

Information Security Operations Center

Prepared by

Dr. Ibrahim Gomaa

جامعة الجميع الذكية

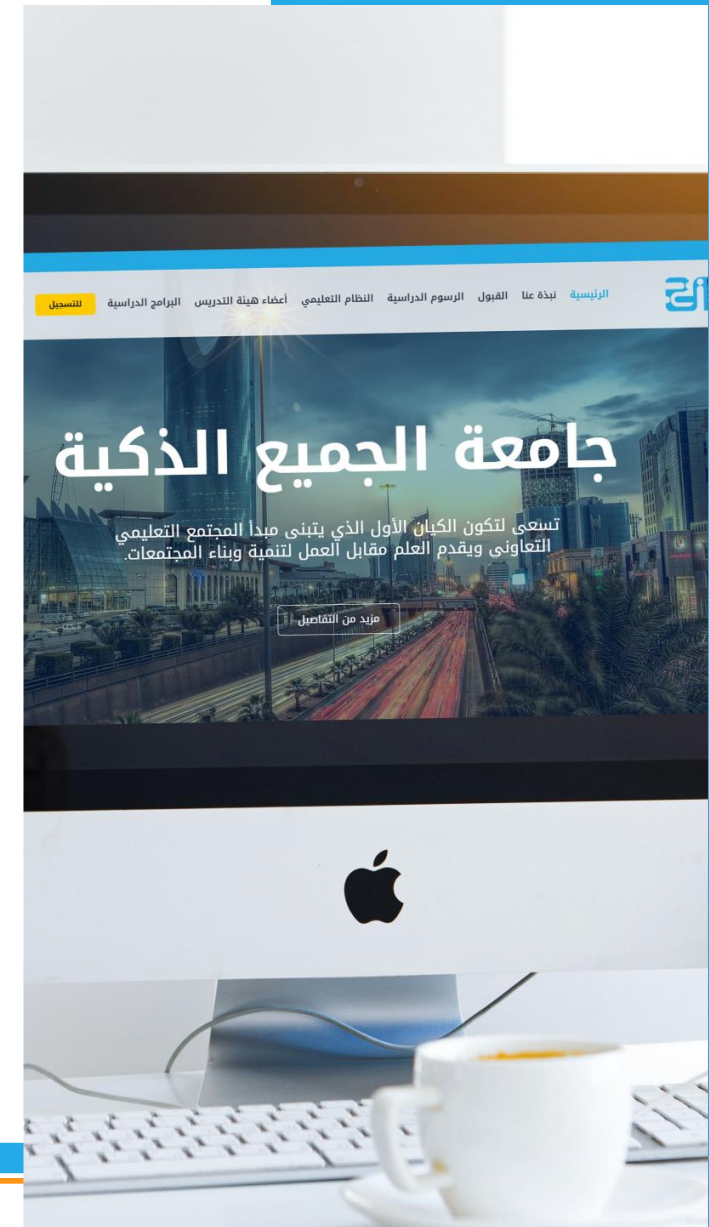
تسعى لتكون الكيان الأول الذي يتبنى مبدأ المجتمع التعليمي
التعاوني ويقدم العلم مقابل العمل لتنمية وبناء المجتمعات.

Lecture 1: Network Security Monitoring

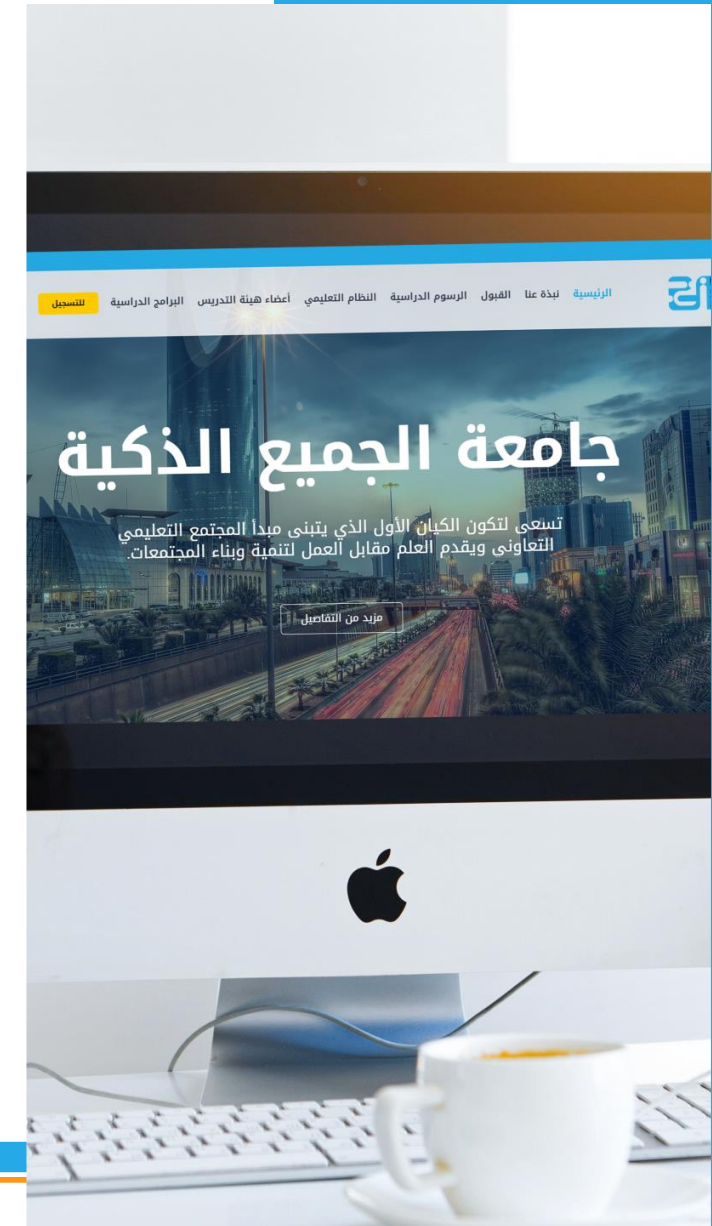


جامعة الجميع الذكية
EVERYONE'S SMART UNIVERSITY

Topic Title	Topic Objective
Introduction	Monitoring, Alerting, and what they can do for you.
War Stories	Explain why networks and data are attacked.
Threat Actors	Explain the motivations of the threat actors behind specific security incidents.
Threat Impact	Explain the potential impact of network security attacks.
The Modern Security Operations Centre	Explain the mission of the Security Operations Center (SOC).
Becoming a Defender	Describe resources available to prepare for a career in cybersecurity operations.



Introduction



Monitoring

- is the process of maintaining surveillance over the existence and magnitude of state change and data flow in a system.
- the process of becoming aware of the state of a system.
- the process of measurement, which might not necessarily involve any human interaction

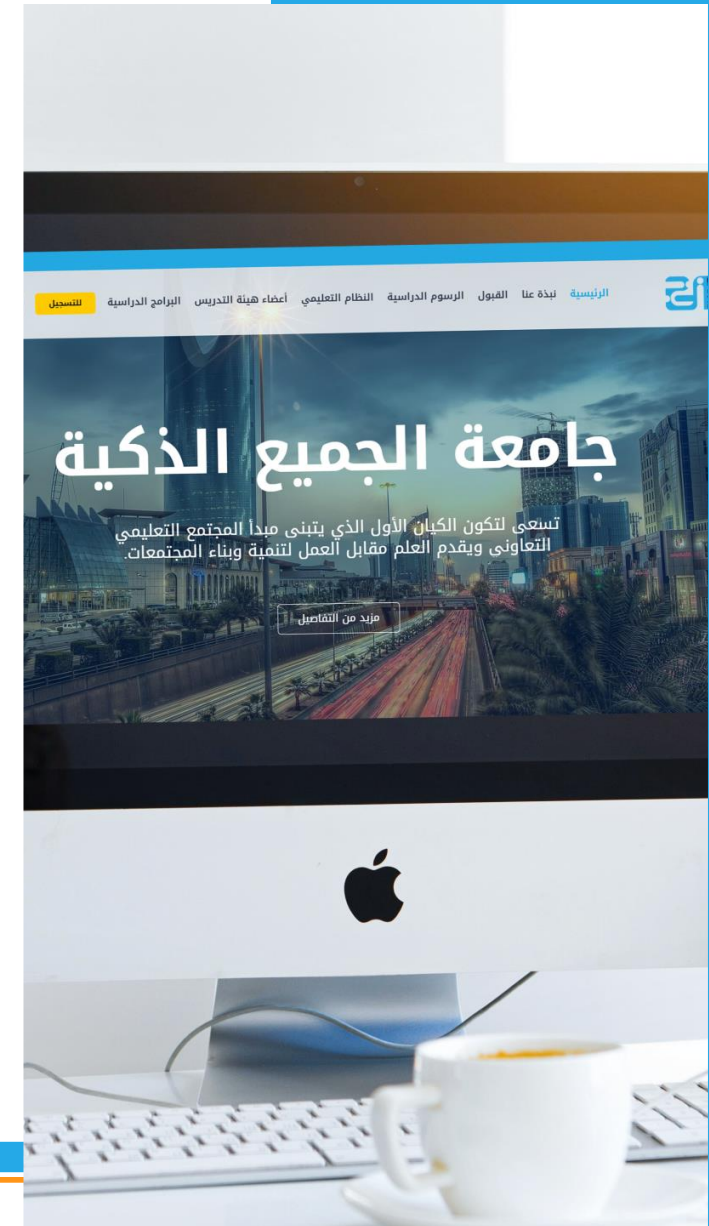
This is done in two ways, **Proactive** and **Reactive**

The former involves watching visual indicators, such as time series and dashboards, and is sometimes what administrators mean by **monitoring**.

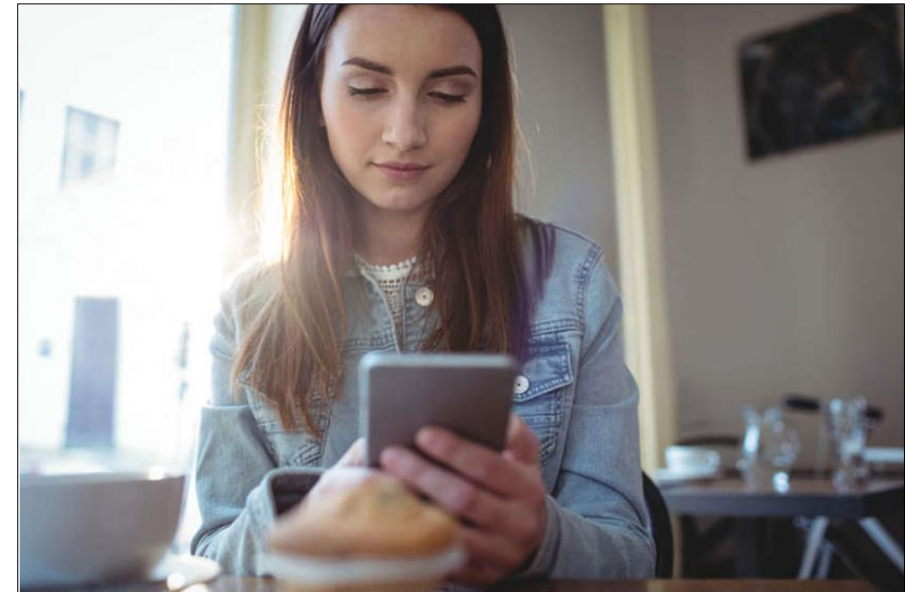
The latter involves automated ways to deliver notifications to operators in order to bring to their attention a grave change in system's state; this is usually referred to as **alerting**.

- * Early Problem Detection
- * Decision Making
- * Baselining
- * Automation
- * Autonomic Computing
 - An architecture in which the system is capable of regulating itself and thus enabling self management and self-healing. The goal of AC is to **minimize the need for human intervention** in a similar way, by replacing it with self-regulation
- * Availability
- * Performance
- * Predictions

War Stories



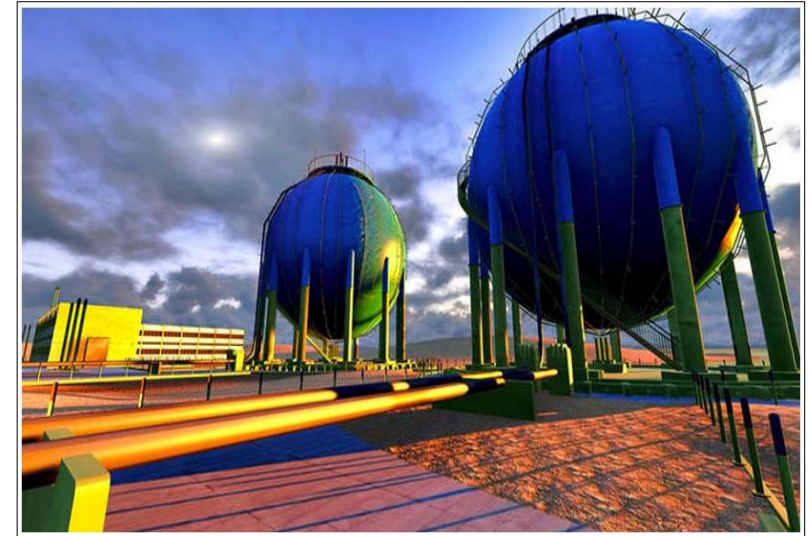
- Hackers can set up open “**rogue**” wireless hotspots posing as a genuine wireless network.
- Rogue wireless hotspots are also known as “**evil twin**” hotspots.



- Employees of an organization are often lured into opening attachments that install ransomware on the employees' computers.
- This **ransomware**, when installed, begins the process of **gathering and encrypting corporate data**.
- The goal of the attackers **is financial gain**, because they hold the company's data for ransom until they are **paid**.



- Some of today's malware is so sophisticated and expensive to create that security experts believe only a nation state or group of nations could possibly have the influence and funding to create it.
- Such **malware** can be targeted to attack a **nation's** vulnerable infrastructure, such as the **water system** or **power grid**.
- One such malware was the **Stuxnet** worm that **infected USB** drives and infiltrated **Windows operating systems**. It then targeted **Step 7** software that was developed by Siemens for their **Programmable Logic Controllers (PLCs)**.

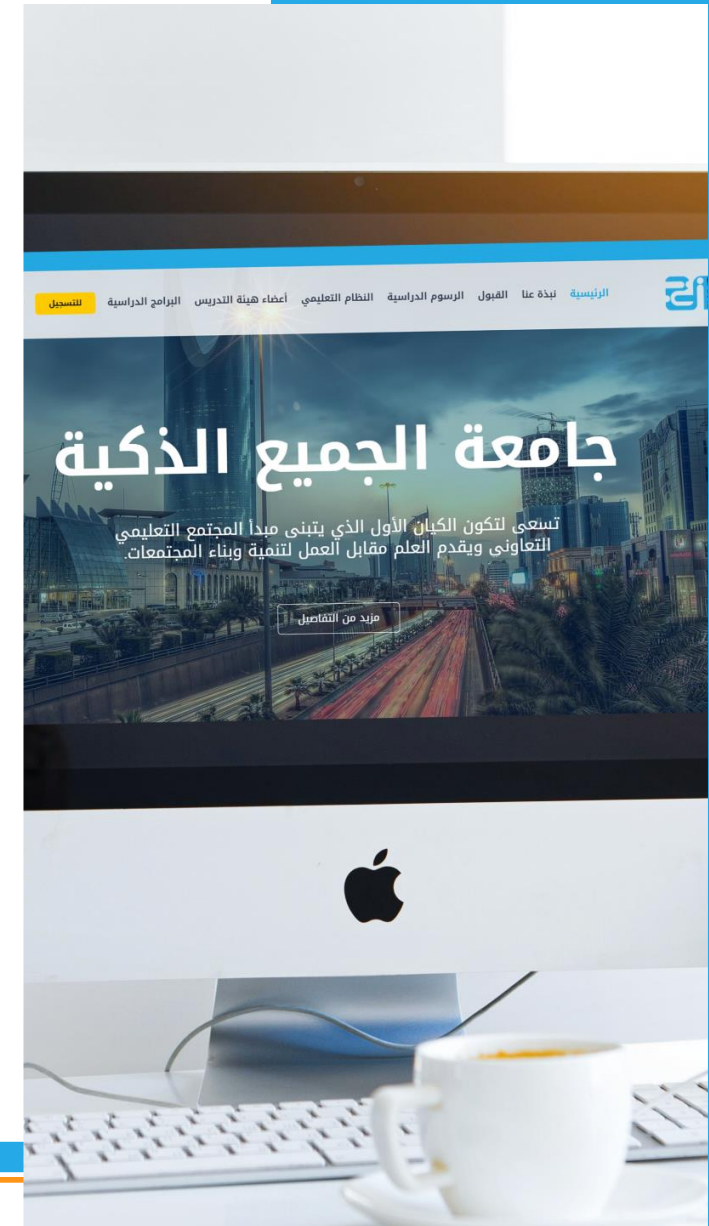


Installing the Virtual Machine

In this lab, you will complete the following objectives:

- Install [VirtualBox](#) on your personal computer
- Download and install the [CyberOps Workstation](#) Virtual Machine (VM).

Threat Actors



Threat Actors

- **Threat actors** are individuals or groups of individuals who **perform cyberattacks**. They include, but are not limited to:
 - Amateurs
 - Hacktivists
 - Organized crime groups
 - State-sponsored groups
 - Terrorist groups
- **Cyberattacks** are intentional **malicious acts** meant to negatively impact another individual or organization.



Threat Actors (Contd.)



Amateurs

- They are also known as **script kiddies** and have little or no skill.
- They existing tools or instructions often use found on the internet to launch attacks.
- Even though they use basic tools, the results can still be devastating.



Hackers

- These are hackers who publicly protest against a variety of political and social ideas.
- They post articles and videos, leaking sensitive information, and disrupting web services with illegitimate traffic in Distributed Denial of Service (DDoS) attacks.



Financial Gain

- Much of the hacking activity that consistently threatens our security is motivated by financial gain.
- Cybercriminals want to gain access to bank accounts, personal data, and anything else they can leverage to generate cash flow.

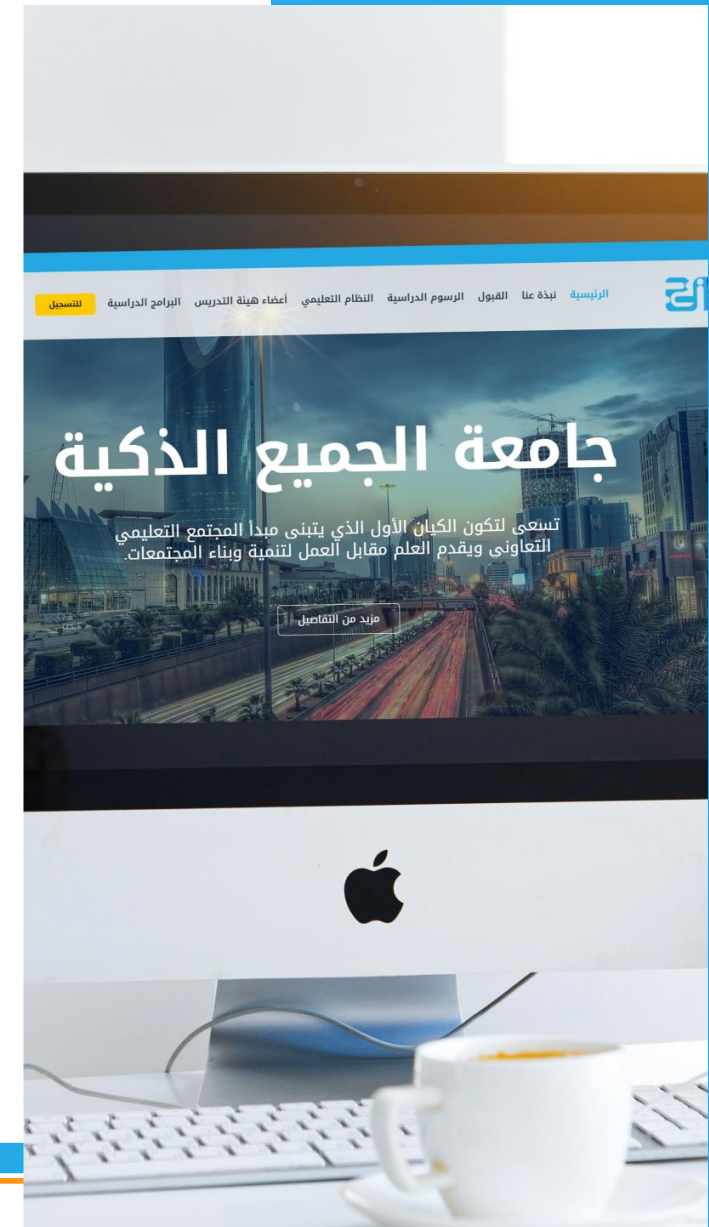


Trade Secrets and Global Politics

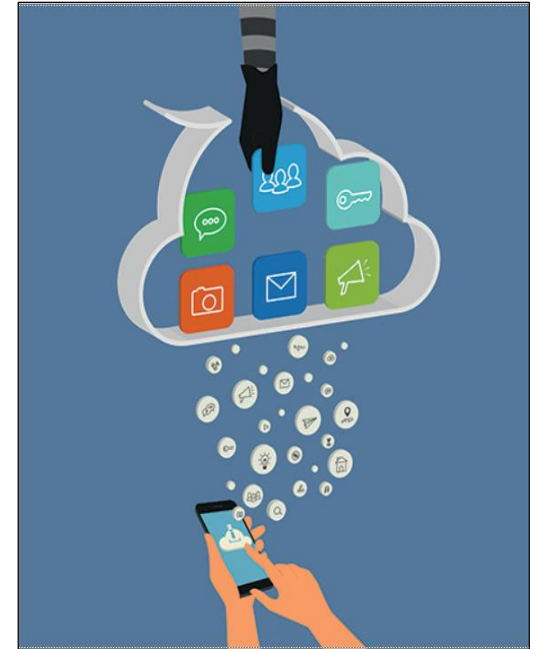
- At times, nation states hack other countries, or interfere with their internal politics.
- Often, they may be interested in using cyberspace for industrial espionage.
- The theft of intellectual property can give a country a significant advantage in international trade.



Threat Impact



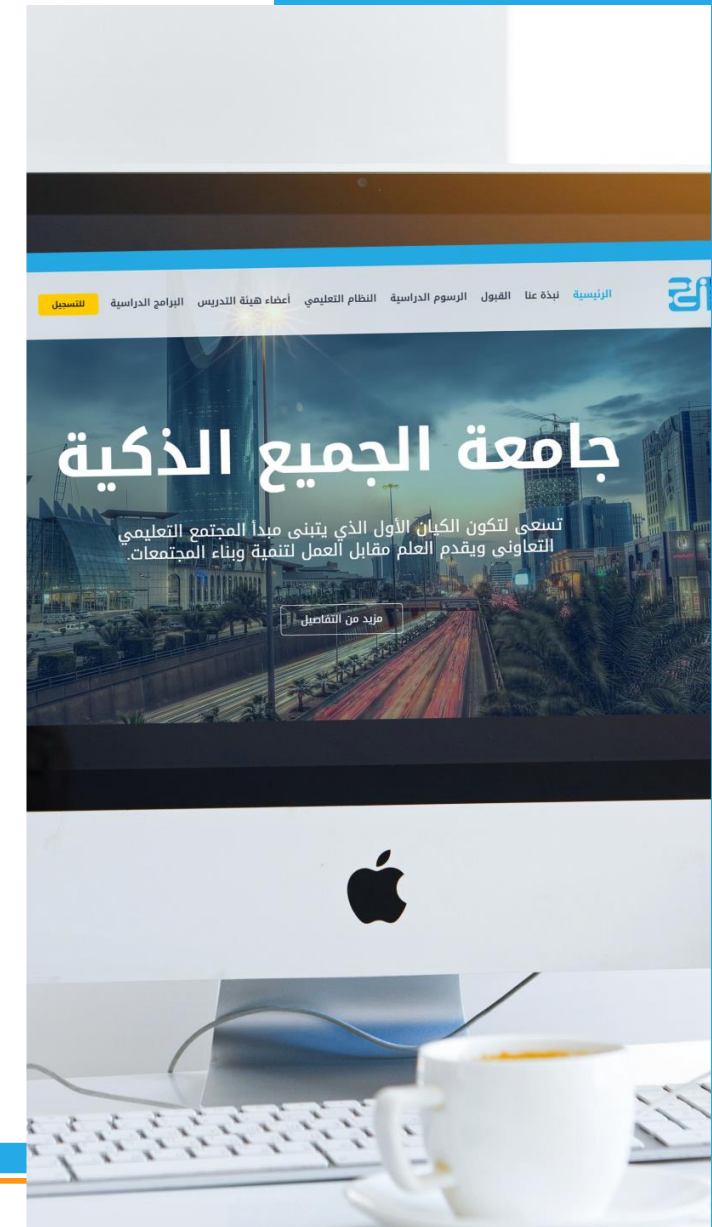
- Personally Identifiable Information (**PII**) is any information that can be used to positively identify an individual, for example, name, social security number, birthdate, credit card numbers etc.
- Cybercriminals aim to obtain these lists of PII that can then be sold on the dark web. Stolen PII can be used to create **fake financial accounts**, such as **credit cards** and **short-term loans**.
- The medical community creates and maintains Electronic Medical Records (**EMRs**) that contain Protected Health Information (**PHI**), a subset of PII.
- Personal Security Information (**PSI**), another type of PII, includes usernames, passwords, and other security-related information that individuals use to access information or services on the network.



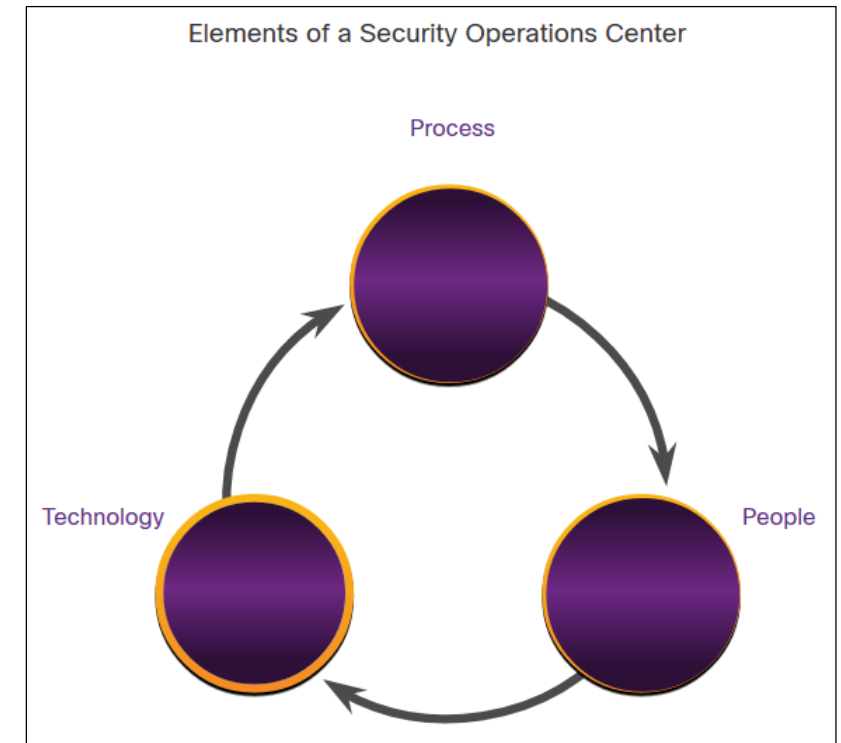
- The **loss of intellectual property** to competitors is a serious concern.
- An additional major concern is the **loss of trust** that comes when a company is unable to protect its customers' personal data.
- The loss of competitive advantage may come from this loss of trust rather than another company or country **stealing trade secrets**.

- It is not just businesses that get hacked.
- State-supported hacker warriors can cause disruption and destruction of vital services and resources within an enemy nation.
- The internet has become essential as a medium for commercial and financial activities. Disruption of these activities can devastate a nation's economy.

The Modern Security Operations Center (SOC)



- To use a formalized, structured, and disciplined approach for defending against cyber threats, organizations typically use the services of professionals from a **Security Operations Center (SOC)**.
- SOC's provide a broad range of **services**, from **monitoring** and **management**, to comprehensive threat solutions and customized **hosted security**.
- SOC's can be **wholly in-house**, owned and operated by a business, or elements of a SOC can be **contracted out to security vendors**.



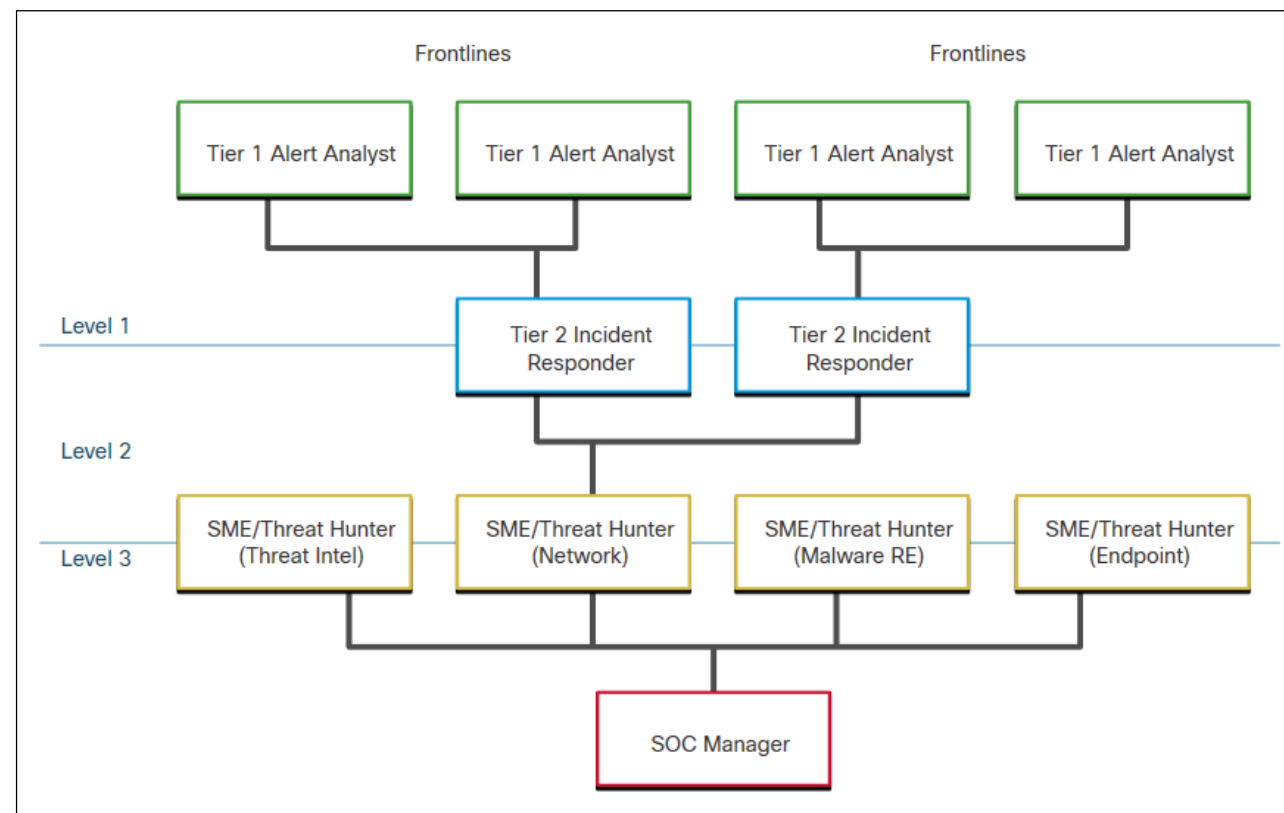
People in the SOC

SOCs assign job roles by tiers, according to the **expertise** and **responsibilities** required for each.

Tiers	Responsibilities
Tier 1 Alert Analyst	Monitor incoming alerts, verify that a true incident has occurred, and forward tickets to Tier 2, if necessary.
Tier 2 Incident Responder	Responsible for deep investigation of incidents and advise remediation or action to be taken.
Tier 3 Threat Hunter	Experts in network, endpoint, threat intelligence, malware reverse engineering and tracing the processes of the malware to determine its impact and how it can be removed. They are also deeply involved in hunting for potential threats and implementing threat detection tools. Threat hunters search for cyber threats that are present in the network but have not yet been detected.
SOC Manager	Manages all the resources of the SOC and serves as the point of contact for the larger organization or customer.

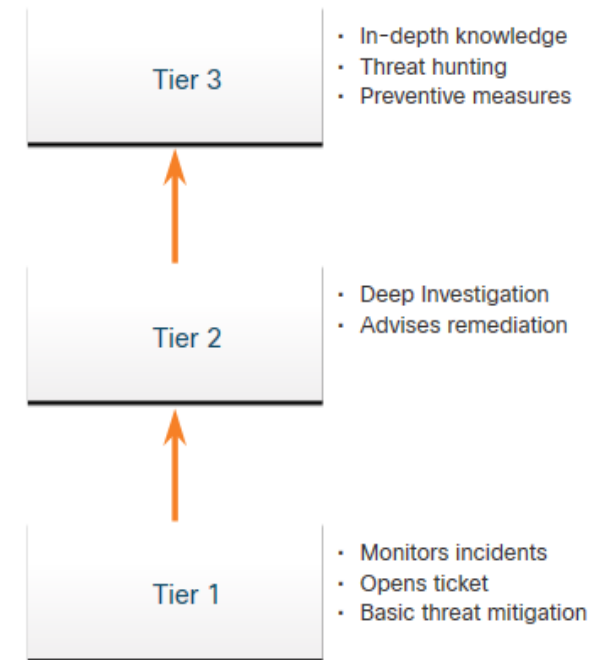
People in the SOC (Contd.)

- **First tier jobs** are more entry level, while third tier jobs require extensive expertise.
- The figure, which is originally from the **SANS Institute**, graphically represents how these roles interact with each other.

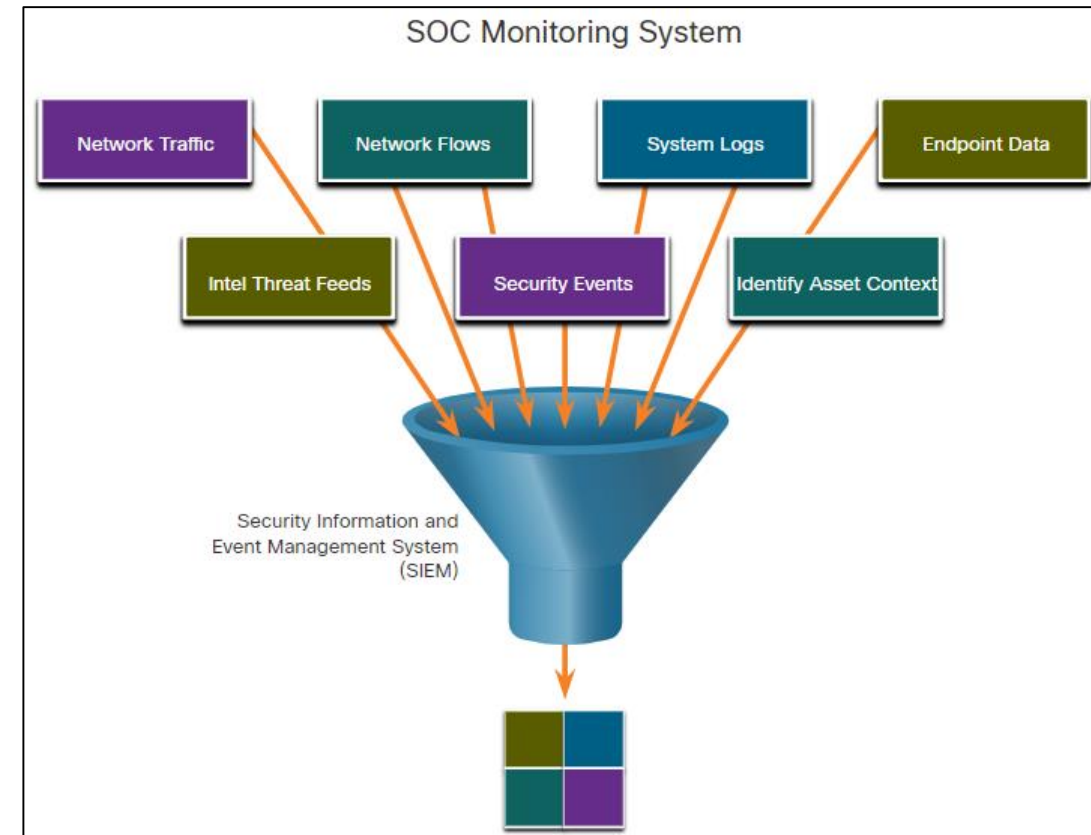


- A **Cybersecurity Analyst** is required to monitor security alert queues and investigate the assigned alerts. A ticketing system is used to assign these alerts to the analyst's queue.
- The software that generates the alerts can trigger **false alarms**. The analyst, therefore, needs to verify that an assigned alert represents a true security incident.
- When this verification is established, the **incident** can be forwarded to **investigators** or other security personnel to be acted upon. Otherwise, the alert is dismissed as a false alarm.
- If a ticket cannot be resolved, the Cybersecurity Analyst forwards the ticket to a **Tier 2 Incident Responder** for deeper investigation and remediation.
- If the Incident Responder cannot resolve the ticket, it is forwarded it to a **Tier 3** personnel.

Roles of the People in a Security Operations Center

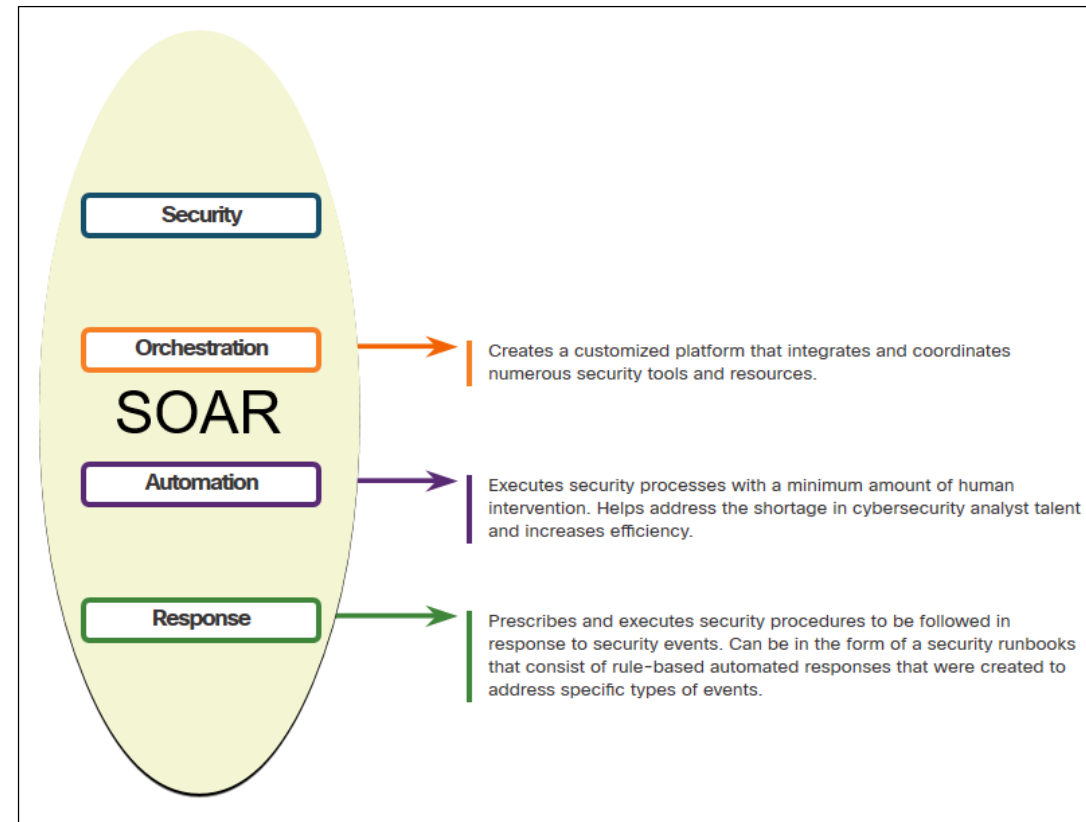


- An SOC needs a Security Information and Event Management (SIEM) system to understand the data that firewalls, network appliances, intrusion detection systems, and other devices generate.
- SIEM systems collect and filter data, and detect, classify, analyze and investigate threats. They may also manage resources to implement preventive measures and address future threats.



Technologies in the SOC: SOAR

- **SIEM** and Security Orchestration, Automation and Response (**SOAR**) are often **paired together** as they have capabilities that complement each other.
- Large security operations (SecOps) teams use both technologies to optimize their SOC.
- **SOAR** platforms are similar to SIEMs as they **aggregate, correlate, and analyze alerts**. In addition, SOAR technology **integrate threat intelligence and automate incident investigation and response** workflows based on playbooks developed by the security team.



- SOAR security platforms:
 - Gather alarm data from each component of the system.
 - Provide tools that enable cases to be researched, assessed, and investigated.
 - Emphasize integration as a means of automating complex incident response workflows that enable more rapid response and adaptive defense strategies.
 - Include pre-defined playbooks that enable automatic response to specific threats. Playbooks can be initiated automatically based on predefined rules or may be triggered by security personnel.

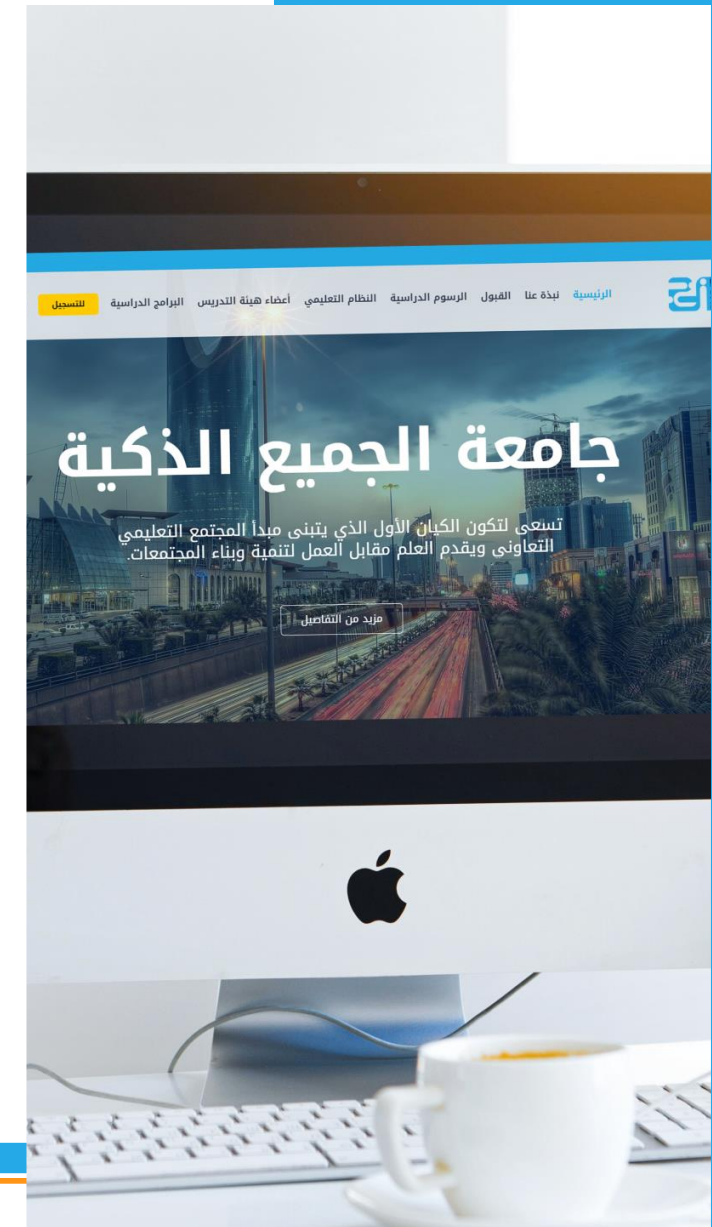
- Many metrics or **Key Performance Indicators** (KPI) can be devised to measure different aspects of SOC performance. However, **five metrics** are commonly used as SOC metrics by SOC managers.

Metrics	Definition
Dwell Time	The length of time that threat actors have access to a network before they are detected, and their access is stopped
Mean Time to Detect (MTTD)	The average time that it takes for the SOC personnel to identify valid security incidents have occurred in the network
Mean Time to Respond (MTTR)	The average time it takes to stop and remediate a security incident
Mean Time to Contain (MTTC)	The time required to stop the incident from causing further damage to systems or data
Time to Control	The time required to stop the spread of malware in the network

Enterprise and Managed Security

- For medium and large networks, the organization will benefit from implementing an **enterprise-level SOC**, which is a **complete in-house solution**.
- **Larger organizations** may outsource at least a part of the SOC operations to a security solutions provider.

Becoming a Defender



- A variety of cybersecurity certifications that are relevant to careers in SOC are available:
 - Cisco Certified CyberOps Associate
 - CompTIA Cybersecurity Analyst Certification
 - (ISC)² Information Security Certifications
 - Global Information Assurance Certification (GIAC)
- Search for “cybersecurity certifications” on the Internet to know more about other vendor and vendor-neutral certifications.



Further Education

- **Degrees:** When considering a career in the cybersecurity field, one should seriously consider pursuing a technical degree or bachelor's degree in computer science, electrical engineering, information technology, or information security.
- **Python Programming:** Computer programming is an essential skill for anyone who wishes to pursue a career in cybersecurity. If you have never learned how to program, then Python might be the first language to learn.
- **Linux Skills:** Linux is widely used in SOC's and other networking and security environments. Linux skills are a valuable addition to your skillset as you work to develop a career in cybersecurity.



Getting Experience

- **Internships:** Internships are an excellent method for entering the cybersecurity field. Sometimes, internships turn into an offer of full time employment. However, even a temporary internship allows you the opportunity to gain experience in the inner workings of a cybersecurity organization
- **Scholarships and Awards:** To help close the security skills gap, organizations have introduced scholarship and awards programs.
- **Temporary Agencies:** Many organizations use temporary agencies to fill job openings for the first 90 days. If the employee is a good match, the organization may convert the employee to a full-time, permanent position.
- **Your First Job:** If you have no experience in the cybersecurity field, working for a call center or support desk may be your first step into gaining the experience you need to move ahead in your career.



Thanks

