6.5: Security Operations Centers

Besides the tools and practices discussed earlier to protect ourselves, companies also have increased their investment to fight against cybercrime. One such investment is a dedicated center called Security Operations Center to safeguard companies from internal and external threats.

Elements of a SOC

Defending against today's threats requires a formalized, structured, and disciplined approach that is carried out by Security Operations Centers professionals who work closely with other groups such as IT or networking staff. SOCs offers a wide variety of services tailored to meet customer needs, from monitoring and compliance to comprehensive threat detection and hosted protection. SOCs may be wholly in-house, owned and run by a company, or security providers, such as Cisco Systems Inc.'s Managed Security Services, may be contracted to elements of a SOC. The key elements of a SOC are individuals, processes, and technology.

A great way to fight against threats is through Artificial Intelligence (AI) and machine learning. AI and machine learning use multi-factor authentication, malware scanning, and fighting spam and phishing to fight against threats.

Process in the SOC

SOC professionals monitor all suspicious activities and follow a set of rules to verify if it is a true security incident before escalating to the next level severity for the incident for appropriate security experts to take appropriate actions.

The SOC has four principal functions:

- Use network data to check the security warnings
- Evaluate accidents that have been checked and determine how to proceed
- Deploy specialists to evaluate risks at the highest possible level.
- Provide timely communication by SOC management to the company or clients

Technologies deployed in the SOC

- Event collection, correlation, and analysis
- Security monitoring
- Security control
- Log management
- Vulnerability assessment
- Vulnerability tracking
- Threat intelligence

Enterprise and Managed Security

The organization will benefit from the implementation of an enterprise-level SOC for medium and large networks. The SOC could be a complete solution within the company. Yet many larger organizations will outsource at least part of the SOC operations to a security solution provider such as Cisco Systems Inc.
