Defensive Security Intro

Creado por	Ammi González
Etiquetas	TryHackMe
Fecha de creación	@26 de enero de 2026 13:49

🔵 Defensive security (blue teaming)

✍🏻 Responsibilites of Defensive Security

🔍 Monitoring and Detecting

Continually observing network and system activity to detect suspicious behaviour and events.

These may include, for example, monitoring for logins from another country while the employee is based in the company's London office.

❎ Incident Response

The team quickly comes together if suspicious activity is confirmed and alerts are raised.

This is when the **Incident Response** process begins. The process involves containing and removing the threat and restoring the business back to normality.

🧠 Threat Intelligence

Gathering and using information about attackers—their latest methods, targets, and trends—can greatly strengthen an organisation’s defences.

For example, understanding that an attacker focuses on a specific software application used within organisations.

🛠️ Vulnerability Management

Fixing software or system flaws is an important preventative measure that can lower the risk of an attack.

Security teams can check which systems attackers are most likely to target. This can be done manually or with the help of automated tools.

🖥️ Investigation and Analysis

Members of a defensive security team are always monitoring and analysing what’s happening inside an organisation.

They work to separate normal activity from suspicious behaviour, digging into the details like solving a puzzle to uncover valuable insights.

🛅 Highly-skilled individuals you would find within a defensive security team

🔦 Bob, SOC Analyst

Bob monitors events on the organisation's network and systems to identify suspicious or expected behaviour. He is at the frontline of protecting the organisation.

⛔ Aaliyah, Incident Responder

Aaliyah is responsible for investigating and responding to ongoing security incidents within the organisation. She will monitor and prevent attackers in real time and share lessons learned during the attack to prevent future incidents.

⌨️ Zoe, Security Engineer

Zoe develops and maintains the essential tools and systems that support the defensive security team. These systems enable the team to monitor, investigate, and explore events within an organisation.

💀 Bill, Digital Forensics

Bill will utilise their expertise to understand what occurred during an incident. They will gather, preserve, and analyse evidence from the network and systems to uncover vital information about the attackers and their methods.

🏰 Defence in Depth

Organisations don’t rely on a single tool or method to stay secure — they build layers of defence, much like an onion or many layers to a castle. It’s called “Defence in Depth,” which means that if one security measure fails, we have others to rely on at various stages.

💪🏼 Employee Training

In today's world, the human factor of cyber security cannot be ignored. With attacks more often than not targeting employees rather than systems, training employees to be proactive in recognising attempts for things like phishing is essential.

📹 Intrusion Detection Systems (IDS)

These devices act as surveillance cameras across the organisation's IT. They monitor and alert when suspicious behaviour or activity is detected across the network or systems.

🧱 Firewalls

These devices act as security guards on an organisation's network. They monitor and determine what traffic is allowed to enter the network, or should be rejected.

👮🏻Security Policies

Security policies help organisations ensure that their systems are used correctly. They can reduce risk by blocking access to dangerous websites or requiring strong passwords, making it harder for attackers to guess login details.

💻 Security Operations Centre (SOC)

SOC is the defensive security centre for an organisation's technology. This busy centre is the frontline of protecting an organisation, often operating around the clock, 365 days a year, and employs a variety of security professionals who monitor and protect the organisation's networks, systems, and data.

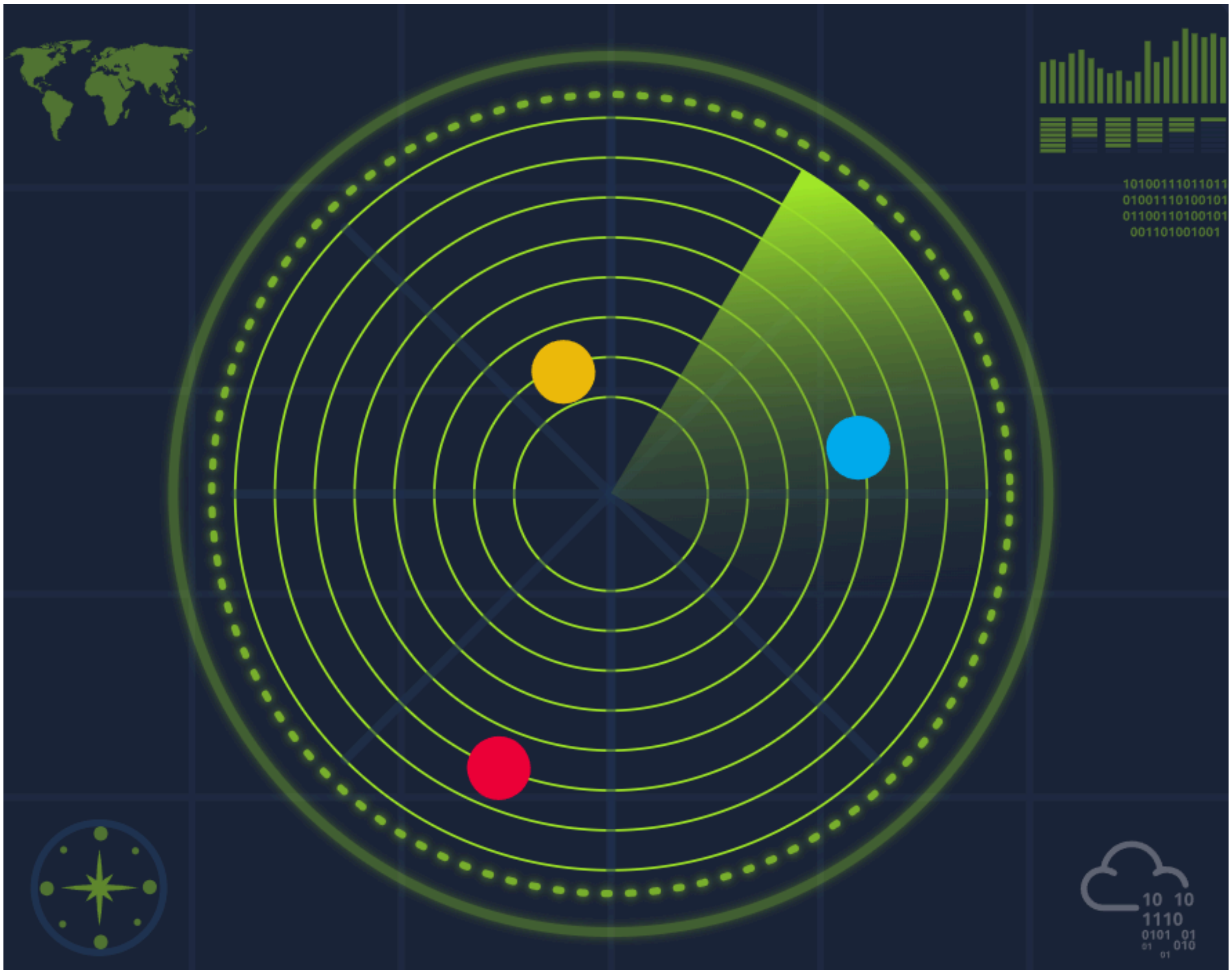
A typical day in the SOC could look like:

- Reviewing alerts triggered by security tooling
- Investigating anomalies

- Responding to incidents

These professionals are often the eyes and ears on the frontline for protecting an organisation.

🚨 SIEMs: The Defensive Security Radar



SIEMs (Security Information and Event Management) systems are the central place for all data and information collected from security devices, workstations, servers, and more within an organisation.

These systems are an absolutely critical part of any organisation's defensive security, as they offer insight into what is happening within the organisation's IT.

The systems inside an organisation produce a large amount of information. This information needs to be brought together in one central and easy-to-access place to understand what's happening quickly and clearly. This way, several people can review and analyse it quickly.