



## 01- Comparing Security Roles and Security Controls

**Ahmed Sultan**

Senior Technical Instructor  
[ahmedsultan.me/about](https://ahmedsultan.me/about)

# Outlines

1.1- Compare and Contrast Information Security Roles

1.2- Compare and Contrast Security Control And Framework Types

## **1.1- Compare and Contrast Information Security Roles**

### **1.2- Compare and Contrast Security Control And Framework Types**

# INFORMATION SECURITY

- **Information Security** (or infosec) refers to the protection of data resources from unauthorized access, attack, theft, or damage. صيانة معلومات

- Data may be vulnerable because of the way it is stored, the way it is transferred, or the way it is processed. تخزين

- Secure information has three properties, often referred to as the **CIA Triad**: الطريقة التي يتم بها

✓ **Confidentiality**: means that certain information should only be known to certain people. معرفة

✓ **Integrity**: means that the data is stored and transferred as intended and that any modification is authorized. معرفة

✓ **Availability**: means that information is accessible to those authorized to view or modify it. الطريقة التي يتم بها

دائما ال Data دائما متوفرة لا مستخدم

# INFORMATION SECURITY (cont.)

- Some security models and researchers identify other properties that secure systems should exhibit.
- The most important of these is **non-repudiation**. → عدم الإنكار  
مستحضر
- **Non-repudiation** means that a subject cannot deny doing something, such as creating, modifying, or sending a resource.
- **For Example:** a legal document, such as a will, must usually be witnessed when it is signed. ان في واحد مستخدم برامض لازم يستجرا
- If there is a dispute about whether the document was correctly executed, the witness can provide evidence that it was.

# INFORMATION SECURITY COMPETENCIES

- IT professionals working in a role with security responsibilities must be competent in a wide range of disciplines, from network and application design to procurement and human resources (HR).
- The following activities might be typical of such a role:
  - ✓ Participate in risk assessments and testing of security systems and make recommendations.
  - ✓ Specify, source, install, and configure secure devices and software.
  - ✓ Set up and maintain document access control and user privilege profiles.
  - ✓ Monitor audit logs, review user privileges, and document access controls.
  - ✓ Manage security-related incident response and reporting.
  - ✓ Create and test business continuity and disaster recovery plans and procedures.
  - ✓ Participate in security training and education programs.

# INFORMATION SECURITY ROLES AND RESPONSIBILITIES

- A **Security Policy** is a formalized statement that defines how security will be implemented within an organization.
- It describes the means the organization will take to protect the confidentiality, availability, and integrity of sensitive data and resources.
- The implementation of a security policy to support the goals of the CIA triad might be very different for a school, a multinational accountancy firm, or a machine tool manufacturer.
- However, each of these organizations, or any other organization should have the same interest in ensuring that its employees, equipment, and data are secure against attack or damage.

# INFORMATION SECURITY ROLES AND RESPONSIBILITIES (cont.)

- As part of the process of adopting an effective organizational security posture, employees must be aware of their responsibilities.
- The structure of security responsibilities will depend on the size and hierarchy of an organization, but these roles are typical.
  - ✓ Overall internal responsibility for security might be allocated to a dedicated department, run by a **Director of Security, Chief Security Officer (CSO)**, or **Chief Information Security Officer (CISO)**.
  - ✓ Managers may have responsibility for a domain, such as building control, ICT, or accounting.
  - ✓ Technical and specialist staff have responsibility for implementing, maintaining, and monitoring the policy.
  - ✓ Non-technical staff have the responsibility of complying with policy and with any relevant legislation.

السياسة  
التي  
تتعلق  
بـ  
السياسة

مطلع من مواصفة ال ادارية



# INFORMATION SECURITY BUSINESS UNITS

## 1. Security Operations Center (SOC)

- A **security operations center (SOC)** is a location where security professionals monitor and protect critical information assets across other business functions, such as finance, operations, sales/marketing, and so on.



هو المركز



اذا بي attack  
الوقت الدقائق الاولى

# INFORMATION SECURITY BUSINESS UNITS (cont.)

فريق الرد على الحوادث

## 2. Incident Response

- A dedicated **cyber incident response team (CIRT)/computer security incident response team (CSIRT)/computer emergency response team (CERT)** as a single point-of-contact for the notification of security incidents.
- This function might be handled by the **SOC**, or it might be established as an independent business unit.

كيفية منع الأذى مستقبلًا

1.1- Compare and Contrast Information Security Roles

**1.2- Compare and Contrast Security Control And Framework Types**

# SECURITY CONTROL CATEGORIES

- Information and cybersecurity assurance is usually considered to take place within an overall process of **business risk management**.
- Implementation of cybersecurity functions is often the **responsibility of the IT department**.
- Some organizations have developed IT service frameworks to provide best practice guides to implementing IT and cybersecurity.
- These frameworks can shape company policies and provide checklists of procedures, activities, and technologies that should ideally be in place.

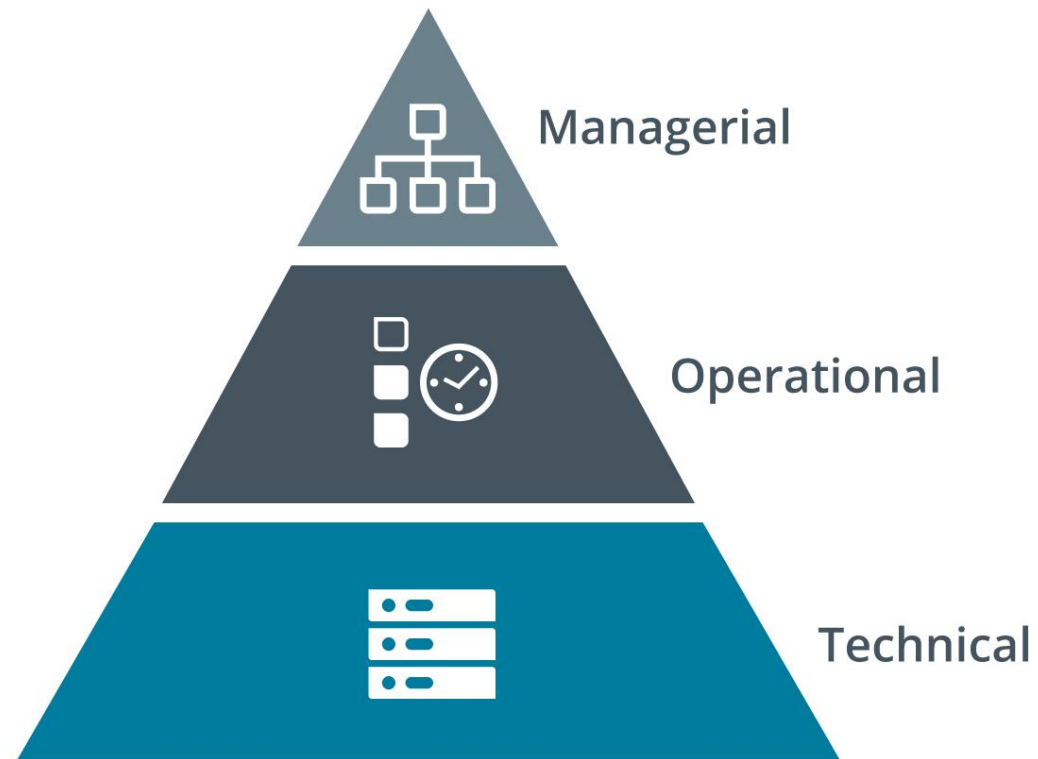
دامله ده دس نی لیه

# SECURITY CONTROL CATEGORIES (cont.)

ان يسهل على الناس

- A **Security Control** is something designed to give a system or data asset the properties of **confidentiality**, **integrity**, **availability**, and **non-repudiation**.
- Controls can be divided into three broad categories, representing the way the control is implemented:
  - ✓ **Technical**—the control is implemented as a system (hardware, software, or firmware), For example, firewalls, antivirus software, and OS access control models are technical controls. Technical controls may also be described as logical controls.
  - ✓ **Operational**—the control is implemented primarily by people rather than systems, For example, security guards and training programs are operational controls rather than technical controls.
  - ✓ **Managerial**—the control gives oversight of the information system, Examples could include risk identification or a tool allowing the evaluation and selection of other security controls.

# SECURITY CONTROL CATEGORIES (cont.)



# SECURITY CONTROL FUNCTIONAL TYPES

- Security controls can also be classified in types according to the **goal** or **function** they perform:

طبع

- ✓ **Preventive**—the control acts to eliminate or reduce the likelihood that an attack can succeed, A preventative control **operates before an attack can take place**, Access control lists (ACL) configured on firewalls and file system objects are preventative-type controls, Anti-malware software also acts as a preventative control, by blocking processes identified as malicious from executing.

مستري قبل ان attack يطلع بسندو

لكش

- ✓ **Detective**—the control may not prevent or deter access, but it will identify and record any attempted or successful intrusion, A detective control **operates during the progress of an attack**, Logs provide one of the best examples of detective-type controls.

في attack عفا لا زام يمتدو



## 02- Explaining Threat Actors and Threat Intelligence

**Ahmed Sultan**

Senior Technical Instructor  
[ahmedsultan.me/about](https://ahmedsultan.me/about)



# Outlines

2.1- Explain Threat Actor Types and Attack Vectors

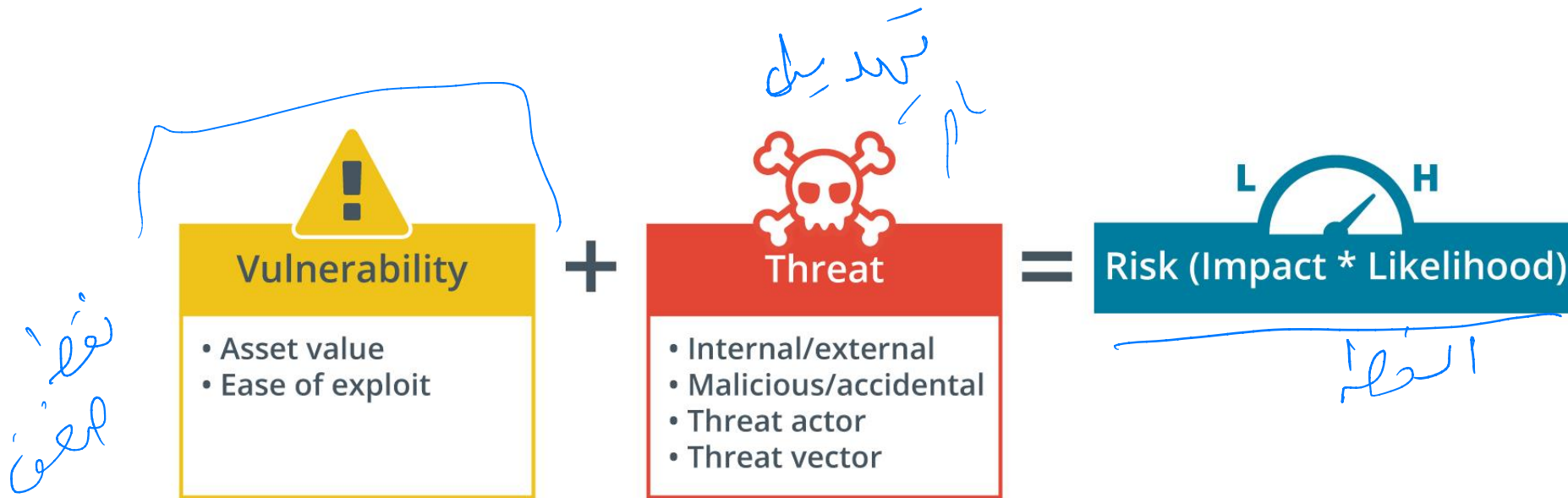
2.2- Explain Threat Intelligence Sources

## **2.1- Explain Threat Actor Types and Attack Vectors**

### **2.2- Explain Threat Intelligence Sources**

# VULNERABILITY, THREAT, AND RISK

- As part of **security assessment** and monitoring, security teams must identify ways in which their systems could be attacked.
- These assessments involve vulnerabilities, threats, and risk.



# VULNERABILITY, THREAT, AND RISK (cont.)

## • Vulnerability

✓ is a weakness that could be triggered accidentally or exploited intentionally to cause a security breach.

✓ Examples of vulnerabilities include:

- Improperly configured or installed hardware or software
- Delays in applying and testing software and firmware patches
- Untested software and firmware patches
- The misuse of software or communication protocols
- Poorly designed network architecture
- Insecure password usage

نقص موجود ہے مثلاً

نقص موجود ہے مثلاً

مثلاً  
Software  
لمتے مودرن  
مثلاً نغزات ویب  
ان مودی پختہ قرار

مثلاً بد تو کد ہے امن

# VULNERABILITY, THREAT, AND RISK (cont.)

- **Threat**

أستأثره أو واحد يستغل الثغرة الأمنية إلى مؤثر

- ✓ is the potential for someone or something to exploit a vulnerability and breach security.
- ✓ A threat may be intentional or unintentional.
- ✓ The person or thing that poses the threat is called a **threat actor** or **threat agent**.
- ✓ The path or tool used by a malicious threat actor can be referred to as the **attack vector**.

- **Risk**

- ✓ is the likelihood and impact (or consequence) of a threat actor exploiting a vulnerability.
- ✓ To assess risk, you identify a vulnerability and then evaluate the likelihood of it being exploited by a threat and the impact that a successful exploit would have.

کیف نفوذ ادا سیک عند الهجوم ؟

① شخصه داخلى او خارجى

# ATTRIBUTES OF THREAT ACTORS

## • Internal/External

شخصه خارجى يحاول يفتق

- ✓ **An external threat actor or agent** is one that has no account or authorized access to the target system.
- ✓ A malicious external threat must infiltrate the security system using malware and/or social engineering.
- ✓ Note that an external actor may perpetrate an attack remotely or on-premises (by breaking into the company's headquarters, for instance).
- ✓ It is the threat actor that is defined as external, rather than the attack method.
- ✓ Conversely, **an internal (or insider) threat actor** is one that has been granted permissions on the system.
- ✓ This typically means an employee, but insider threat can also arise from contractors and business partners.

عن بعد

شخصه داخلى كان بشركه و يعمل اقتران

# ATTRIBUTES OF THREAT ACTORS (cont.)

ما هو دافع الهacker ؟  
البركة لله

- **Intent/Motivation**

- ✓ **Intent** describes what an attacker hopes to achieve from the attack, while **motivation** is the attacker's reason for perpetrating the attack.
- ✓ A malicious threat actor could be motivated by greed, curiosity, or some sort of grievance, for instance.
- ✓ The intent could be to vandalize and disrupt a system or to steal something.
- ✓ Malicious intents and motivations can be contrasted with accidental or unintentional threat actors and agents.
- ✓ Unintentional threat actors represents accidents, oversights, and other mistakes.

# CATEGORIES OF THREAT ACTORS

- To fully assess intent and capability, it is helpful to identify different categories of threat actors.
- **Hackers**
  - ✓ Hacker describes an individual who has the skills to gain access to computer systems through unauthorized or unapproved means.
  - ✓ Originally, hacker was a neutral term for a user who excelled at computer programming and computer system administration.
  - ✓ Hacking into a system was a sign of technical skill and creativity.
  - ✓ The terms **black hat (unauthorized)** and **white hat (authorized)** are used to distinguish these motivations.



# CATEGORIES OF THREAT ACTORS (cont.)

- **Hackers (cont.)**

- ✓ Of course, between black and white lie some shades of gray.
- ✓ A **Gray hat hacker (semi-authorized)** might try to find vulnerabilities in a product or network without seeking the approval of the owner; but they might not try to exploit any vulnerabilities they find.
- ✓ A gray hat might seek voluntary compensation of some sort (a bug bounty), but will not use an exploit as extortion.
- ✓ A white hat hacker always seeks authorization to perform penetration testing of private and proprietary systems.

# CATEGORIES OF THREAT ACTORS (cont.)

- **Script Kiddies**

- ✓ A script kiddie is someone who uses hacker tools without necessarily understanding how they work or having the ability to craft new attacks.
- ✓ Script kiddie attacks might have no specific target or any reasonable goal other than gaining attention or proving technical abilities.

# CATEGORIES OF THREAT ACTORS (cont.)

- **Hacker Teams and Hacktivists**

- ✓ The historical image of a hacker is that of a loner, acting as an individual with few resources or funding.
- ✓ While any such "lone hacker" remains a threat that must be accounted for, threat actors are now likely to work as part of some sort of team or group.
- ✓ The collaborative team effort means that these types of threat actors are able to develop sophisticated tools and novel strategies.
- ✓ A **hacktivist group**, such as [Anonymous](#), [WikiLeaks](#), or [LulzSec](#), uses cyber weapons to promote a political agenda.
- ✓ Hacktivists might attempt to obtain and release confidential information to the public domain, perform denial of service (DoS) attacks, or deface websites.

# STATE ACTORS AND ADVANCED PERSISTENT THREATS

- Most nation states have developed cybersecurity expertise and will use cyber weapons to achieve both military and commercial goals.
- The term **Advanced Persistent Threat (APT)** was coined to understand the behavior underpinning modern types of cyber adversaries.
- Rather than think in terms of systems being infected with a virus or Trojan, an APT refers to the ongoing ability of an adversary to compromise network security—to obtain and maintain access—using a variety of tools and techniques.
- **State actors** have been implicated in many attacks, particularly on energy and health network systems.
- The goals of state actors are primarily espionage and strategic advantage, but it is not unknown for countries—**North Korea** being a good example—to target companies purely for commercial gain.

# ATTACK VECTORS

كيف ينفذ الهجوم

- An **Attack Vector** is the path that a threat actor uses to gain access to a secure system.
- In the majority of cases, gaining access means being able to run malicious code on the target.
- ✓ **Direct access**—this is a type of physical or local attack, The threat actor could exploit an unlocked workstation, use a boot disk to try to install malicious tools, or steal a device, for example.
- ✓ **Removable media**—the attacker conceals malware on a USB thumb drive or memory card and tries to trick employees into connecting the media to a PC, laptop, or smartphone, For some exploits, simply connecting the media may be sufficient to run the malware, In many cases, the attacker may need the employee to open a file in a vulnerable application or run a setup program.

## ATTACK VECTORS (cont.)

- ✓ **Email**—the attacker sends a malicious file attachment via email, or via any other communications system that allows attachments, The attacker needs to use social engineering techniques to persuade or trick the user into opening the attachment.
- ✓ **Remote and wireless**—the attacker either obtains credentials for a remote access or wireless connection to the network or cracks the security protocols used for authentication, Alternatively, the attacker spoofs a trusted resource, such as an access point, and uses it to perform credential harvesting and then uses the stolen account details to access the network.

## ATTACK VECTORS (cont.)

- ✓ Web and social media—malware may be concealed in files attached to posts or presented as downloads, An attacker may also be able to compromise a site so that it automatically infects vulnerable browser software (a drive-by download).
- ✓ Cloud—many companies now run part or all of their network services via Internet-accessible clouds, The attacker only needs to find one account, service, or host with weak credentials to gain access, The attacker is likely to target the accounts used to develop services in the cloud or manage cloud systems, They may also try to attack the cloud service provider (CSP) as a way of accessing the victim system.

2.1- Explain Threat Actor Types and Attack Vectors

**2.2- Explain Threat Intelligence Sources**



# THREAT RESEARCH SOURCES

شرکت‌ها، مراکز تحقیقاتی، موسسات دولتی، بخش خصوصی، مراکز تحقیقاتی، مراکز تحقیقاتی

- Threat research is a counterintelligence gathering effort in which security companies and researchers attempt to discover the **tactics, techniques, and procedures (TTPs)** of modern cyber adversaries.
- There are many companies and academic institutions engaged in primary cybersecurity research.
- Security solution providers with firewall and anti-malware platforms derive a lot of data from their own customers' networks.
- As they assist customers with cybersecurity operations, they are able to analyze and publicize TTPs and their indicators.
- These organizations also operate **honeynets** to try to observe how hackers interact with vulnerable systems.

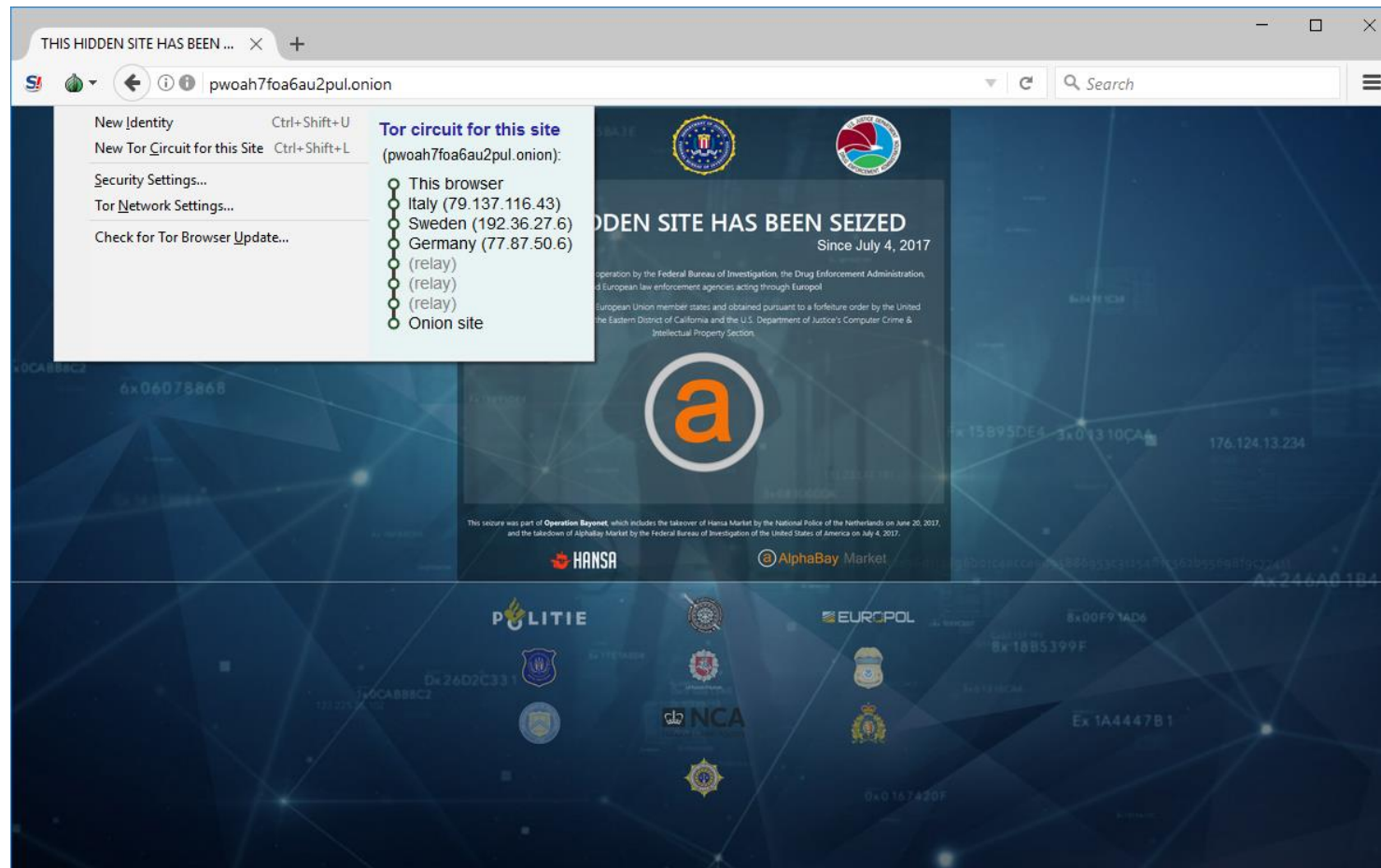
موسسات دولتی، بخش خصوصی، مراکز تحقیقاتی، مراکز تحقیقاتی

## THREAT RESEARCH SOURCES (cont.)

لو اسے بیزل سے dark web اور Data کے نام سے کہا جاتا ہے

- Another primary source of threat intelligence is the dark web.
- The deep web is any part of the World Wide Web that is not indexed by a search engine.
- This includes pages that require registration, pages that block search indexing, unlinked pages, pages using nonstandard DNS, and content encoded in a nonstandard manner.
- Within the deep web, are areas that are deliberately concealed from "regular" browser access.

# THREAT RESEARCH SOURCES (cont.)



# THREAT RESEARCH SOURCES (cont.)

- **Dark net**—a network established as an overlay to Internet infrastructure by software, such as The Onion Router (TOR), Freenet, or I2P, that acts to anonymize usage and prevent a third party from knowing about the existence of the network or analyzing any activity taking place over the network, Onion routing, for instance, uses multiple layers of encryption and relays between nodes to achieve this anonymity.
- **Dark web**—sites, content, and services accessible only over a dark net, While there are dark web search engines, many sites are hidden from them, Access to a dark web site via its URL is often only available via "word of mouth" bulletin boards.

# THREAT INTELLIGENCE PROVIDERS →

لَيْفَ نَعْرِفُ الْفُتْرَا =

- Threat intelligence platforms and feeds are supplied as one of three different commercial models:
- ✓ **Closed/proprietary**—the threat research is made available as a **paid subscription** to a commercial threat intelligence platform.
- The security solution provider will also make the most valuable research available early to platform subscribers in the form of blogs, white papers, and webinars. Some examples of such platforms include:
  - **IBM X-Force Exchange** ([exchange.xforce.ibmcloud.com](https://exchange.xforce.ibmcloud.com))
  - **FireEye** ([fireeye.com/solutions/cyber-threat-intelligence/threat-intelligence-subscriptions.html](https://www.fireeye.com/solutions/cyber-threat-intelligence/threat-intelligence-subscriptions.html))
  - **Recorded Future** ([recordedfuture.com/solutions/threat-intelligence-feeds](https://www.recordedfuture.com/solutions/threat-intelligence-feeds))

مِنْ أَهْلِ الْفُتْرَا =

# THREAT INTELLIGENCE PROVIDERS (cont.)

The screenshot displays the IBM X-Force Exchange dashboard, a platform for threat intelligence. The top navigation bar includes the IBM X-Force Exchange logo, a search bar, and links for 'Create IBMid' and 'Log In'. The main header area features the tagline 'Research, Collaborate and Act on threat intelligence' and a search bar with the placeholder text 'Search by Application name, IP address, URL, Vulnerability, MD5, #Tag...'. A 'Trending' section on the right lists popular tags and their associated counts: #blacklist (185,153,196.97), #malware (149,202,251.78), 208.97.139.113 (62,210.54.33), and 66.240.205.34 (#malware-loc-url).

The dashboard is divided into several sections:

- IBM Advanced Threat Protection Feed:** A section for identifying malicious threats in real-time. It includes a description of the feed and a 'Start your 30-day trial' button.
- Early Warning Feed:** A section for staying ahead of threats. It lists several domains: emails-apple.com, midadvancetypeappclicks.top, and btvmxpk.com, each with a 'Registered' date of Dec 16, 2019. It also includes a 'Start your 30-day trial' button.
- IRIS Threat Intelligence:** A section for premium threat intelligence on threat groups, industries, and malware. It lists several reports: ITG08 Analysis Report, Pharmaceutical Manufacturing Industry Profile, BadFlick Analysis Report, and others.
- Recent IBM X-Force Advisories:** A section for collections created by the IBM X-Force team. It lists two advisories: 'New Monero Cryptominer Discovered' and 'Anchor Targeting PoS Systems', both dated Dec 13, 2019.
- Threat Activity:** A section for malicious IP addresses in the last hour. It includes a table with the following data:

Category	Count
Total	976
Command and Control	0
Spam	670
Malware	0
Scanning	333

# THREAT INTELLIGENCE PROVIDERS (cont.)

- ✓ Vendor websites — proprietary threat intelligence is not always provided at cost. تأخر ال Windows
- All types of security, hardware, and software vendors make huge amounts of threat research available via their websites as a general benefit to their customers.
  - One example is Microsoft's Security Intelligence blog ([microsoft.com/security/blog/microsoft-security-intelligence](https://microsoft.com/security/blog/microsoft-security-intelligence)).

# THREAT INTELLIGENCE PROVIDERS (cont.)

- ✓ **Public/private information sharing centers**—in many critical industries, have been set up to share threat intelligence and promote best practice ([nationalisacs.org/member-isacs](https://nationalisacs.org/member-isacs)).
- These are sector-specific resources for companies and agencies working in critical industries, such as power supply, financial markets, or aviation. Where there is no coverage by an ISAC, local industry groups and associations may come together to provide mutual support.



# THREAT INTELLIGENCE PROVIDERS (cont.)

- ✓ **Open source intelligence (OSINT)**—some companies operate threat intelligence services on an open-source basis, earning income from consultancy rather than directly from the platform or research effort.
- Some examples include:
  - AT&T Security, previously Alien Vault Open Threat Exchange (OTX) ([otx.alienvault.com](https://otx.alienvault.com))
  - Malware Information Sharing Project (MISP) ([misp-project.org/feeds](https://misp-project.org/feeds))
  - Spamhaus ([spamhaus.org/organization](https://spamhaus.org/organization))
  - VirusTotal ([virustotal.com](https://virustotal.com))

# SECURITY CONTROL FUNCTIONAL TYPES (cont.)

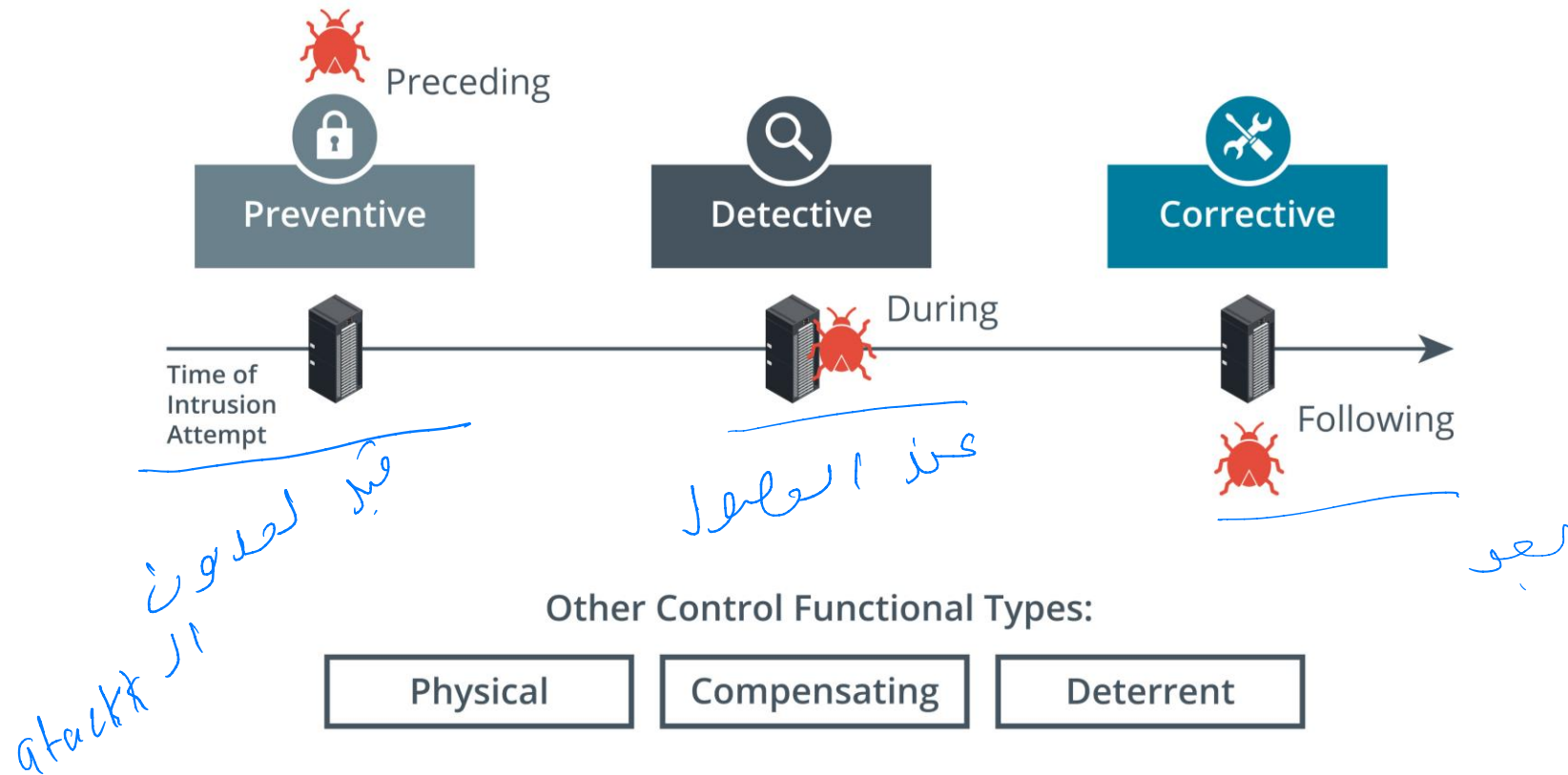
- Security controls can also be classified in types according to the **goal** or **function** they perform (cont.)

نقطة

✓ **Corrective**—the control acts to eliminate or reduce the impact of an intrusion event, A corrective control is **used after an attack**, A good example is a backup system that can restore data that was damaged during an intrusion, Another example is a patch management system that acts to eliminate the vulnerability exploited during the attack.

نقطة  
التي  
تستخدم  
بعد  
الهجوم

# SECURITY CONTROL FUNCTIONAL TYPES (cont.)



# SECURITY CONTROL FUNCTIONAL TYPES (cont.)

- While most controls can be classed functionally as preventative, detective, or corrective, a few other types can be used to define other cases:
  - ✓ **Physical**—controls such as alarms, gateways, locks, lighting, security cameras, and guards that deter and detect access to premises and hardware are often classed separately.
  - ✓ **Deterrent**—the control may not physically or logically prevent access, but psychologically discourages an attacker from attempting an intrusion. This could include signs and warnings of legal penalties against trespass or intrusion.
  - ✓ **Compensating**—the control serves as a substitute for a principal control, as recommended by a security standard, and affords the same (or better) level of protection but uses a different methodology or technology.

# ISO AND CLOUD FRAMEWORKS

- The **International Organization for Standardization (ISO)** has produced a cybersecurity framework in conjunction with the **International Electrotechnical Commission (IEC)**.
- The framework was established in 2005 and revised in 2013.
- **ISO 27001** is part of an overall 27000 series of information security standards, also known as **27K**.
- Of these, **27002** classifies security controls, **27017** and **27018** reference cloud security, and **27701** focuses on personal data and privacy.

# ISO AND CLOUD FRAMEWORKS (cont.)

- [ISO 31K \(iso.org/iso-31000-risk-management.html\)](https://iso.org/iso-31000-risk-management.html) is an overall framework for **enterprise risk management (ERM)**.
- **ERM** considers risks and opportunities beyond cybersecurity by including financial, customer service, competition, and legal liability factors.
- **ISO 31K** establishes best practices for performing risk assessments.
- The not-for-profit organization [Cloud Security Alliance \(CSA\)](#) produces various resources to assist **cloud service providers (CSP)** in setting up and delivering secure cloud platforms.
- These resources can also be useful for cloud consumers in evaluating and selecting cloud services.