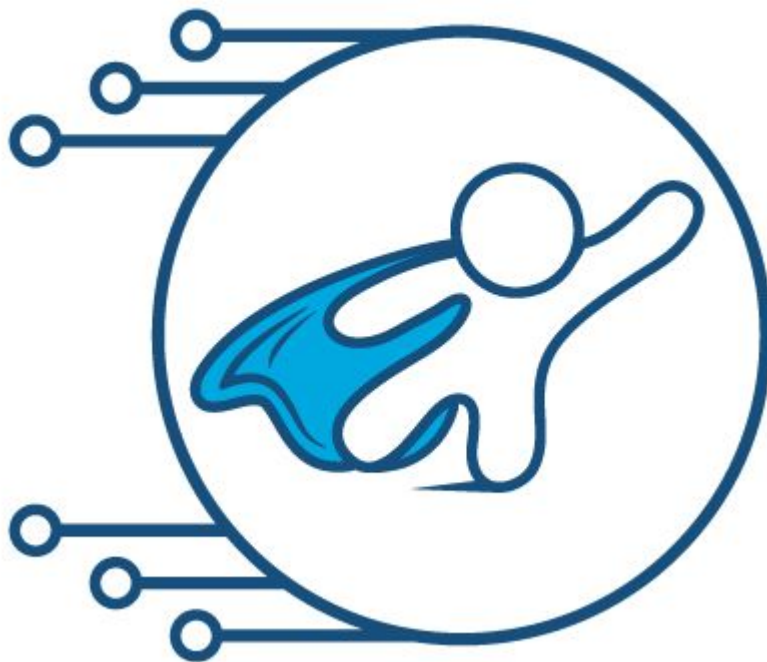


Blue Teams



INFOSEC WHEEL





BLUE TEAM

- ✓ **Defensive Security**
- ✓ **Infrastructure protection**
- ✓ **Damage Control**
- ✓ **Incident Response(IR)**
- ✓ **Operational Security**
- ✓ **Threat Hunters**
- ✓ **Digital Forensics**



Definition



*“A **blue team** is a group of individuals who perform an analysis of **information systems** to ensure security, identify security flaws, verify the effectiveness of each security measure, and to make certain all security measures will continue to be effective after implementation” - Wikipedia*

Advantage of the Attacker

OBJ

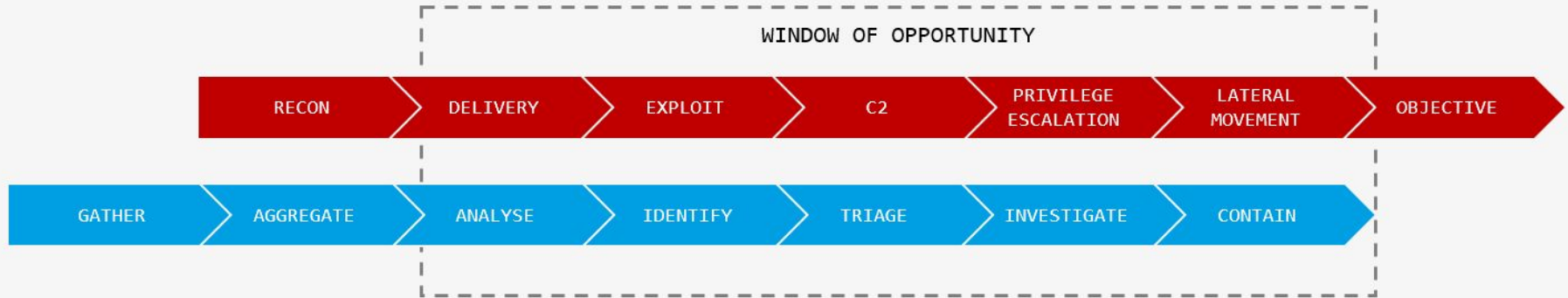


- Attacker must succeed once!**
- Attacker can choose the weakest spot**
- Attacker can leverage zero-days**
- Attacker can play dirty**



- Defender must get it right all the time**
- Defender must defend all places**
- Defender can only defend against known attacks**
- Defender needs to play by the rules**

Blue team Incident workflow



The 5 phases in the incident response plan

1. Preparation
2. Detection & Analysis
3. Containment, Eradication, Recovery
4. Post-Incident Review
5. Update the plan !



Phase 1: Preparation

Condensed steps to prep and create a plan

1. Identify and prioritize your assets
2. Identify your potential risks
3. Establish procedures
4. Assemble a response team
5. Train your employees

Phase 1: Preparation

1. Identify and prioritize your assets

Identifying the 'crown jewels'

Identify what would;

- cost the company most financially
- what would create the biggest disruption and
- cause the biggest reputational damage.



Phase 1: Preparation

2. Identify your potential risks

See Lesson 1 - White teams about risk assessment

Phase 1: Preparation

3. Establish procedures

Lists & checklists

- Forensic analysis checklists (customized for all critical systems)
- Emergency contact communications checklist
- System backup and recovery checklists (for all OSes in use, including databases)
- "Jumpbag" checklists
- Security policy review checklist (post-incident)

<https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901>

Phase 1: Preparation

4. Assemble a response team

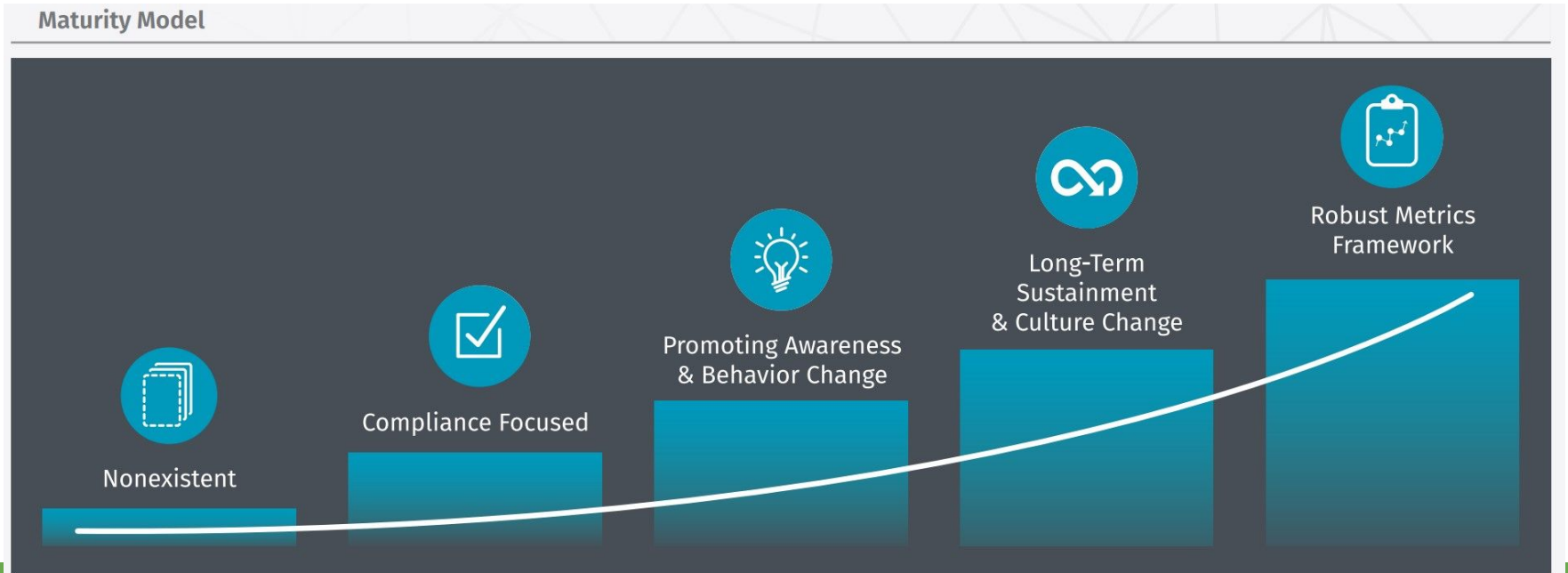
Multidisciplinary & clear about their role

Not only (IT-)Technical people! Think about communication and processes

Phase 1: Preparation

5. Train your employees

Awareness & culture are often overlooked!



Phase 2: Detection

Network Intrusion Detection systems (NIDS)

Intrusion Detection Systems (IDSs) passively monitor the traffic on a network.

- **Signature-based detection**
- **Statistical anomaly-based detection**
- **Stateful protocol analysis detection**

Host Intrusion Detection systems (HIDS)

monitoring all or parts of the dynamic behavior and the state of a computer system.

- Similar to AV
- Disc/process activity
- RAM
- ...

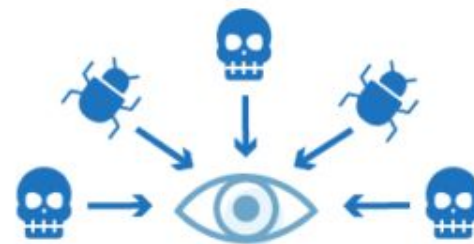
What Does an Intrusion Detection System Do?



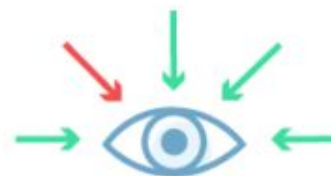
Network Intrusion
Detection



Host Intrusion
Detection



Signature-based
Detection



Anomaly-Based
Detection

Phase 2: Detection

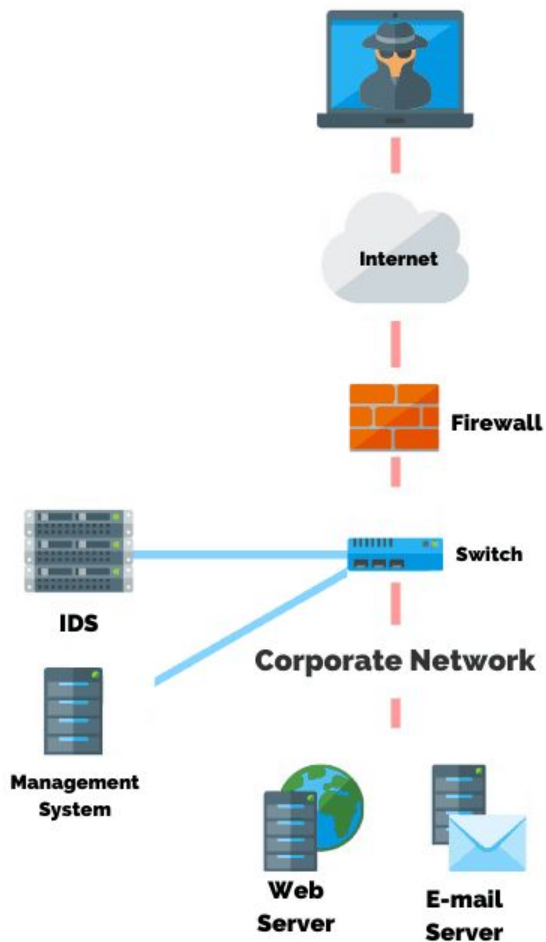
A better solution is to use a device that can immediately detect and stop an attack. An Intrusion Prevention System (IPS) performs this function.

Network Intrusion Prevention systems (NIPS)

Host Intrusion Prevention systems (HIPS)

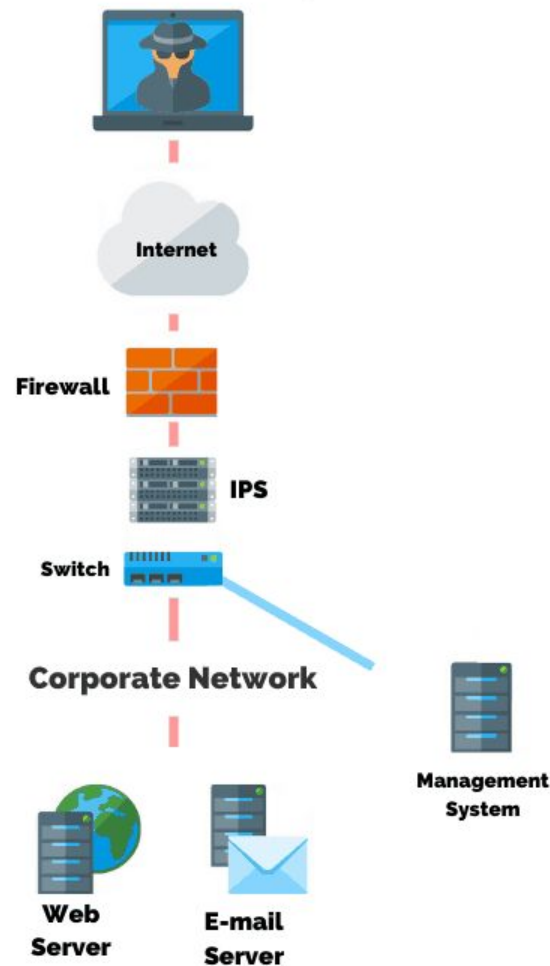
Evolved into -> Endpoint Protection Systems - “AV on steroids”

Intrusion Detection System (IDS)



VS

Intrusion Prevention System (IPS)



Phase 2: Detection

Tool Examples:

NIDS

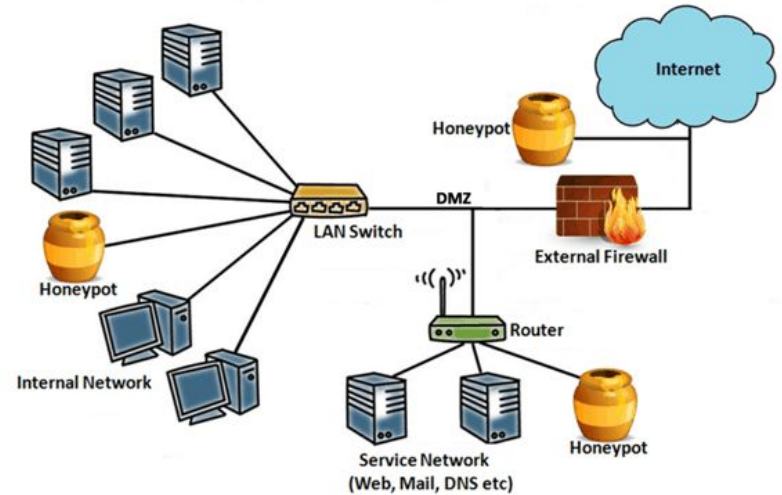
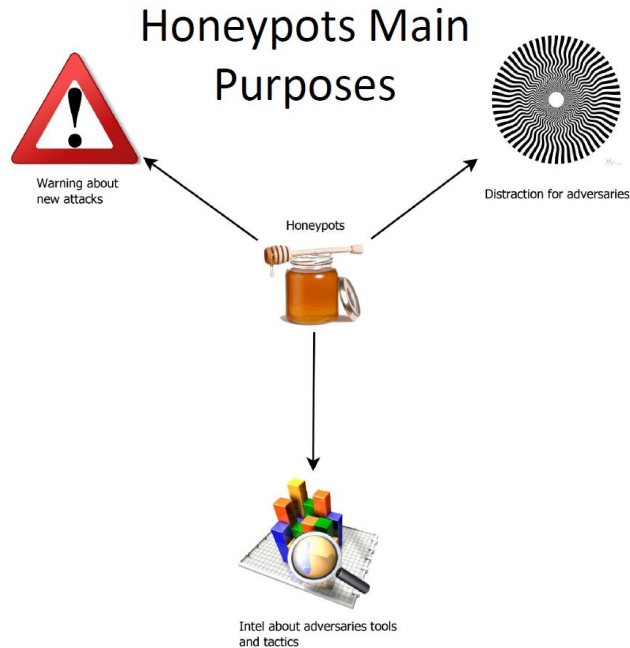


HIDS



Phase 2: Detection

Honeypot



Types of Honeypot

Low-Interaction

- Emulate attractive services such as FTP and SMB)
- Focuses on collecting probes from attackers
- Can't genuinely be compromised, it's merely an emulation
- Easier to identify it as a honeypot

High-Interaction

- Adhere to behavioural norms
- May constitute a "honeynet"
- Attackers can interact with it like a normal machine...
- ...but it collects forensic data in a central repository
- Harder to identify as a honeypot



Phase 2: Detection

Tool Examples:

“Supertools”

Combining it all - Aggregate data and correlate “With AI and Blockchain”



Pluralsight video's



PLURALSIGHT

Pluralsight video: [link](#)

Relevant : Incident Detection and Response: The Big Picture

Pluralsight video: [link](#)

Relevant : Security Event Triage: Detecting Malicious Traffic with Signature and Session Analysis

Pluralsight video: [link](#)

Relevant : Assessing Red Team Post Exploitation Activity

Pluralsight video: [link](#)

Relevant : Ethical Hacking: Evading IDS, Firewalls, and Honeypots