# Security Operations

Matthew Edwards

Focus: Threat Modelling

September 13, 2020

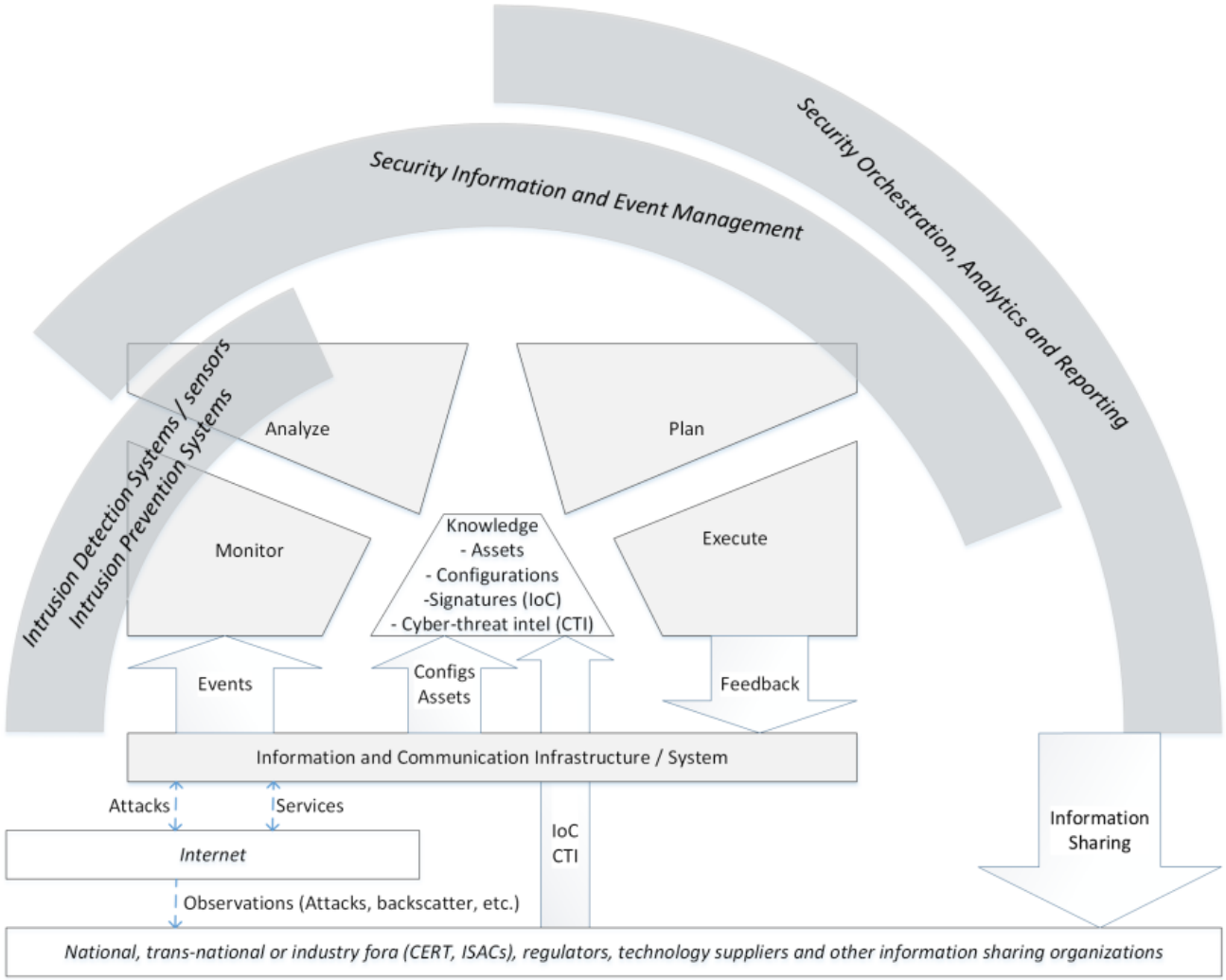
# Constant vigilance

Security is (unfortunately) not a case of ‘protect & forget’.

Systems need to be constantly monitored for intrusions.

We need to understand what is going on inside and outside our system in order to prevent attacks.

# MAPE-K




[1]H. Debar, "Security operations knowledge area," in Cyber Security Body of Knowledge, 2019.

# Monitor

Generally, monitoring is achieved through a combination of technical controls.

| | |
|---|---|
| System | File access, system and kernel event logs, e.g., syslog. |
| Network | Highly granular (pcap) or aggregated (Netflow). |
| Application | Application-level (e.g., web server) logs. |

Also includes human **reporting**.

# Analyse

Two general approaches:

## Misuse Detection

Search for patterns matching **known malicious events** in the logs.

## Anomaly Detection

Analyse logs for **anomalous deviations** from ordinary behaviour.

# Plan

The responses to attacks need to be planned.

**Risk** can be thought of as

- Assets to be protected;
- Risks inherent to the industry;
- Countermeasures in place already;
- The threats this organisation in particular faces.

A SOC needs to go through **performance appraisal**.
Rather than incident-based, this is based on *preparedness*.

# Execute

**Prevention**

Targeted countermeasures to halt an ongoing attack.

May need to be automated through an **Intrusion Prevention System**.

**Recovery**

Responses to rebuild security after an attack. Can be dependent, but should usually include investigation to find:

1. How the attackers got in;
2. Whether they left any backdoors open.

# Knowledge

CTI *Cyber Threat Intelligence*. Organisations that run **honeypots** and share information on threats and IoC between affected organisations.

IoC *Indicators of Compromise*. Patterns that indicate an ongoing, imminent or previous attack on your system.

CERT *Computer Emergency Response Team*. Share information on threats, but also best practices.

# Knowledge: Common Vulnerabilities and Exposures

Most commonly referred to as **CVE**. Paired with **CVSS**, the *Common Vulnerability Scoring System*. Acts as a common dictionary for known software vulnerabilities.

At a higher level, the **CWE** describes weaknesses in software authorship that lead to vulnerabilities.

**MITRE CVE Database**

Accessible at `https://cve.mitre.org/`.

# Knowledge: CAPEC

The **Common Attack Pattern Enumeration and Classification** framework. Classifies and describes attack patterns at a high level, with links to supporting weaknesses.

MITRE CAPEC Database

Accessible at `https://capec.mitre.org/`

# Knowledge: ATT&CK

Reference framework for **Adversarial Tactics, Techniques and Common Knowledge** – describing the specific actions an attacker takes while operating in a network. Covers groups of ongoing concern to the security community.

## MITRE ATT&CK Database

Accessible at `https://attack.mitre.org/`