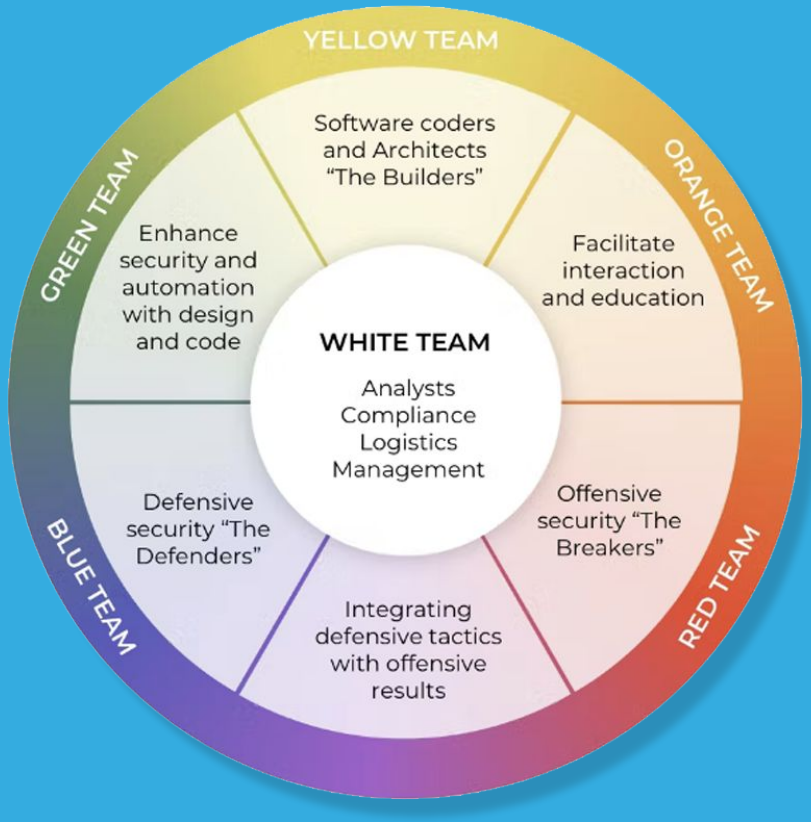
BLUE TEAMS

Deel 1

PXL DIGITAL


YELLOW TEAM
Software coders and Architects "The Builders"
ORANGE TEAM
Facilitate interaction and education
RED TEAM
Offensive security "The Breakers"
Integrating defensive tactics with offensive results
BLUE TEAM
Defensive security "The Defenders"
GREEN TEAM
Enhance security and automation with design and code
WHITE TEAM
Analysts
Compliance
Logistics
Management

PXL DIGITAL

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*

PXL DIGITAL

Advantage of the attacker

Attacker…

… must succeed once!

… can choose the weakest spot

… can leverage zero-days

… can play dirty

Defender…

… must get it right all the time

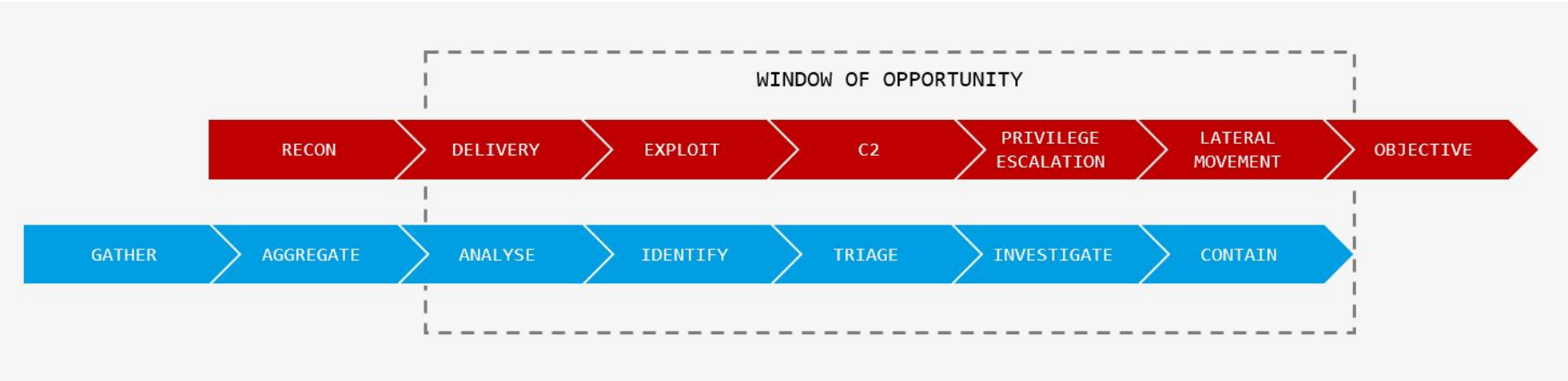
… must defend all places

… can only defend against known attacks

… needs to play by the rules

PXL DIGITAL

BLUE TEAM - Incident workflow



THE INCIDENT RESPONSE PLAN

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

PXL DIGITAL

THE INCIDENT RESPONSE PLAN

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

PXL DIGITAL

PHASE 1

PREPARATION

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

1 - IDENTIFY AND PRIORITIZE YOUR ASSETS

Identifying the ‘crown jewels’.

What would:

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

2 - IDENTIFY YOUR POTENTIAL RISKS

See Lesson 1 - White Teams about Risk assessment

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

4 - ASSEMBLE RESPONSE TEAM

Multidisciplinary & clear about their role

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

5 - TRAIN YOUR EMPLOYEES

Awareness & culture are often overlooked

PHASE 2

DETECTION & ANALYSIS

2 - DETECTION

NETWORK INTRUSION DETECTION SYSTEM (NIDS)

passively monitor the traffic on a network.

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

HOST INTRUSION DETECTION SYSTEM (HIDS)

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

- Disc/process activity
- RAM
- ...

2 - DETECTION

Network Intrusion Detection

Host Intrusion Detection

Signature-based Detection

Anomaly-Based Detection

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.

~ Endpoint Protection Systems - “AV on steroids”

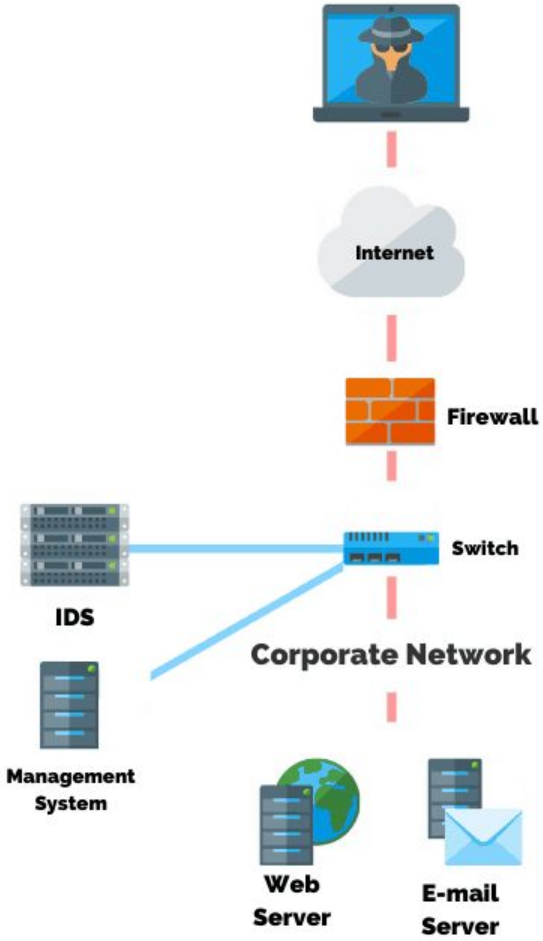
NETWORK INTRUSION

PREVENTION SYSTEM (NIPS)

HOST INTRUSION

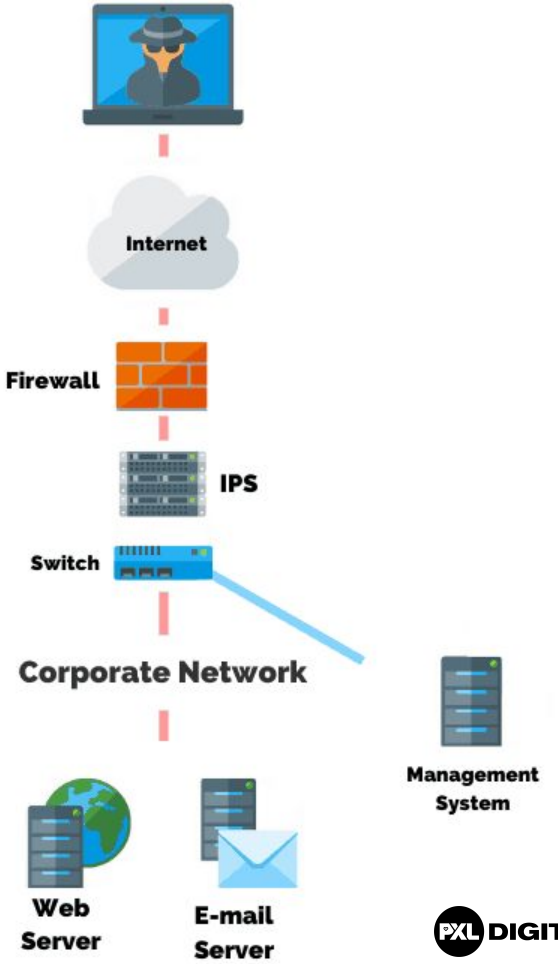
PREVENTION SYSTEM (HIPS)

Intrusion Detection System (IDS)



VS

Intrusion Prevention System (IPS)



PXL DIGITAL

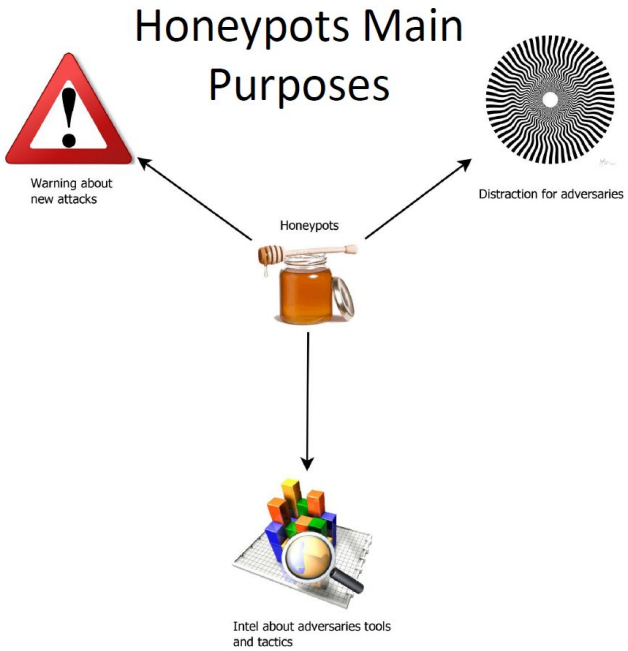
2 - DETECTION

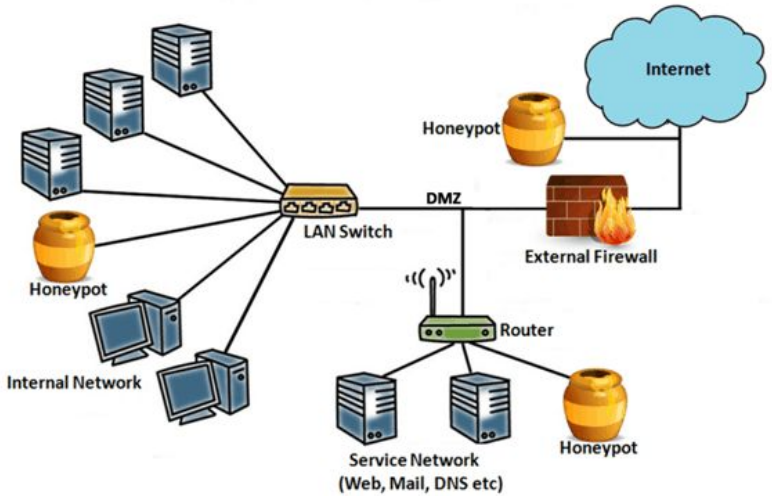
Tool Examples:

NIDS

HIDS

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

2 - DETECTION

“Supertools”

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

PLURALSIGHT VIDEOS

Pluralsight video: link
Relevant : Incident Detection and Response: The Big Picture

Pluralsight video: link
Relevant : Operations and Incident Response for CompTIA Security+

Pluralsight video: link
Relevant : Assessing Red Team Post Exploitation Activity

Pluralsight video: link
Relevant : Ethical Hacking: Evading IDS, Firewalls, and Honeypots

PXL DIGITAL