The Security Operations Center—Current state and plans for the future security center

- The Security Operations Center (SOC) is a central operation for managing and coordinating threats.
- It focuses on threat hunting, triage, and response.

A Year at Ransomware

- In Q3 2015, there were 215% more ransomware samples compared to Q2 2016. This trend continued at a high rate.
- The number of ransomware samples has grown 32% in the past quarter.

- The most significant technical advancements of 2016 included:
  - Exploit kits and ransomware delivery.
  - More sophisticated ransomware attacks.

Threat Statistics

- In Q3 2016, there were 32 million ransomware samples.
- The number of ransomware samples dropped 97% in Q3 but 21% from Q2.

- McAfee GTI received on average 44.1 billion queries per day.
- Almost nine out of 10 companies have a SOC.

Malware Global Threat Intelligence

- In Q3 2016, there were 138 million new malware samples.
- There were 19% more malware samples compared to Q2 2016.

Ways to Trojanize legitimate software:

- Rogue Apps
- Ransomware
- Adware
- Malvertising

McAfee GTI protections against malicious URLs and 93% are relevant threats.

McAfee GTI protections against risky IP adresses showed a slight decrease.

The security industry fought back.

- A new wave of tools and services providers were available.
- Vendors offered prevention advice, decryption tools, and optimized security operations.

Ransomware Delivery:

- The most common methods included:
  - Exploit kits
  - Malicious websites
  - Phishing emails

Ransomware Technical:

- The most common techniques used were:
  - Malware families
  - New macro malware
  - Macro malware

- The number of new malware samples grew 215% in the past year.