ASP4134 - Audit Sistem Informasi

(week 7)

Confidential. Terbatas untuk mahasiswa PKN STAN

ASP4134 - Audit Sistem Informasi

Protection of Information Assets

Confidential. Terbatas untuk mahasiswa PKN STAN

AGENDA

- Lecture Protection of Information Assets
- Quiz 2

Last Week Recap

Information should be protected at various points in its life cycle; notably, in process, in transit and at rest

Measures should be put in place to mitigate risk to information such as unauthorized access, use,disclosure, modification and destruction.

Effective information protection requires a multidisciplinary approach involving people, processes andinformation technology and typically revolves around the objectives of confidentiality, integrity and availability (CIA).

ASP4134 - Audit Sistem Informasi

Key objectives:

1. memahami kerangka **konsep audit tata kelola** teknologi informasi berdasarkan standar tata Kelola
2. menyusun **program audit tata kelola** sistem informasi
3. menyusun **laporan audit tata kelola** sistem informasi
4. melaksanakan **pengauditan atas pengoperasian dan pemeliharaan** atas sistem informasi
5. melakukan **audit atas perolehan, pengembangan, dan implementasi sistem informasi**
6. melakukan **pengauditan atas keamanan informasi** Here we are
7. menggunakan **Teknik Audit Berbantuan Komputer** dalam pengujian pengendalian dan pengujian substantif
8. menjelaskan dampak kelemahan **pengendalian umum dan pengendalian aplikasi** terhadap peluang terjadinya kecurangan dan kesalahan saji pada laporan keuangan

What we learn:

1. Evaluate the effectiveness of **Security Awareness Programs**
2. Identify common **Information System Attack** methods
3. Distinguish between various **Security Testing Tools**
4. Understand **Security Monitoring** techniques (IDS, IPS, SIEM)
5. Audit the **Incident Response** process and **Forensics** procedures

Security Event Management

ASP4134 - Audit Sistem Informasi

Security Awareness

Einstein said:

“Two things are infinite: the universe and human stupidity”

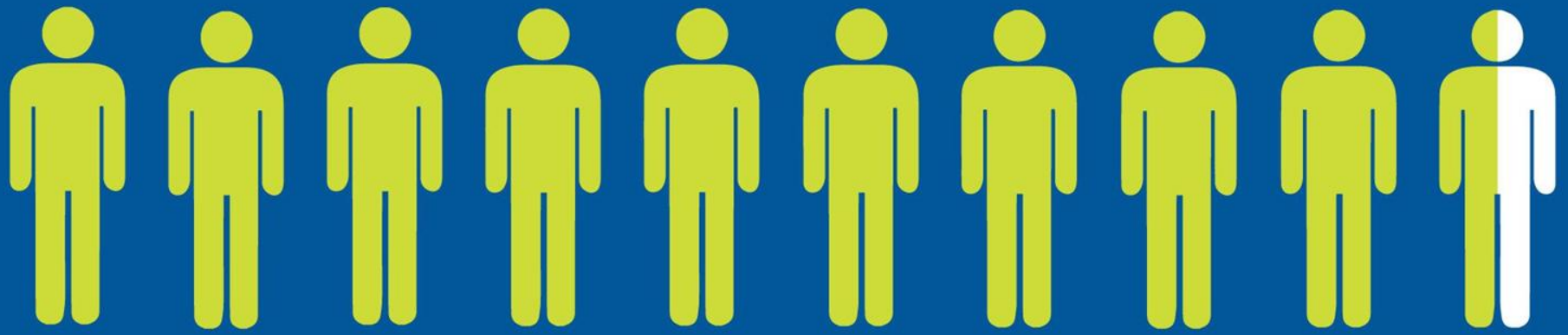
Engineers said:

“There is no patch for human stupidity”

95%

of all successful cyber attacks is caused by human error

Source: IBM Cyber Security Intelligence Index



Security Awareness Training and Programs

Effective security in an organization depends on **people**.

The success and effectiveness of any security initiative is largely based on whether the people (in this case employees and partners) understand the **operation of the security solution** and know **what is expected of them**.



Awareness → Training → Education

Level	Awareness	Training	Education
Objective	Change behavior and create a security culture. Answers the **"what."**	Teach skills to perform a job more securely. Answers the **"how."**	Provide in-depth knowledge for security professionals. Answers the **"why."**
Audience	All employees, from day one.	Specific functional areas (e.g., IT staff, developers).	Security professionals seeking career expertise.
Method	Passive learning: videos, newsletters, posters, phishing simulations.	Formal, hands-on learning: instructor-led classes, labs.	Intensive learning: university courses, seminars, research.

Security Awareness Training and Programs

An effective IS security awareness, training and education program consists of:

- Developing a **security culture** that encourages a shared mindset and empowers individuals to be vigilant about cybersecurity, which is critical in shaping a comprehensive strategy for information assets protection
- Developing an IS information **security policy** that incorporates the elements of security awareness, training and education to provide **direction** to the organization
- Informing everyone in the organization of their IS security **roles and responsibilities** and **what is expected of them** to enhance information security
- Establishing **processes and procedures** for monitoring and reviewing the program
- Focusing on the entire organization
- Setting the **tone at the top** for proper IS security behavior in the organization
- Explaining, in **simple terms**, the proper rules of behavior in the use of information systems
- Establishing the basis for any **penalties** and other **sanctions** to be imposed due to noncompliance
- Centering on the organization's IS security policy and issue-specific policies

How to Audit?

- **Document Review:**
  - Review the training curriculum against the current security policy.
  - Verify attendance records (look for gaps: contractors, temp staff).
- **Interview Process:**
  - Interview random staff members.
  - *Ask:* "What do you do if you receive a suspicious email?" (Test their knowledge).
- **Social Engineering Testing:**
  - The Auditor may perform (or oversee) a controlled phishing campaign.
  - Physical walkthroughs (try to tailgate, look for passwords under keyboards).
- **Review of Remediation:**
  - What happens when an employee fails a test repeatedly? Is there a formal process?

Information System Attack Methods and Techniques

Information System Attack Methods and Techniques

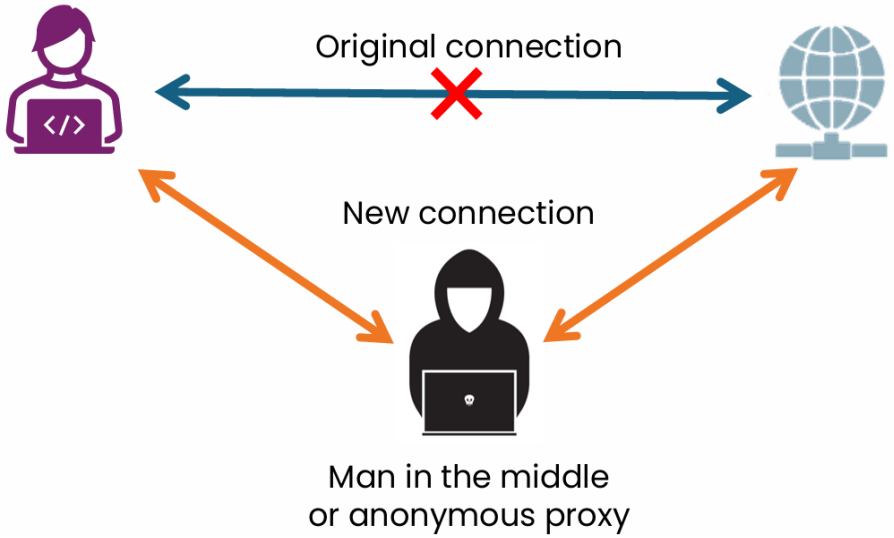
- Risk arises from vulnerabilities (whether technical or human) within an environment.
- Attack techniques exploit those vulnerabilities and may originate either within or outside the enterprise.
- Computer attacks can result in proprietary or confidential data being stolen or modified, loss of customer confidence and market share, embarrassment to management and legal actions against an enterprise.

	Passive (Espionage)	Active (Sabotage/Manipulation)
Goal	Steal information without altering it.	Modify data, disrupt service, or gain unauthorized access.
Examples	• Network sniffing • Traffic analysis • Wiretapping	• Malware • Denial of Service (DoS) • modifying database records
Audit Difficulty	Very hard to detect because data is not changed.	Easier to detect (logs, changed hashes) but damage is immediate.

Common Attack Methods and Techniques

1. Network & Communication Attacks

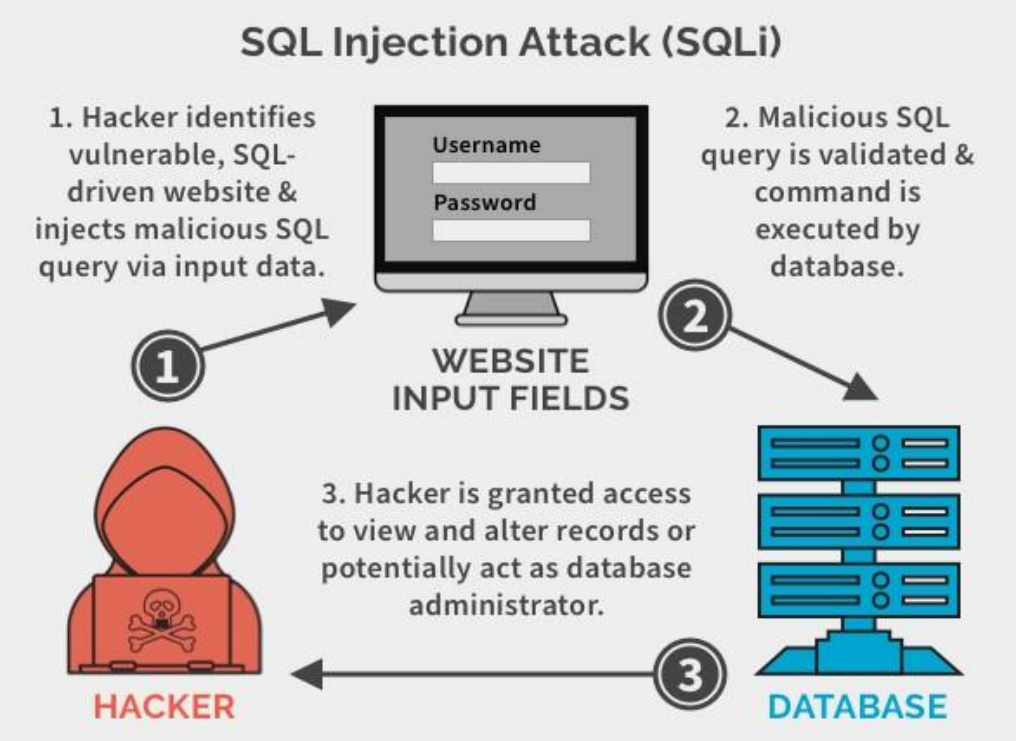
- **Eavesdropping:** Unauthorized interception of private communications.
- **Man-in-the-Middle (MitM) Attack:** An attacker secretly relays and possibly alters the communication between two parties.
- **Packet Replay:** Capturing network traffic and re-sending it later to trick a system into unauthorized actions.
- **DNS Spoofing / DNS Tunneling:** Manipulating DNS records to redirect traffic to malicious sites or bypass security controls.
- **Traffic Analysis:** Monitoring the frequency and load of messages to gain intelligence, even if the data is encrypted.
- **Dialing (War Dialing):** Automatically calling a range of phone numbers to find unsecured modems or entry points.



Common Attack Methods and Techniques

2. Data & Code Manipulation

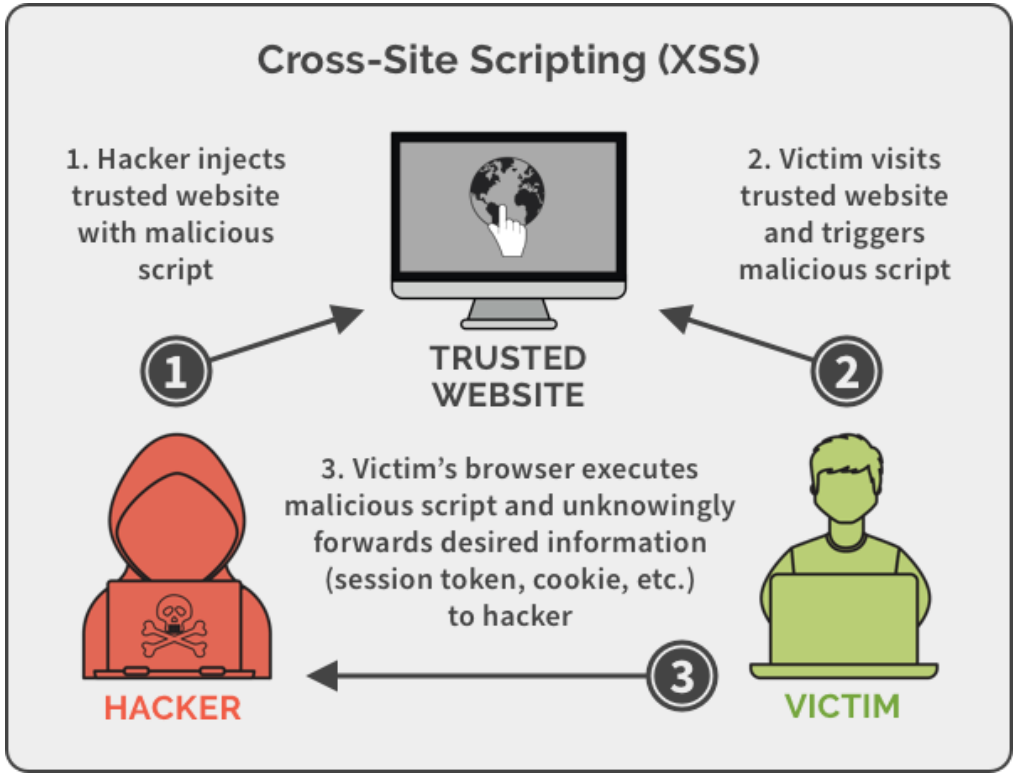
- **Injection Attack:** Inserting malicious commands (e.g., SQL Injection) into system inputs to manipulate the database.
- **Message Modification:** Altering the content of a message or data while it is in transit.
- **Alteration Attack:** Unauthorized modification of data, system settings, or software.
- **Salami Attack:** A series of minor, almost unnoticeable data alterations (usually financial) that result in a significant impact over time.
- **Malicious Codes:** Software designed to damage or gain unauthorized access (includes **Viruses, Worms, Spyware, and Malware**).



Common Attack Methods and Techniques

3. Web & Application Attacks

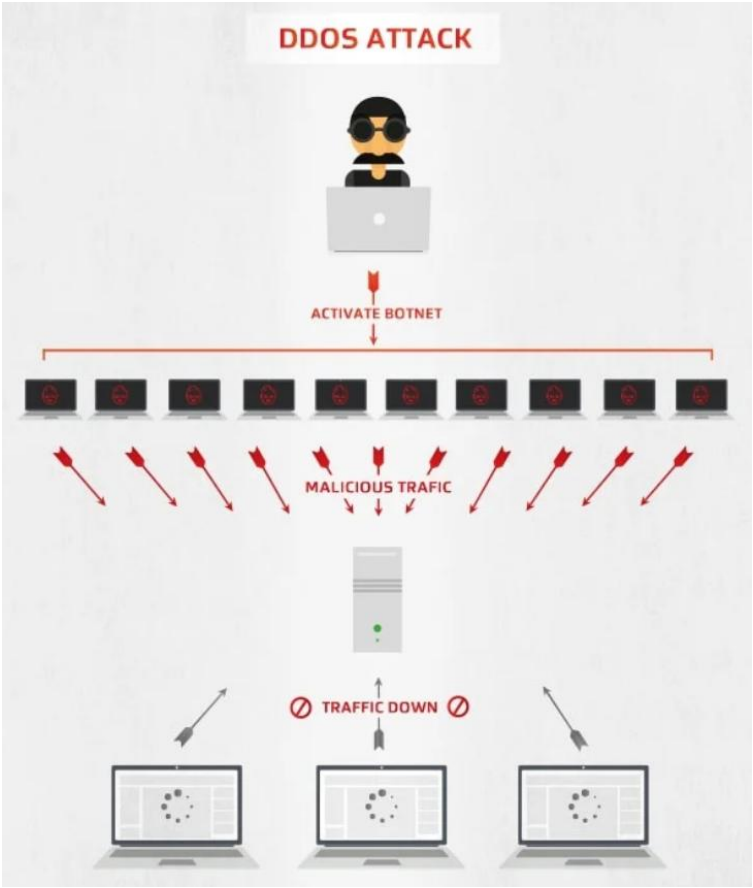
- **Cross-site Scripting (XSS):** Injecting malicious scripts into trusted websites to target the end-user's browser.
- **Cross-site Request Forgery (CSRF):** Forcing an authenticated user to execute unwanted actions on a web application.
- **URL Poisoning:** Modifying URL parameters to bypass security or access sensitive information.
- **Zero-day Exploit:** Attacking a software vulnerability before the vendor has released a patch.



Common Attack Methods and Techniques

4. Availability & Resource Attacks

- **Denial-of-Service (DoS):** Overwhelming a system with traffic to make its services unavailable.
- **Flooding:** Sending massive amounts of data to exhaust a network or system's resources.
- **Botnets:** A network of compromised computers ("zombies") used to launch large-scale attacks.
- **Interrupt Attack:** An attack that aims to break the continuity or availability of a service or asset.



Common Attack Methods and Techniques

5. Human-Centric & Access Attacks

- **Social Engineering:** Manipulating individuals into divulging confidential information.
- **Phishing:** Using fraudulent emails or websites to steal sensitive data like login credentials.
- **Pharming:** Maliciously redirecting users to a fake website, even if they typed the correct URL.
- **Masquerading:** Pretending to be an authorized user to gain access to a system.
- **Piggybacking:** Following an authorized person into a restricted area (physical or digital).
- **Unauthorized Access:** Gaining entry to systems via the Internet or web-based services without permission.



Ransomware

Ransomware is malware that employs encryption techniques to hold a victim's information at ransom

Figure 5.59—Stages of a Ransomware Attack



Mitigating Active Ransomware Infections

- Quarantine the machine
- Contain the spread
- Do not switch off the system
- Create a backup
- Check for decryptors
- Locate patient zero
- Wipe and restore

Security Testing Tools and Techniques



Security Testing

Security testing is a process that is performed to reveal flaws and vulnerabilities in information systems.

IS auditors should underscore the importance of security testing to avoid loss of customer confidence, disturbances to Organization systems and related compliance complications in the organization.

The results of security testing should lead to improvement in the systems' security architectures.

Security Testing Tools and Techniques

- **Security assessments**—a method of identifying, evaluating and prioritizing potential vulnerabilities and threats and their possible impacts to determine whether and how to implement security controls.
- **Security audits**—a process of reviewing an organization's security practices against a recognized and published standard or framework.

The Goal: We cannot secure what we do not test.

Two Main Approaches:

1. **Vulnerability Scanning**: Automated, broad, and non-intrusive. (Like walking around a house checking if windows are unlocked).
2. **Penetration Testing** (Ethical Hacking): Manual, targeted, and intrusive. (Like actually climbing through the window and trying to open the safe).

The "Kill Chain": Testing helps break the attacker's path before they complete their objective.

Vulnerability assessments

The goals of **vulnerability assessments** are:

- **Evaluate** the security posture of the organization.
- **Identify**, evaluate and prioritize vulnerabilities.
- **Assess** the reaction of the information security environment to vulnerabilities and attacks.
- **Learn** about the vulnerabilities currently present.
- Identify ways vulnerabilities can be **exploited** by attackers.
- Decide on **controls** to **implement** to address the vulnerabilities.

Penetration testing

- During penetration testing, an auditor attempts **to circumvent the security features of a system and exploits the vulnerabilities to gain access** that would otherwise be unauthorized.

Methods

- **Manual penetration testing** – Penetration Testing Phases conducted by humans who are experts in information security.
- **Automated penetration testing** – involves the application of tools that require very little to no human interaction

The IS Auditor’s Role

Independence is Key:

- The person who built the system should *not* be the one testing it.
- External 3rd parties are often required for Pen Tests to ensure objectivity.

Scope Management:

Did the test cover the whole environment or just "safe" non-critical servers?

Remediation (The most important part):

- Finding bugs is useless if you don't fix them.
- *Audit Question:* "Show me the tracking ticket for the Critical finding from last year's Pen Test." If it's still open, that is a failed control.

Security Monitoring Logs, Tools and Techniques



Security Monitoring Logs, Tools and Techniques

- Monitoring, detection and logging are **integral** parts of security.
- With potential for attacks and data loss, it is **necessary** to monitor data and information flowing into and out of an organization.
- There are several **methods and tools** an organization can use to detect and log potential problems.

Security Monitoring Logs, Tools and Techniques

Monitoring provides several benefits for an organization including:

- **Enforces accountability**—users can be held accountable for their actions and activities.
- **Promotes positive behavior**—users are less likely to attempt to circumvent security controls.
- **Encourages compliance culture**— Legislation, regulations and internal policies typically require specific monitoring and accountability practices.
- **Supports investigations**—Monitoring audit trails enables investigators to reconstruct events after their occurrence.
- **Identifies security problems**—Monitoring provides important information about events such as system failures, OS bugs, software errors and malicious attacks.

Intrusion Detection System

- An **IDS** works with routers and firewalls by monitoring network use anomalies. -> **Detective**

Categories	Components	Types
• **Network-based IDSs** • **Host-based IDSs**	Sensors Analyzers Administration console User interface	Signature-based – protect against detected intrusion patterns Statistical-based – based on known and expected behavior of systems Neural network – similar to the statistical model but with added self-learning functionality

Intrusion Prevention System

- **IPS**s are closely related to IDSs and are designed not only to detect attacks, but also to prevent the intended victim hosts from being affected by the attacks. -> **Preventive**

Type of IPS	Description
Host-based IPS (HIPS)	Information security software that is located on individual clients and servers. It monitors events and thwarts attacks at the device level.
Network-based IPS (NIPS)	Deployed within the enterprise network infrastructure. It monitors all the data in the complete network and thwarts threats before they can reach their targets.
Wireless IPS (WIPS)	A network security device that monitors radio waves for unauthorized access points (APs). It automatically takes countermeasures to prevent them from causing damage to enterprise systems.

Honeypots and Honeynets

- A honeypot is a software application that pretends to be a vulnerable server on the Internet and is not set up to actively protect against break-ins.

- A honeypot acts as a decoy system that lures hackers.

- Honeynets: A network of multiple, linked honeypots that simulates a larger, more realistic network for attackers to interact with

Types of honeypots:
- High-interaction—Gives hackers a real environment to attack
- Low-interaction—Emulates production environments and provides limited information

Logs

- Access rights to system logs for security administrators to perform logging and monitoring activities should be strictly controlled.
- Media logging is used to support accountability
- Tools for Audit Trail (Logs) Analysis
  - Audit reduction tools
  - Trend/variance-detection tools
  - Attack-signature-detection tools
  - SIEM systems
- Audit trails involve many costs that factor into IT's determination as to how much logging is enough.

SIEM - Security Information and Event Management

- Security incidents are often made up of a series of events that occur throughout a network.
- By correlating data, the SIEM can take many isolated events and combine them to create one single relevant security incident.
- SIEM is an umbrella term for centralized information security software packages that combine the following two technologies:
  - Security information management (SIM) —The SIM component collects data from log files for analysis and reporting on past security threats and events.
  - SEM—SEM works in similar fashion to SIM, the only difference being that instead of focusing on historic log data, it works in real-time mode to identify relevant security events

Security Incident Response Management

Security Incident Response Management

- **Incident management** is the management of incidents that are potentially damaging to an organization.
- In information security, it is critical for the IS auditor to grasp the fact that not all incidents are computer-related; for example, a burglary at the office is also an incident.
- To minimize damage from security incidents and to recover and to learn from such incidents, **a formal incident response capability** should be established.

Incident Response Process

Figure 5.66—Incident Response Process



Source: Cichonski, P.; T. Millar; T. Grance; K. Scarfone; *Special Publication 800-61 Revision 2, Computer Security Incident Handling Guide*, National Institute of Standards and Technology (NIST), *https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf*

Security Incident Response Management

SOAR is a collection of technologies that allow the organization to gather inputs monitored by the security operations team and incorporate automated responses to the resolution of security events.

Components

- **Orchestration** – connecting security tools and integrating a series of interdependent and disparate security systems
- **Automation** –execution of tasks without human intervention. E.g creating scripts that automatically perform repetitive tasks such as data collection, analysis, and initial response actions.
- **Response** – the actions taken to mitigate or remediate a Components of SOAR security threat, can be automated or semi-automated

Evidence Collection and Forensics

- In the aftermath of a computer crime, it is very important that proper procedures be used to collect evidence from the crime scene.
- If proper procedures are not followed, data could be damaged, and even if the perpetrator is eventually identified, the evidence may not be useful to the prosecution.

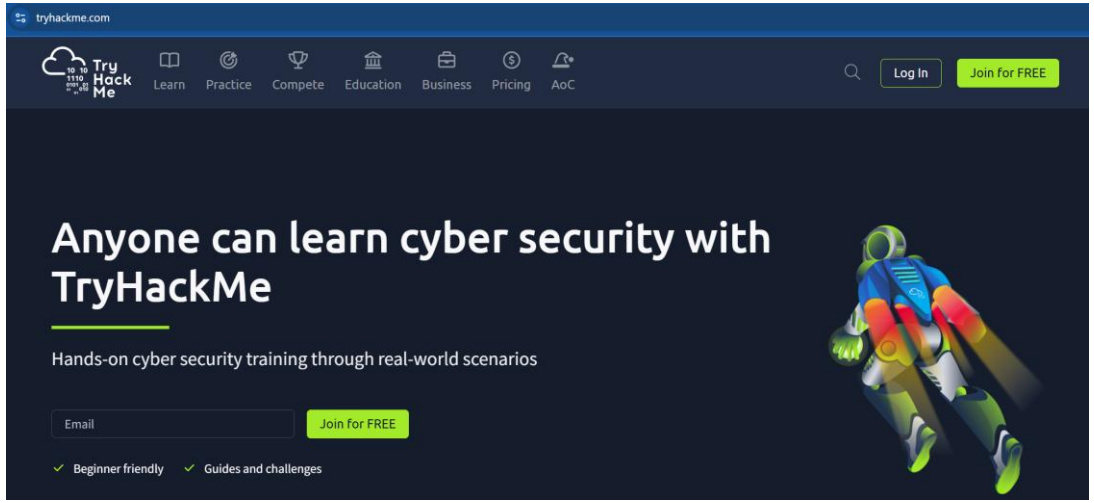
Chain of Custody

- **Chain of custody** refers to documenting, in detail, how evidence is handled and maintained, including its ownership, transfer and modification.
- For evidence to be admissible in a court of law, the chain of custody needs to be maintained professionally. The chain of evidence contains information regarding:
  - Who had access to the evidence (chronological)
  - The procedures followed in working with the evidence (e.g., disk duplication, virtual memory dump)
  - Proving that the analysis is based on copies that are identical to the original evidence (e.g., documentation, checksums or timestamps)

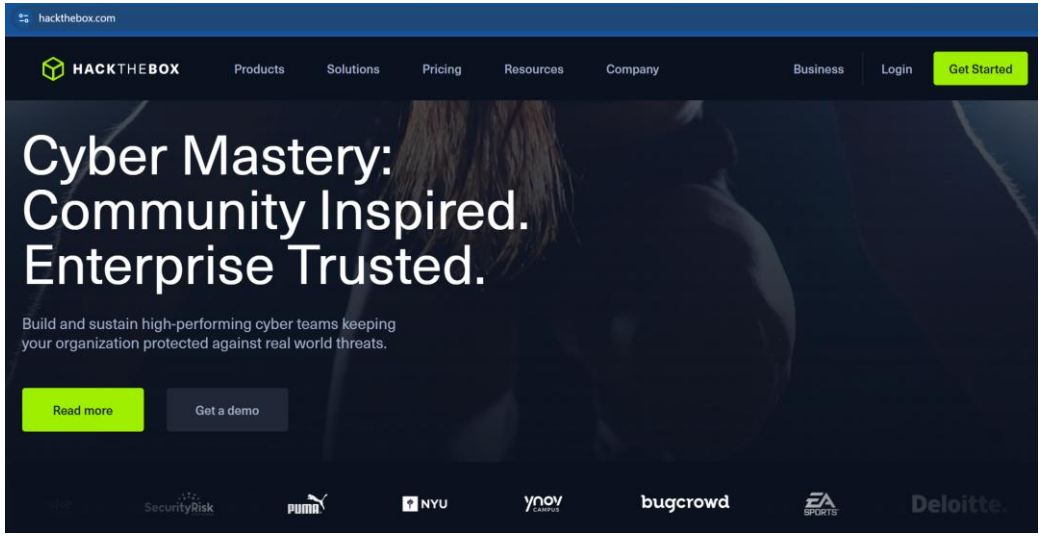
Key Learning Points

1. The most sophisticated firewall can be bypassed by one person clicking a malicious link. You must audit the "Human Element" through three levels:
    - Awareness: General behavior (posters, tips).
    - Training: Specific skills (how to handle a phishing email).
    - Education: Strategic understanding (security certifications for managers).
2. An auditor should check if the organization proactively looks for its own weaknesses. Review the frequency and results of **Vulnerability Scans** and **Penetration Testing**. An effective organization finds its own "holes" and patches them before a hacker does.
3. The auditor's primary concerns are the chain of custody and the preservation of original evidence.

Learn more About Security



https://tryhackme.com



https://www.hackthebox.com