

Introduction To Blue Team

BLUE
VS
RED





CYBERSECURITY BLUE TEAM

ปกป้ององค์กรทุกภัยไซเบอร์

SOC (Security Operations Center)



107,050

- Total -

0

- Level 12 or above alerts -

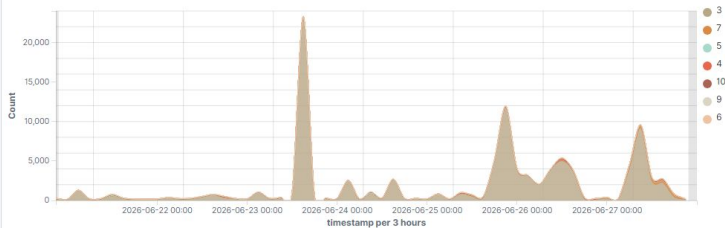
2

- Authentication failure -

123

- Authentication success -

Top 10 Alert level evolution



Top 10 MITRE ATTACKS

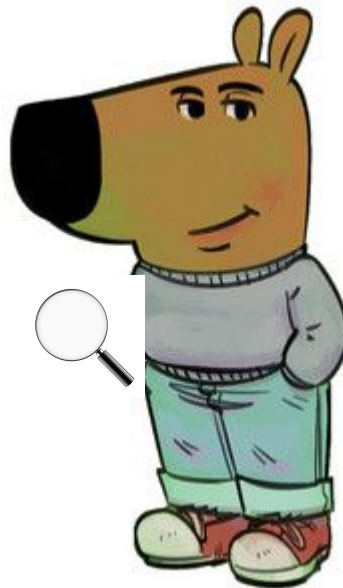
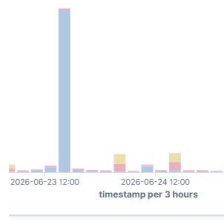


Top 5 agents

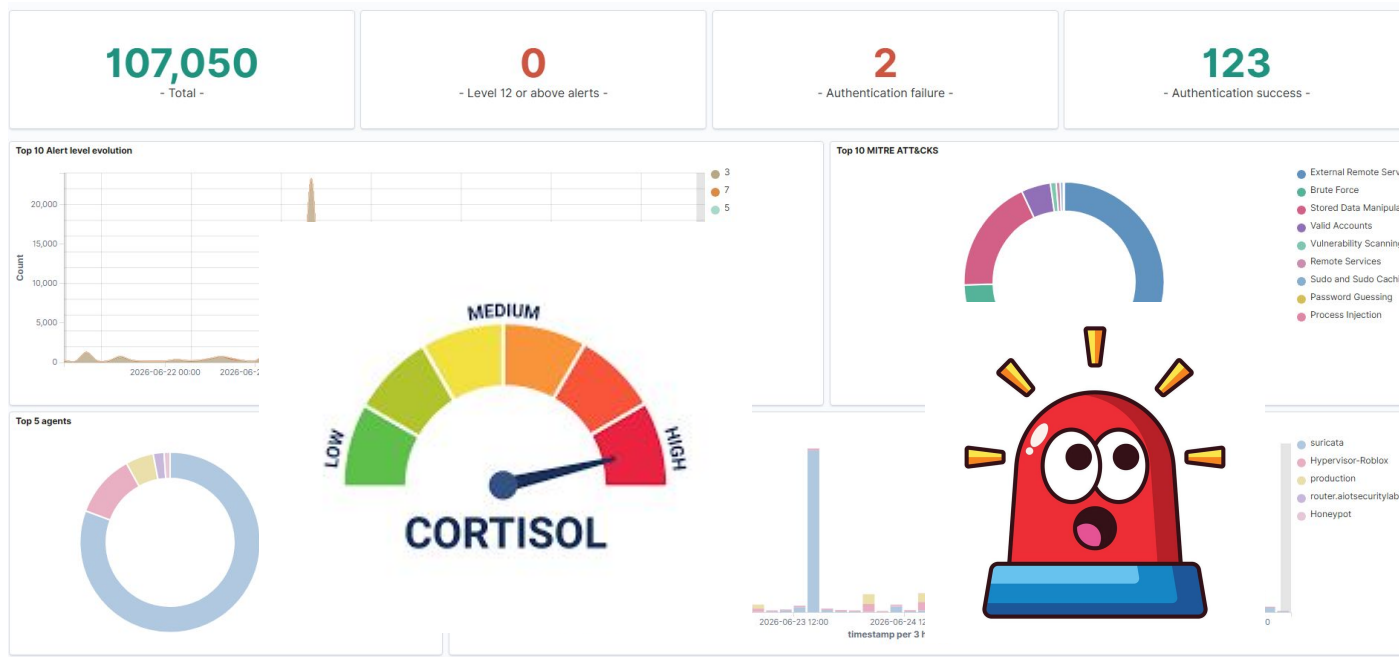


Alerts evolution - Top 5 agents

CORTISOL LEVEL

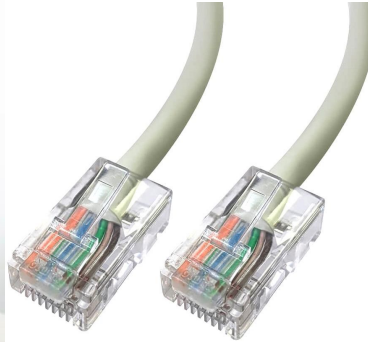


Monitor

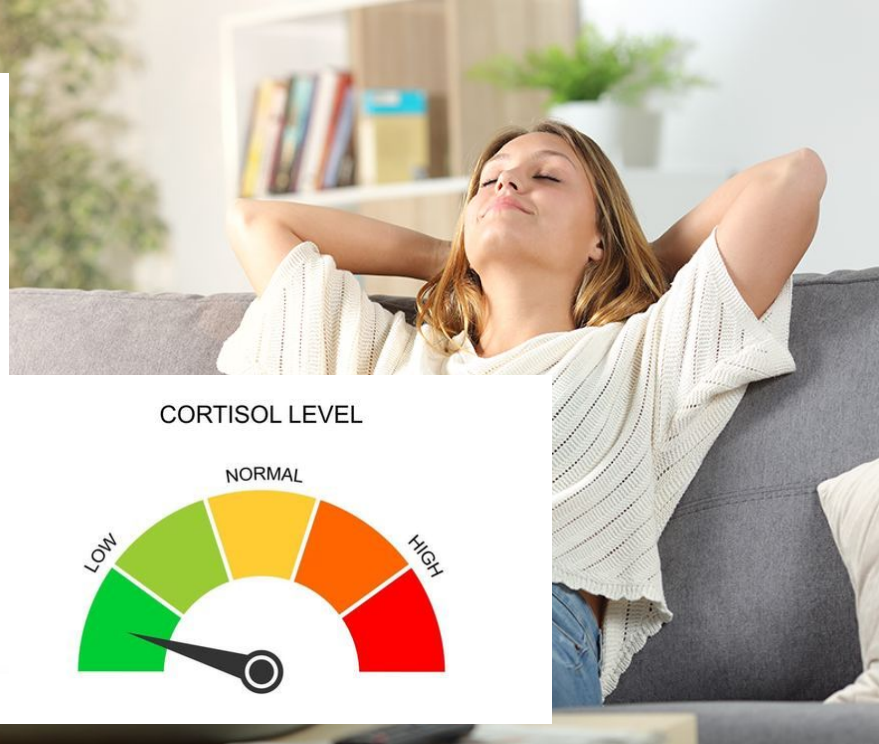
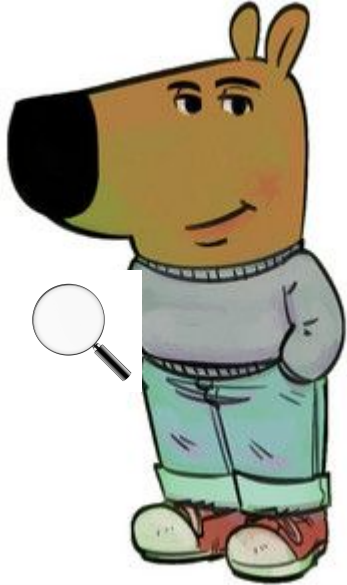


Detect

Response



- SOC's analysis tier I



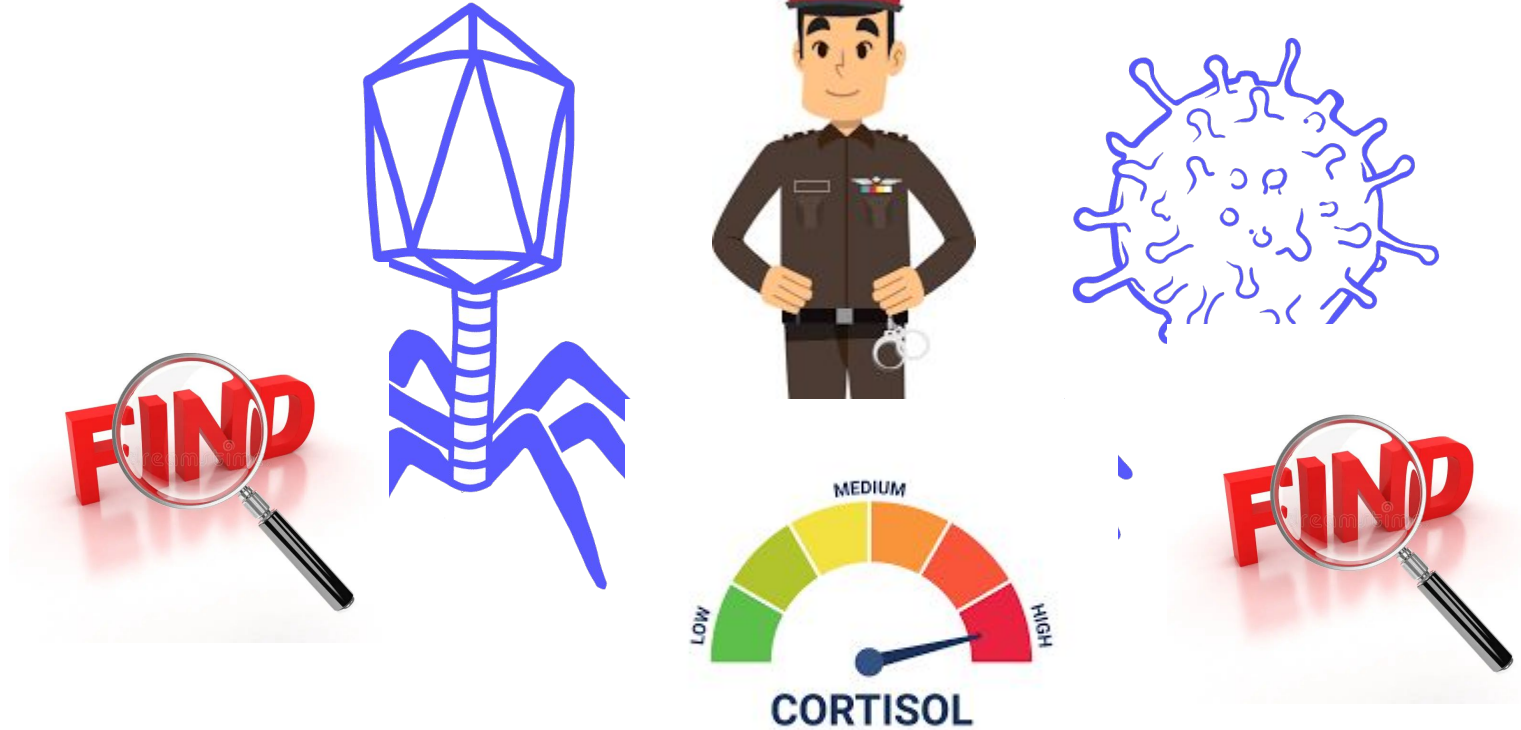


- Threat hunter

- Incident Responder



- Forensic analyst

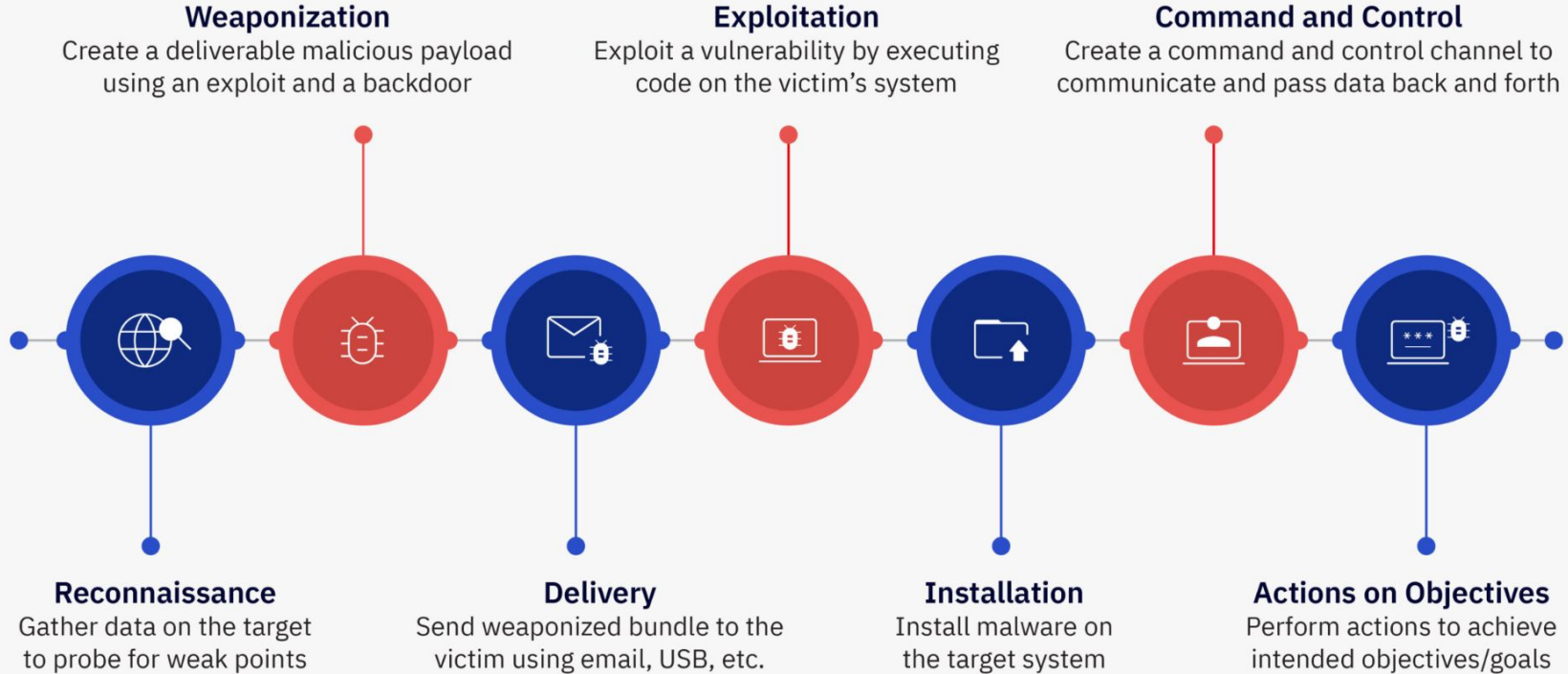




Cyber Kill Chain

Cyber Kill Chain

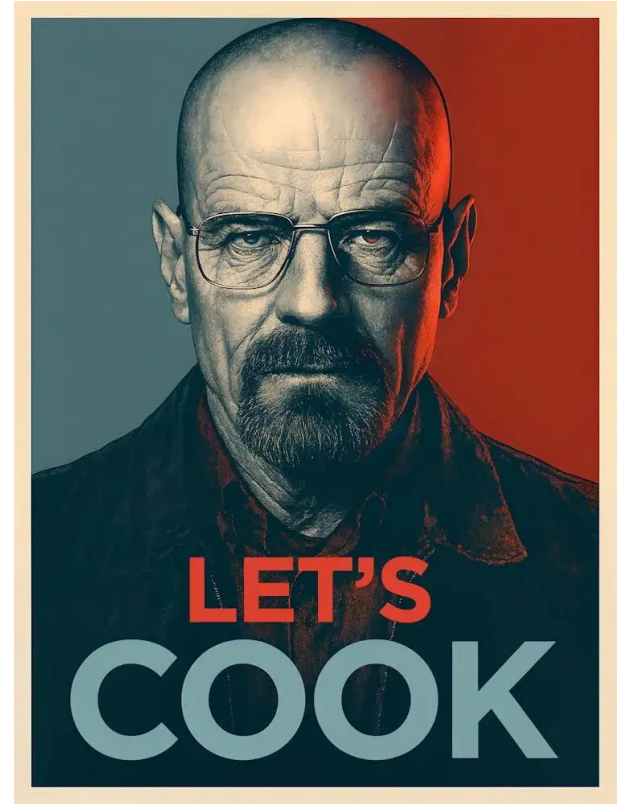
UIH

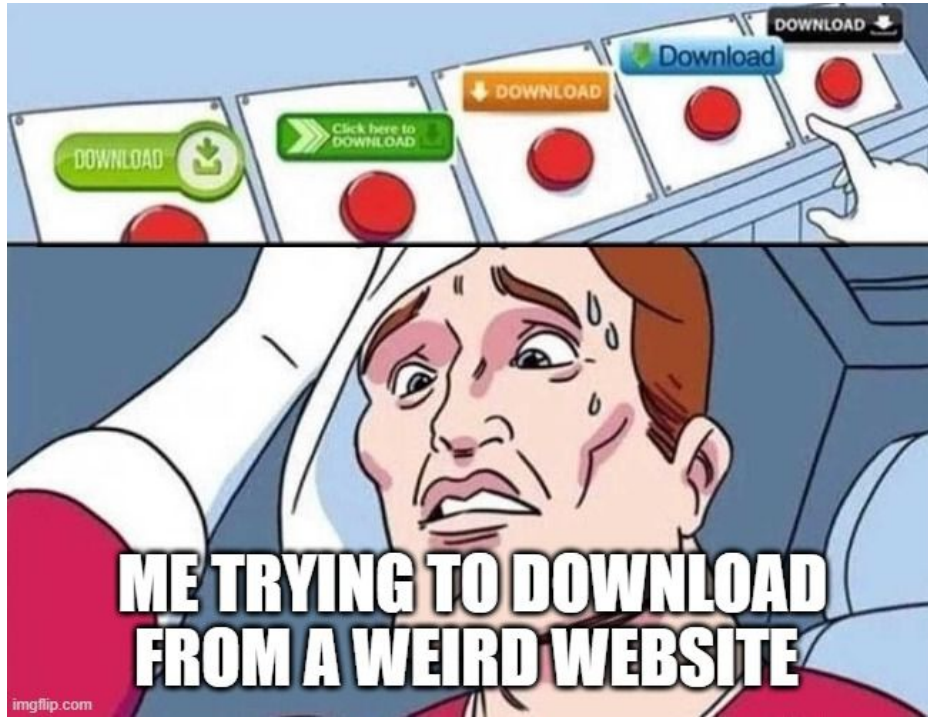




Reconnaissance

Weaponization





Delivery

Exploitation





Installation

Command & Control

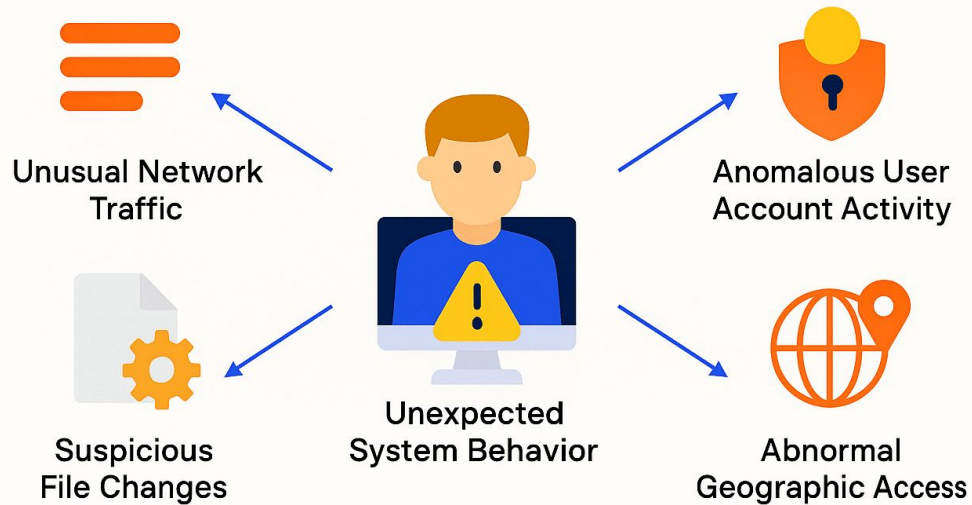


Actions

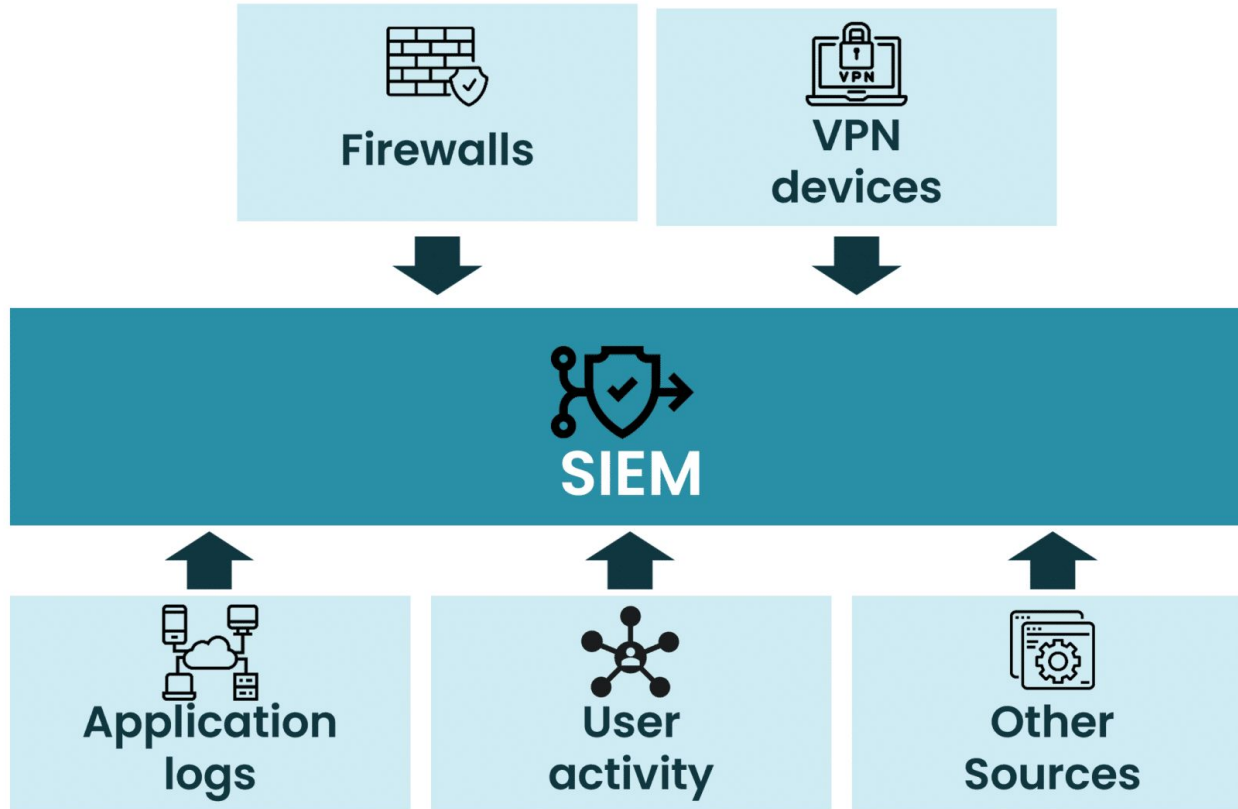
Threat Detection

IOC (Indicator of Compromise)

Common Examples of Indicators of Compromise



SIEM (Security Information and Event Management)

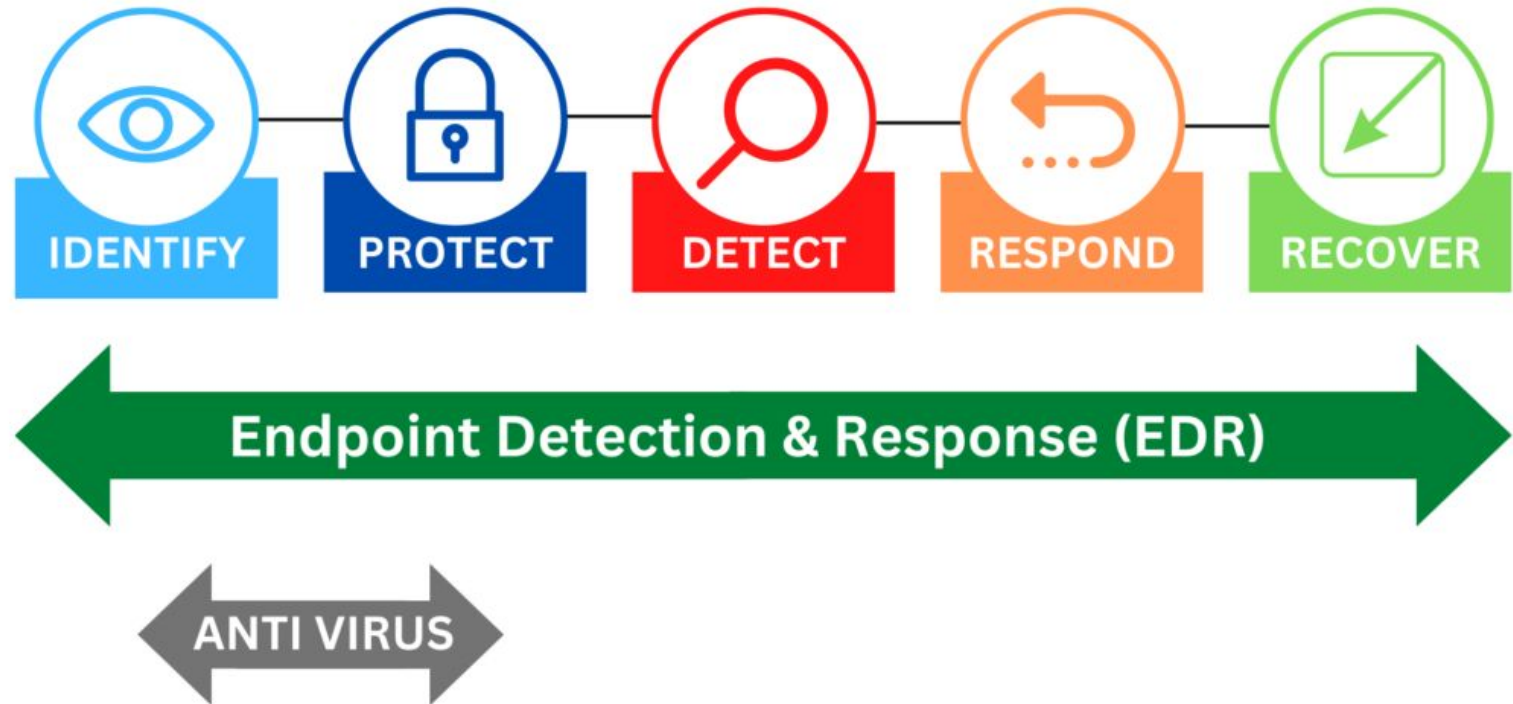


6 Steps of an Incident Response

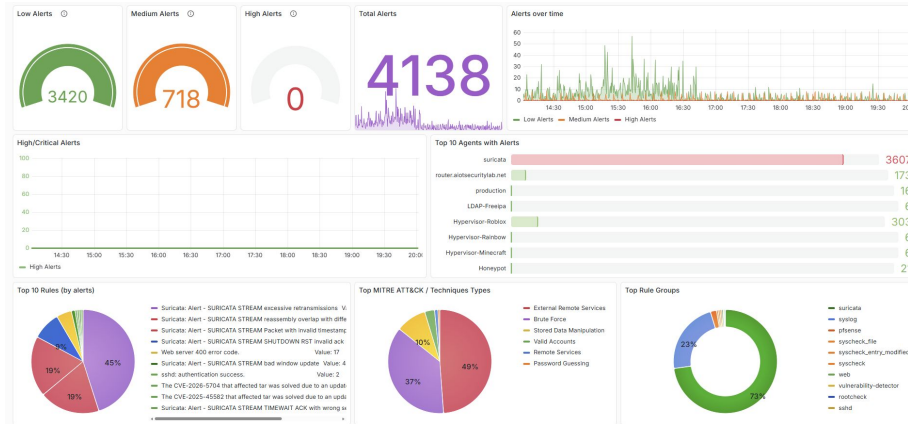


Tools

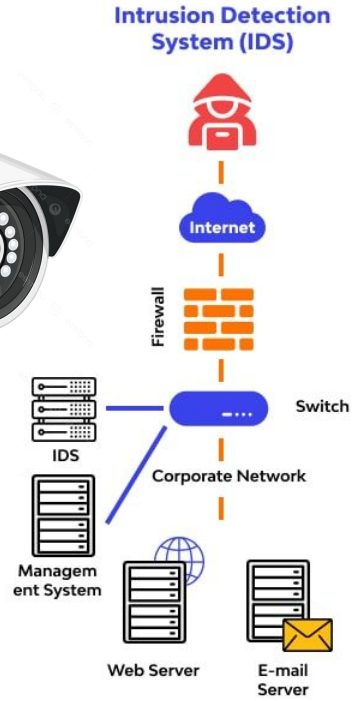
EDR



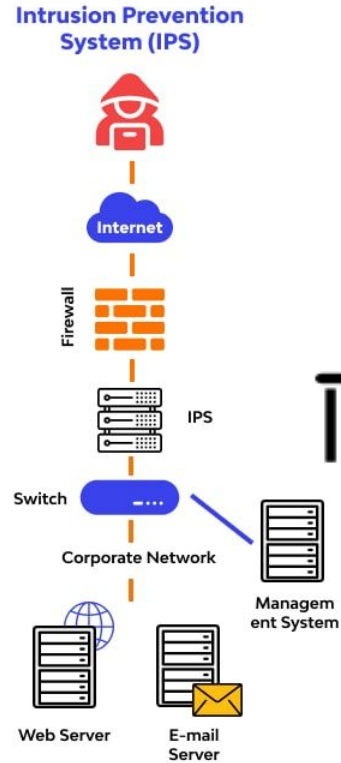
SIEM (Security Information and Event Management)



IDS/IPS



VS



Honeypot



Purple Team



