by the primary IDS)	Machine-like behavior Periodic communication
Variant of known malware Troj/VB-GXP		--