Orange
Cyberdefense

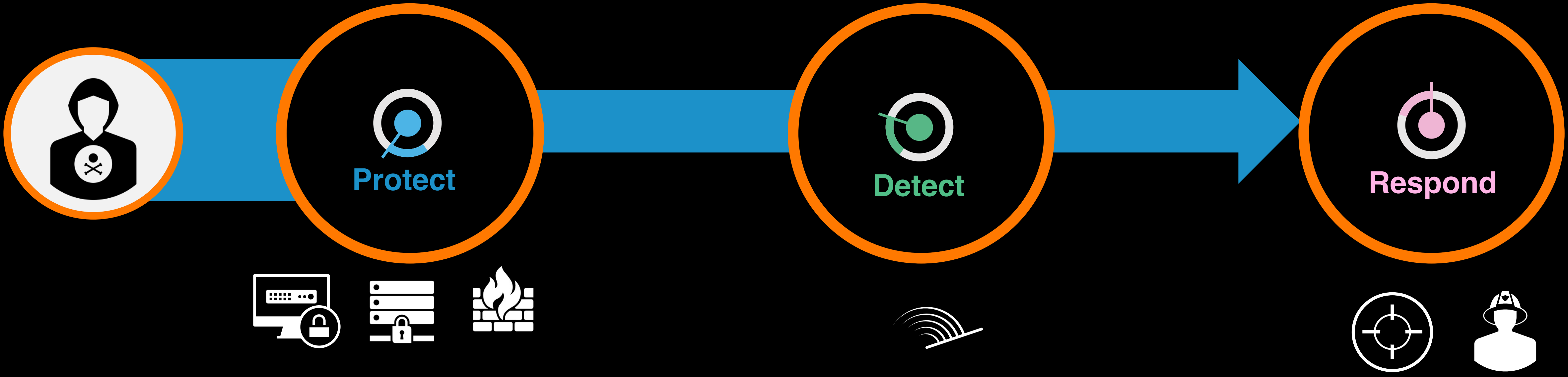
Detection capabilities

What does it mean in the real world?

<date>

orange™

Why is detection and response important?

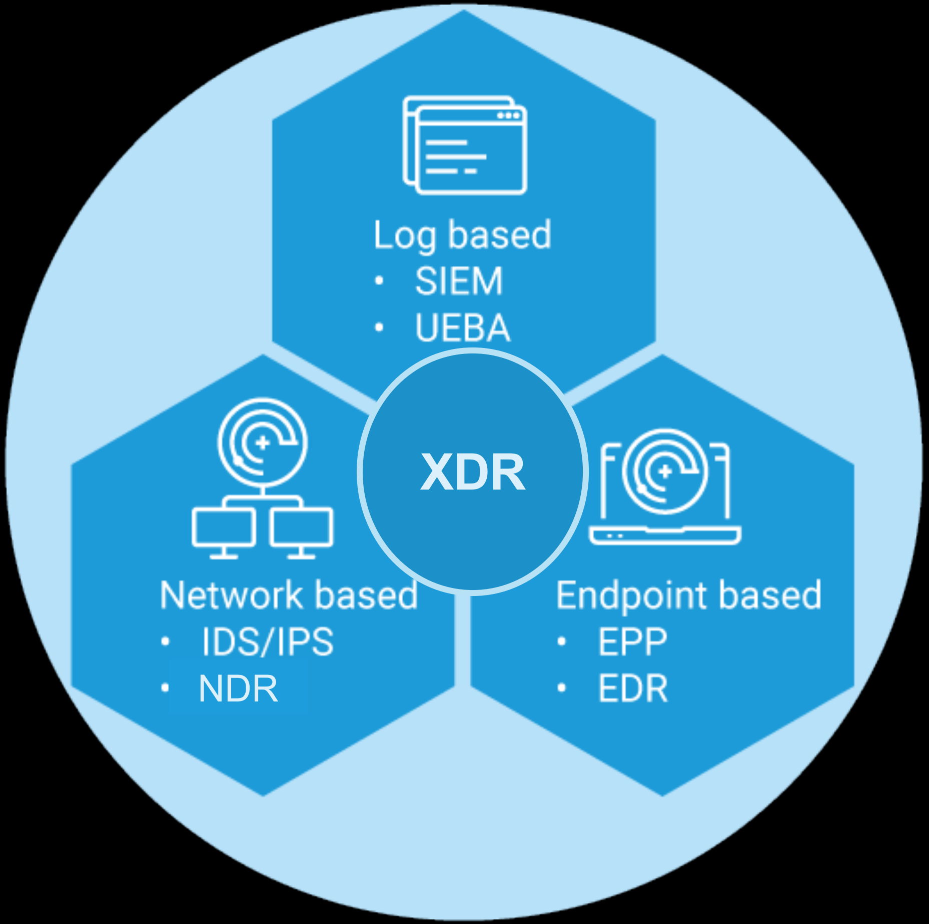


- Firewall
- Antivirus
- Access control
- Security awareness
- Segmentation
- Etc…

- SIEM
- EDR, XDR
- NDR, IDS

- Threat Hunting
- Compromise assessments
- Incident Response

What is the visibility (SOC) triad?



"Many customers fail with their threat monitoring, detection and response initiatives because of the focus on wide-scale collection of data and generic security monitoring.

Instead, they should be focusing on **risks** and **outcomes** that will directly impact their business objectives."

Source: Gartner – Market Guide for Managed Detection and Response services 2021

Key risks addressed by Detection and Response

Intelligence-led security

Secure your endpoints

Your endpoints are central to how your users interact with the business. This makes them a prime target for attacks such as ransomware

Monitor your key business systems

Your networks and collaboration tools are key to connecting your users to each other, to third parties and to applications. They can also be backdoor for stealthy attackers

Detect threats in the Cloud

The cloud enables business agility. But if these resources are compromised, that same agility can be used against you

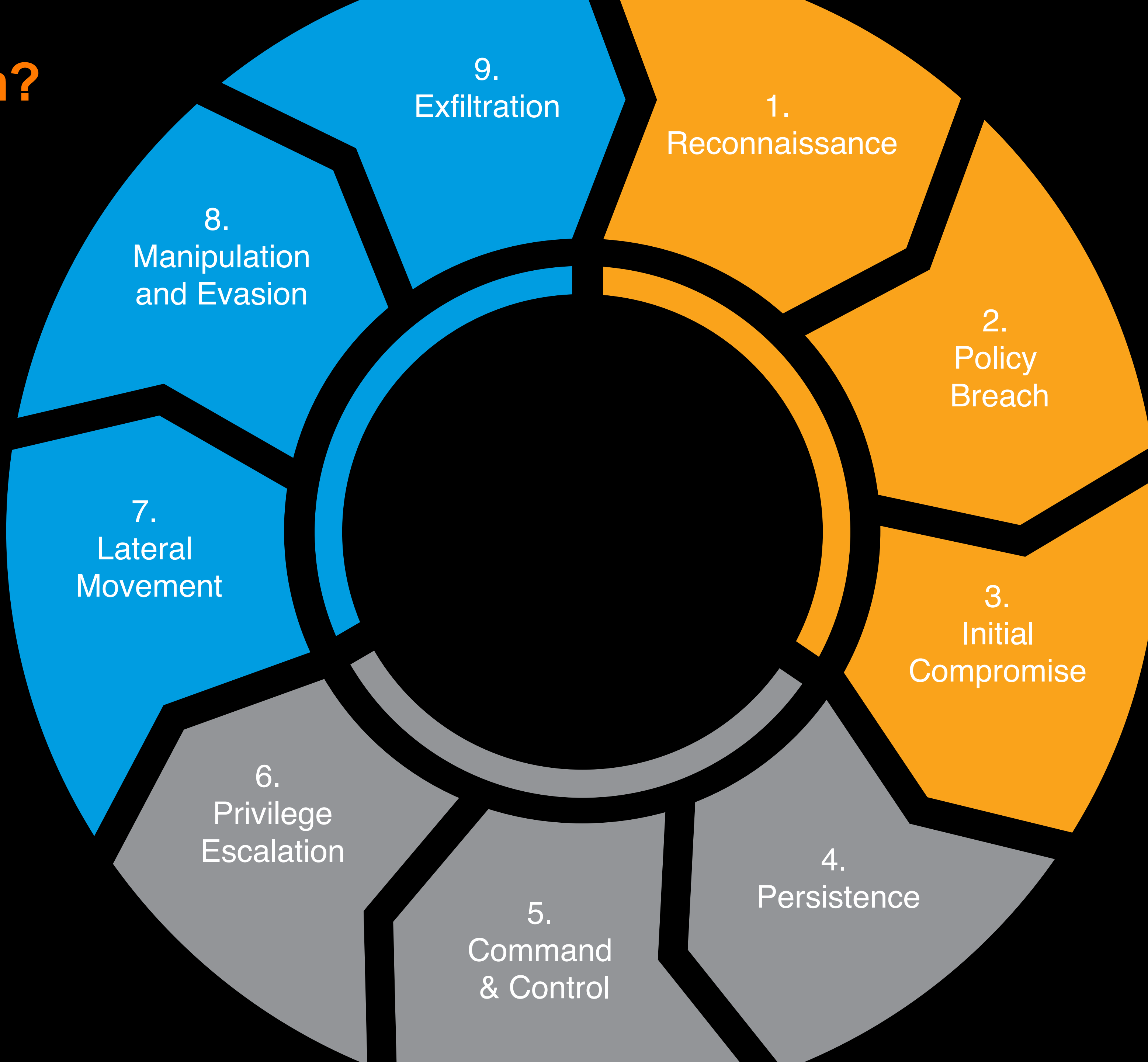
Get visibility of your digital risk

Monitoring the “inside” is not enough, we must also look at the inherent risks of the digital footprint that exists “outside” our business

Prepare to respond to incidents

Cyber security incidents will happen. Being prepared for them gives you the best chance of minimizing the impact

What is the Cyber Kill Chain?



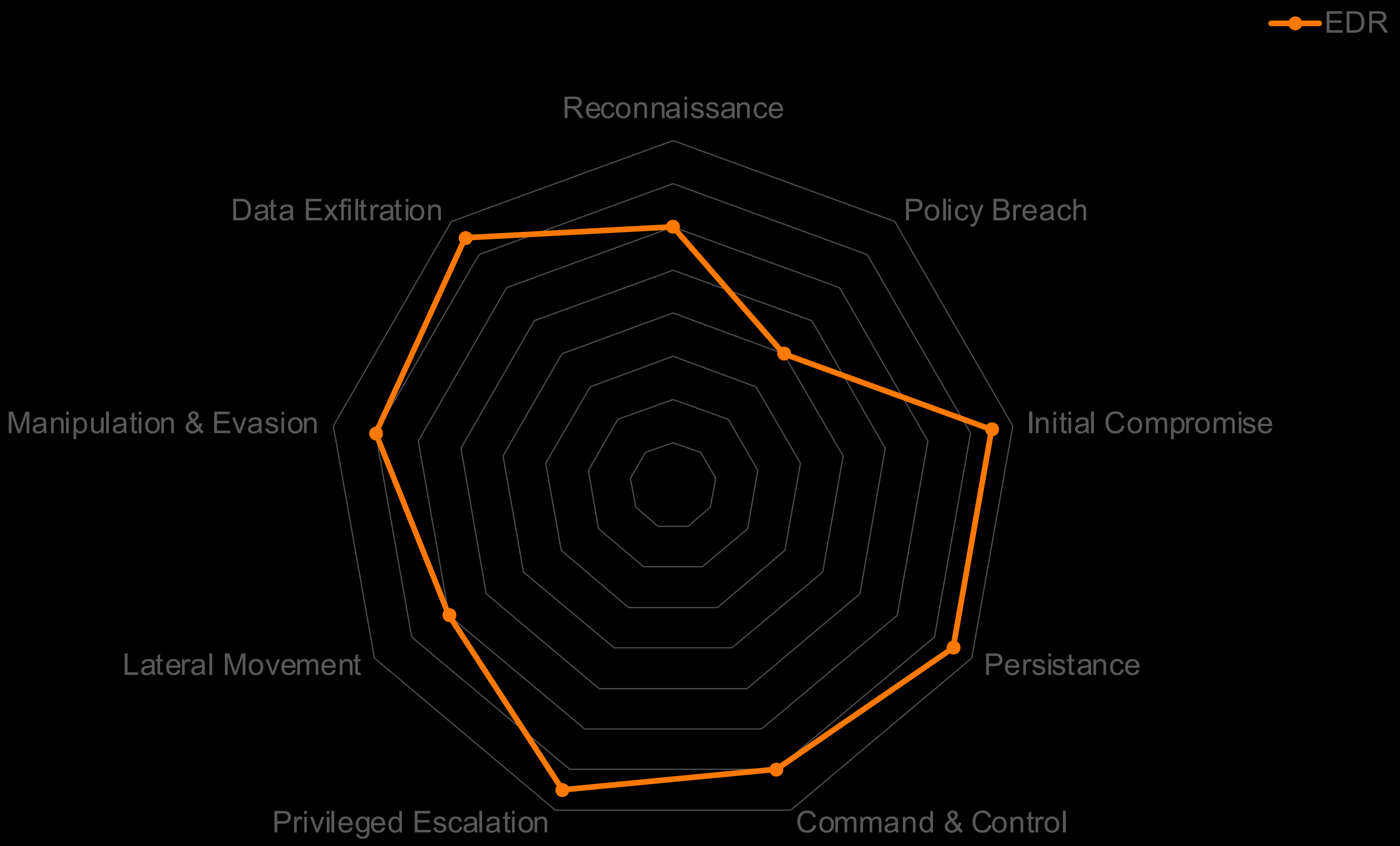
What is EDR?

- focuses on detecting and responding to threats on individual devices or endpoints.

- Collects telemetry from the endpoints, like a black box.

- typically monitor and analyze endpoint activity in real-time to identify potential threats, and can respond to those threats by isolating affected endpoints, terminating malicious processes, and rolling back changes.

What is the cyber kill chain?
Detecting threats using EDR



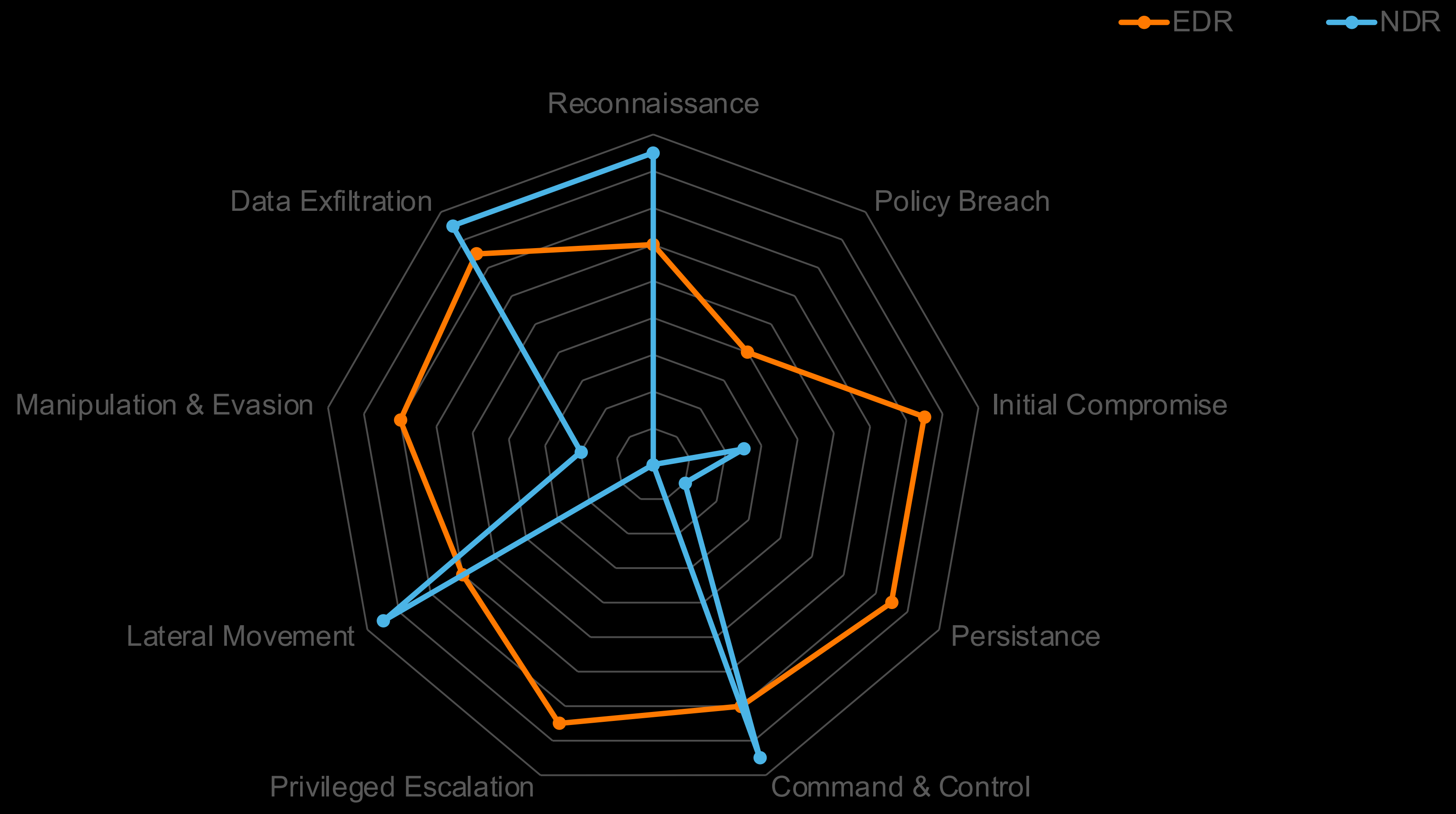
What is NDR?

- focuses on detecting and responding to threats on the network level.

- monitors network traffic to identify potential threats, such as malware infections or unauthorized access attempts

- can respond to those threats by isolating affected devices, blocking malicious traffic, and generating alerts.

What is the cyber kill chain?
Detecting threats using EDR



What is XDR?

- XDR (Extended Detection and Response) is an evolution of EDR (Endpoint Detection and Response)

- expands the scope of threat detection and response beyond individual endpoints.

- correlate data from multiple security products and sources across an organization's environment, including endpoints, networks, and cloud services.

- typically introduces automated response capabilities

What is SIEM?

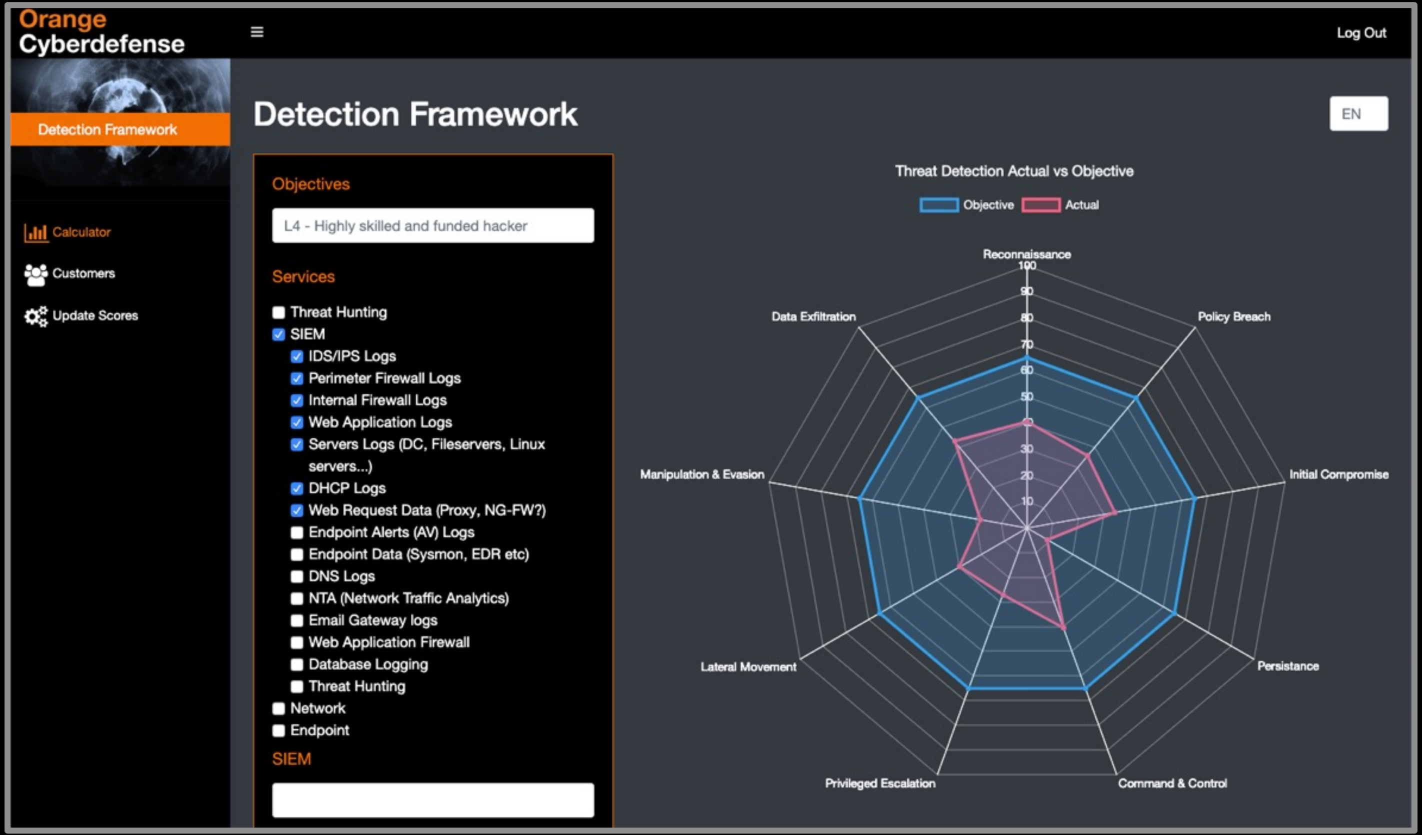
- cybersecurity technology that focuses on collecting and analyzing security-related data from multiple sources across an organization's network.

- can aggregate and correlate data from a variety of sources, such as firewalls, intrusion detection systems, and endpoint security solutions, to identify potential threats and generate alerts.

- can also be used for incident response and forensic analysis.

Threat Detection Framework

- Set an objective
- Add data sources
- Visualize detection ability
- Model improvements



Detection Framework

Objectives

L4 - Highly skilled and funded hacker

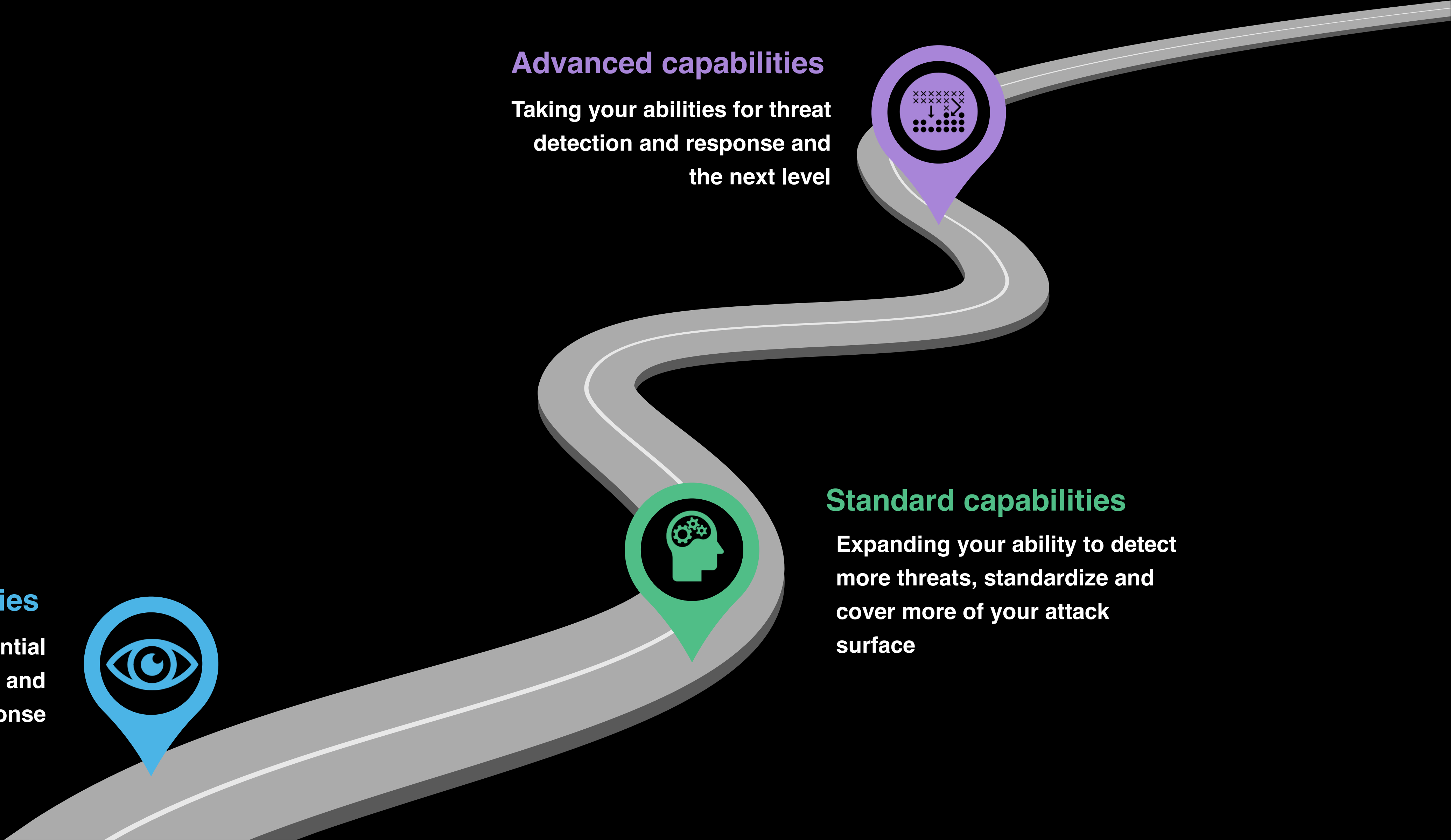
Services

- □ Threat Hunting
- ☑ SIEM
  - ☑ IDS/IPS Logs
  - ☑ Perimeter Firewall Logs
  - ☑ Internal Firewall Logs
  - ☑ Web Application Logs
  - ☑ Servers Logs (DC, Fileservers, Linux servers...)
  - ☑ DHCP Logs
  - ☑ Web Request Data (Proxy, NG-FW?)
  - □ Endpoint Alerts (AV) Logs
  - □ Endpoint Data (Sysmon, EDR etc)
  - □ DNS Logs
  - □ NTA (Network Traffic Analytics)
  - □ Email Gateway logs
  - □ Web Application Firewall
  - □ Database Logging
  - □ Threat Hunting
- □ Network
- □ Endpoint

SIEM

Approaching detection and response in layers

The Detection & Response journey



Essential capabilities

Providing the essential level of detection and response

Standard capabilities

Expanding your ability to detect more threats, standardize and cover more of your attack surface

Advanced capabilities

Taking your abilities for threat detection and response and the next level

Wherever you want to go.

Let’s get started today.