MODULE 5

Security Landscape, Red team & Blue Team

The Current threat Landscape:

The current threat landscape with the prevalence of always-on connectivity and advancements in technology that are available today, the threats are evolving rapidly to exploit different aspects of these technologies. Any device is vulnerable to attack, and with Internet of Things (IoT) this became a reality. In October 2016, a series of Distributed Denial of Service (DDoS) attacks were launched against DNS servers, which caused some major web services to stop working, such as GitHub, Paypal, Spotify, Twitter, and others.

Cybersecurity challenges

- To analyze the cybersecurity challenges faced by companies nowadays, it is necessary to obtain tangible data, and evidence of what's currently happening in the market.
- Not all industries will have the same type of cybersecurity challenges, and for this reason we will enumerate the threats that are still the most prevalent across different industries.
- This seems to be the most appropriate approach for cybersecurity analysts that are not specialized in certain industries, but at some point in their career they might need to deal with a certain industry that they are not so familiar with.
- According to Kaspersky Global IT Risk Report 2016 (14), the top causes for the most costly data breaches are based on old attacks that are evolving over time, which are in the following order:
    - Viruses, malware, and trojans
    - Lack of diligence and untrained employees
    - Phishing and social engineering
    - Targeted attack
    - Crypto and ransomware
- Top three are old suspects and very well known attacks in cybersecurity community, and they are still succeeding and are still part of current cybersecurity challenge.
- The real problem with the top three is that they are usually correlated to **human error**.

Incident Response Process

- To enhance the foundation of your security posture, you need to have a solid **incident response process**.
- This process will dictate how to handle security incidents and rapidly respond to them.
- Many companies do have an incident response process in place, but they fail to constantly review it to incorporate lessons learned from previous incidents.
- There are many industry standards, recommendations, and best practices that can help you to create your own incident response.
- The one that we are going to use as a reference is the **Computer Security Incident Response (CSIR)—publication 800-61R2 from NIST(1).**

What is an Incident Response Plan?

- **Incident response (IR)** is an organizational process that enables timely, effective response to cyberattacks. The incident response process includes identifying an attack, understanding its severity, and prioritizing it, investigating, and mitigating the attack, restoring operations, and taking action to ensure it won't recur.
- An **incident response plan (IRP)** is a set of documented procedures detailing the steps that should be taken in each phase of incident response. It should include guidelines for roles and responsibilities, communication plans, and standardized response protocols.

Reasons You Need an Incident Response Plan:

Here are the main reasons you must have a strong incident response plan in place:

1. **Prepares you for emergency**—security incidents happen without warning, so it's essential to prepare a process ahead of time.
2. **Repeatable process**—without an incident response plan, teams cannot respond in a repeatable manner or prioritize their time.
3. **Coordination**—in large organizations, it can be hard to keep everyone in the loop during a crisis. An incident response process can help achieve this.
4. **Exposes gaps**—in mid-sized organizations with limited staff or limited technical maturity, an incident response plan exposes obvious gaps in the security process or tooling which can be addressed before a crisis occurs.
5. **Preserves critical knowledge**—an incident response plan ensures critical knowledge and best practices for dealing with a crisis are not forgotten over time and lessons learned are incrementally added.
6. **Practice makes perfect**—an incident response plan creates a clear, repeatable process that is followed in every incident, improving coordination and effectiveness of response over time.
7. **Documentation and accountability**—an incident response plan with clear documentation reduces an organization's liability—it allows you to demonstrate to compliance auditors or authorities what was done to prevent the breach.

Incident Response Frameworks

The two most well-respected IR frameworks were developed by NIST and SANS to give IT teams a foundation to build their incident response plans on. Below are steps of each framework:

NIST Incident Response Steps

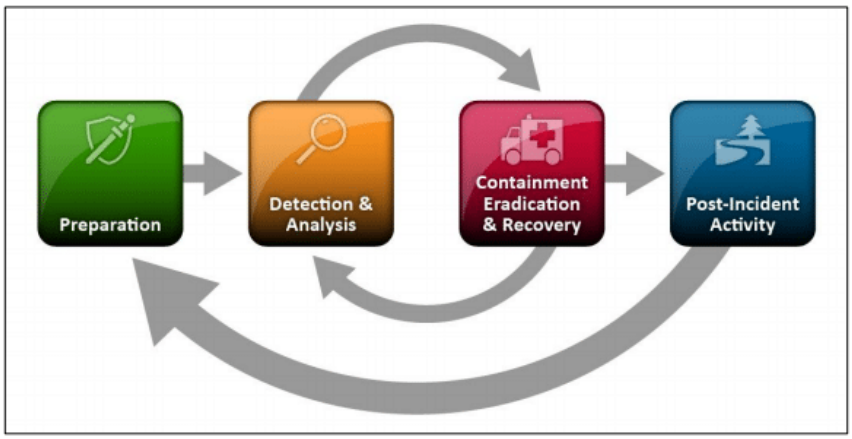
- Step #1: Preparation
- Step #2: Detection and Analysis
- Step #3: Containment, Eradication and Recovery
- Step #4: Post-Incident Activity

SANS Incident Response Steps

- Step #1: Preparation
- Step #2: Identification
- Step #3: Containment
- Step #4: Eradication
- Step #5: Recovery
- Step #6: Lessons Learned

The NIST Incident Response Life Cycle

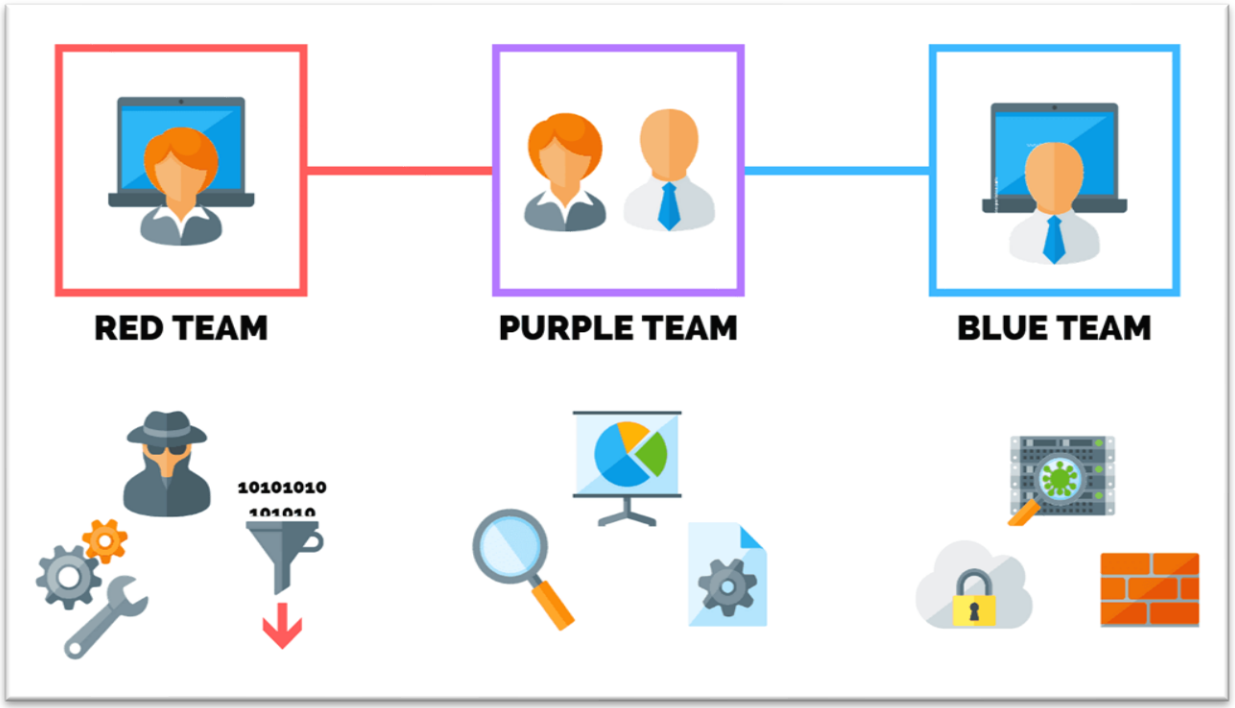
- NIST defines a four-step process for incident response, illustrated in the diagram below.



- The NIST process emphasizes that incident response is not a linear activity that starts when an incident is detected and ends with eradication and recovery. Rather, incident response is a cyclical activity, where there is continuing learning and improvement to discover how to better defend the organization.

- The NIST incident response model involves four phases recommended to effectively handle cybersecurity incidents. Some of the phases can be further subdivided to provide more steps:
  - **Preparation** - Organizations should take the necessary steps to be prepared for a cybersecurity incident when one occurs.
  - **Detection and analysis** - The cybersecurity response team is responsible for detecting and analysing incidents to determine how to proceed and who needs to be notified.
  - **Containment, eradication, and recovery** - After an incident, the response team should stop its spread, remove the threat from the environment, and begin the process of recovering affected systems.
  - **Post-incident activity** - The focus of post-incident activity is identifying lessons learned and using them to strengthen defences to minimize the probability of similar incidents in the future.

RED TEAM & BLUE TEAM



- Red and blue teams play an important role in defending against advanced cyber-attacks that threaten business communications, sensitive client data, or trade secrets.
- Red teams are offensive security professionals who are experts in attacking systems and breaking into defences.
- Blue teams are defensive security professionals responsible for maintaining internal network defences against all cyber-attacks and threats.
- Red teams simulate attacks against blue teams to test the effectiveness of the network's security. These red and blue team exercises provide a holistic security solution ensuring strong defences while keeping in view evolving threats.
- The Red Team must be composed of highly trained individuals, with different skill sets and they must be fully aware of the current threat landscape for the organization's industry. The Red Team must be aware of trends and understand how current attacks are taking place. In some circumstances and depending on the organization's requirements, members of the red Team must have coding skills to create their own exploit and customize it to better exploit relevant vulnerabilities that could affect the organization.

RED TEAM

- A red team consists of security professionals who act as adversaries to overcome cyber security controls.
- Red teams often consist of independent ethical hackers who evaluate system security in an objective manner.
- They utilize all the available techniques to find weaknesses in people, processes, and technology to gain unauthorized access to assets.
- As a result of these simulated attacks, red teams make recommendations and plans on how to strengthen an organization's security posture.

How Does a Red Team work?

- First the organization sets goals for red team on which they have to do the exercise.
- Planning is an important factor in red teaming. It is a simulation-based attack that intends to get access of specific information. So, after getting the goals they plan the whole scenario.
- Then the red teamers will start finding and exploiting all the possible vulnerabilities on the system to gain unauthorized of the targeted system.
- The red team will escalate the vulnerability to see until which limit, they can extend it if they find any vulnerability.
- After this the red team will make a report and analysis report for the defence security team (blue team) addressing the steps to recuperate and patch the vulnerability they addressed during their search.

Typical information gathered during this phase includes:

- Uncovering operating systems in use (Windows, macOS, or Linux).
- Identifying the make and model of networking equipment (servers, firewalls, switches, routers, access points, computers, etc.).
- Understanding physical controls (doors, locks, cameras, security personnel).
- Learning what ports are open/closed on a firewall to allow/block specific traffic.
- Creating a map of the network to determine what hosts are running what services along with where traffic is being sent.

Examples of red team exercises include:

- **Penetration testing**, also known as ethical hacking, is where the tester tries to gain access to a system, often using software tools. For example, 'John the Ripper' is a password-cracking program. It can detect what type of encryption is used and try to bypass it.
- **Social engineering** is where the Red Team attempts to persuade or trick members of staff into disclosing their credentials or allowing access to a restricted area.
- **Phishing** entails sending apparently authentic emails that entice staff members to take certain actions, such as logging into the hacker's website and entering credentials.
- **Intercepting** communication software tools such as packet sniffers and protocol analysers can be used to map a network, or read messages sent in clear text. The purpose of these tools is to gain information on the system. For example, if an attacker knows a server is running on a Microsoft operating system, then they would focus their attacks to exploit Microsoft vulnerabilities.
- **Card cloning** of an employee's security card to grant access into unrestricted areas, such as a server room.
- The Red Team is also accountable to register their core metrics, which are very important for the business. The main metrics are as follows:
    - **Mean Time to Compromise (MTTC):** This starts counting from the minute that the Red Team initiated the attack to the moment that they were able to successfully compromise the target.
    - **Mean Time to Privilege Escalation (MTTP):** This starts at the same point as the previous metric, but goes all the way to full compromise, which is the moment that the Red Team has administrative privilege on the target.

BLUE TEAM

- A blue team consists of security professionals who have an inside out view of the organization. Their task is to protect the organization's critical assets against any kind of threat.
- They are aware of the business objectives and the organization's security strategy. Therefore, their task is to strengthen the castle walls so no intruder can compromise the defences.

How does Blue Team Work?

- The blue team first gathers data, documents exactly what needs to be protected and carries out a risk assessment.
- Blue team basically perform **SOC (Security Operation Centre)** functions **and SIEM (Security Information and Event Management),** packet capture, packet analysis, threat detection and solving (threat intelligence).
- They then tighten up access to the system in many ways, including introducing stronger password policies and educating staff to ensure they understand and conform to security procedures.
- Monitoring tools are often put in place, allowing information regarding access to the systems to be logged and checked for unusual activity.
- Blue teams will perform regular checks on the system, for example, DNS audits, internal or external network vulnerability scans and capturing sample network traffic for analysis.
- Blue teams have to establish security measures around key assets of an organization. They start their defensive plan by identifying the critical assets, document the importance of these assets to the business and what impact the absence of these assets will have.
- Blue teams then perform risk assessments by identifying threats against each asset and the weaknesses these threats can exploit. By evaluating the risks and prioritizing it, the blue team develops an action plan to implement controls that can lower the impact or likelihood of threats materializing against assets.

Examples of blue team exercises include:

- **Performing DNS audits** (domain name server) to prevent phishing attacks, avoid stale DNS issues, avoid downtime from DNS record deletions, and prevent/reduce DNS and web attacks.
- **Conducting digital footprint** analysis to tracks users' activity and identify any known signatures that might indicate a breach of security.
- Installing endpoint security software on external devices such as laptops and smartphones.
- Ensuring firewall access controls are properly configured and that antivirus software are kept up to date.
- Deploying IDS and IPS software as a detective and preventive security control.
- Implementing SIEM solutions to log and ingest network activity.
- Analysing logs and memory to pick up unusual activity on the system and identify and pinpoint an attack.
- Segregating networks and ensure they are configured correctly.
- Performing routine vulnerability scans.
- Securing systems by using antivirus or anti-malware software.

- Embedding security in processes.
- Just like the Red Team, the Blue Team also has accountability for some security metrics, which in this case is not 100% precise. The reason the metrics are not precise is that the true reality is that the Blue Team might not know precisely what time the Red Team was able to compromise the system. These estimations are self-explanatory as you can see in the following list:
    - Estimated Time to Detection (ETTD)
    - Estimated Time to Recovery (ETTR)

Blue Team vs Red Team

	Blue Team	Red Team
Activities	**Blue team defends against attack and respond to it.**	**Red Team plays a role of attacker by finding and exploiting vulnerabilities.**
Main Aim	**Main practice of blue team is protecting the infrastructure and monitoring.**	**Main practice is ethical hacking and Penetration Testing.**
Skills	**Uses skills like digital forensics, secure attack areas and protect the organization's infrastructure.**	**Use methods like Social Engineering, vulnerability exploit, etc.**
Tools	**Operational Security (protects the data from getting into the wrong hand).**	**Black box Testing (Not aware about internal working).**
Exercise	**Blue team contains digital forensics.**	**Red team contains web App scanning.**
Activities	**Blue team will control the damage.**	**Red team will exploit the vulnerability**