CompTIA

Security+

SY0 - 601

02- Explaining Threat Actors and Threat Intelligence

Ahmed Sultan
Senior Technical Instructor
ahmedsultan.me/about

Outlines

2.1- Explain Threat Actor Types and Attack Vectors

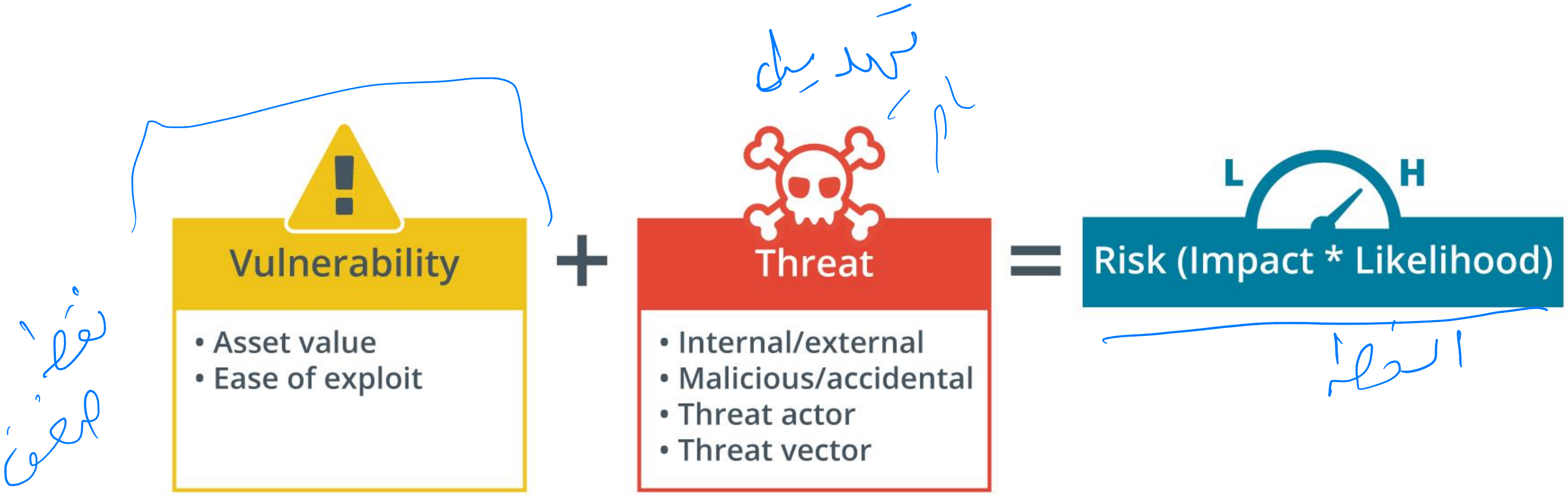
2.2- Explain Threat Intelligence Sources

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.



نقاط
الضعف

Vulnerability

- Asset value
- Ease of exploit

+

تهديد

Threat

- Internal/external
- Malicious/accidental
- Threat actor
- Threat vector

=

Risk (Impact * Likelihood)

الخطر

VULNERABILITY, THREAT, AND RISK (cont.)

- **Vulnerability**

نقاط ضعف موجودة يتم استغلالها

  ✓ 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

كلمة مرور ضعيفة

مثلا
software
لسه محدثة
فيها ثغرات وعيوب
ان هاكر يخترقك

مثلا بروتوكول غير امن

VULNERABILITY, THREAT, AND RISK (cont.)

- **Threat**

احتماليه انو واحد يستغل النقاط الضعف الي فوق

  - ✓ 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.

كيف نوقف اول شيء عند الهجوم ؟

ATTRIBUTES OF THREAT ACTORS

١) شخص داخلي او خارجي

- **Internal/External**

  شخص خارجي يحاول يخترق

  - ✓ **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 (عن بعد) 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.

    شخص داخلي كان بشركه و يعمل اختراق
  - ✓ This typically means an employee, but insider threat can also arise from contractors and business partners.

ATTRIBUTES OF THREAT ACTORS (cont.)

Q ما هو دافع للشخص
الي عمل attack ؟

- **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 يحدث ال attack

- 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

شركة لها قسم ابحاث ؛ يوميا بدور على اي ثغرات عشان يعرفوا تواجد الهجمات

- 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.

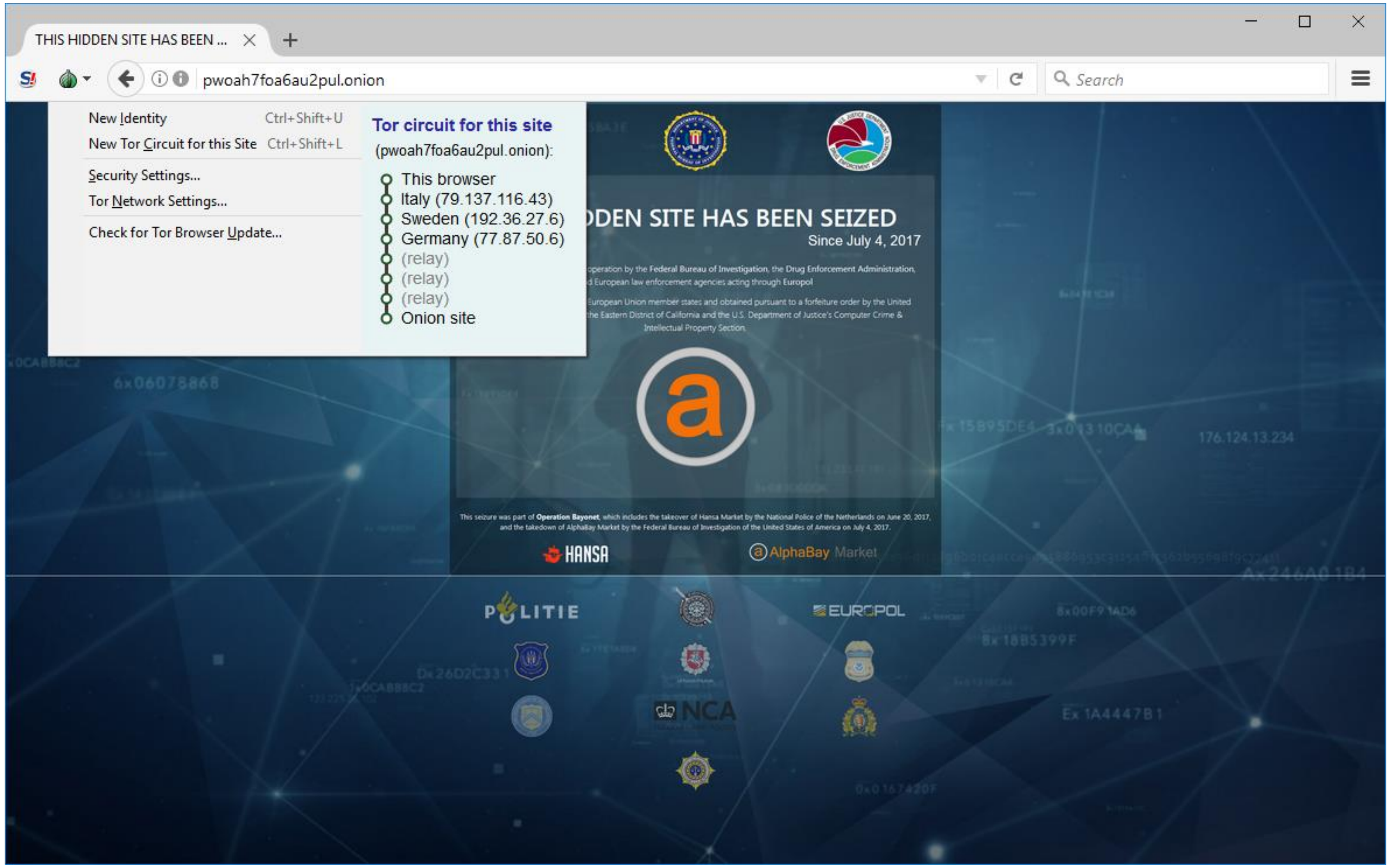
مصيدة عن طريق شبكة وهمية

THREAT RESEARCH SOURCES (cont.)

اول اشي بنزل عل darkweb ال Data تاعت الشركة لما تنهكر

- 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.)


THIS HIDDEN SITE HAS BEEN ...
pwoah7foa6au2pul.onion
Search
New Identity Ctrl+Shift+U
New Tor Circuit for this Site Ctrl+Shift+L
Security Settings...
Tor Network Settings...
Check for Tor Browser Update...

Tor circuit for this site
(pwoah7foa6au2pul.onion):

- This browser
- Italy (79.137.116.43)
- Sweden (192.36.27.6)
- Germany (77.87.50.6)
- (relay)
- (relay)
- (relay)
- Onion site

DEN SITE HAS BEEN SEIZED

Since July 4, 2017

operation by the Federal Bureau of Investigation, the Drug Enforcement Administration,
d European law enforcement agencies acting through Europol

European Union member states and obtained pursuant to a forfeiture order by the United
the Eastern District of California and the U.S. Department of Justice's Computer Crime &
Intellectual Property Section.

This seizure was part of **Operation Bayonet**, which includes the takeover of Hansa Market by the National Police of the Netherlands on June 20, 2017, and the takedown of AlphaBay Market by the Federal Bureau of Investigation of the United States of America on July 4, 2017.

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

كيف نعرف اخر الثغرات

- Threat intelligence platforms and feeds are supplied as one of three different commercial models:

اخر

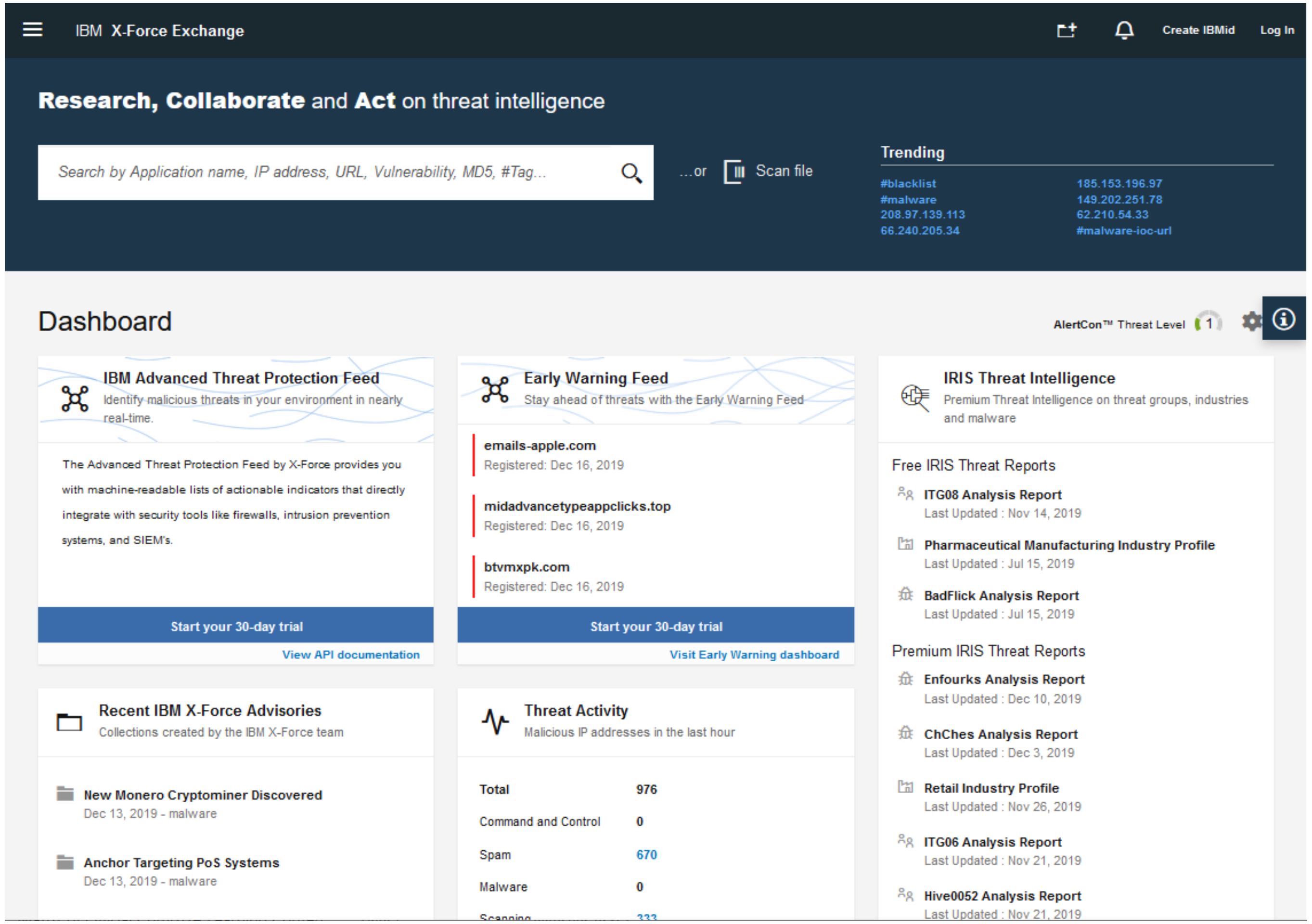
✓Closed/proprietary—the threat research is made available as a **paid subscription** to a commercial threat intelligence platform.

- 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:

شركات يطلعوا اخر ثغرات

  - ➢ **IBM X-Force Exchange** (exchange.xforce.ibmcloud.com)
  - ➢ **FireEye** (fireeye.com/solutions/cyber-threat-intelligence/threat-intelligence-subscriptions.html)
  - ➢ **Recorded Future** (recordedfuture.com/solutions/threat-intelligence-feeds)

THREAT INTELLIGENCE PROVIDERS (cont.)



IBM X-Force Exchange

Create IBMid

Log In

Research, Collaborate and **Act** on threat intelligence

Search by Application name, IP address, URL, Vulnerability, MD5, #Tag...

...or Scan file

Trending

#blacklist	185.153.196.97
#malware	149.202.251.78
208.97.139.113	62.210.54.33
66.240.205.34	#malware-ioc-url

Dashboard

AlertCon™ Threat Level 1

IBM Advanced Threat Protection Feed

Identify malicious threats in your environment in nearly real-time.

The Advanced Threat Protection Feed by X-Force provides you with machine-readable lists of actionable indicators that directly integrate with security tools like firewalls, intrusion prevention systems, and SIEM's.

Start your 30-day trial

View API documentation

Early Warning Feed

Stay ahead of threats with the Early Warning Feed

emails-apple.com
Registered: Dec 16, 2019

midadvancetypeappclicks.top
Registered: Dec 16, 2019

btvmxpk.com
Registered: Dec 16, 2019

Start your 30-day trial

Visit Early Warning dashboard

IRIS Threat Intelligence

Premium Threat Intelligence on threat groups, industries and malware

Free IRIS Threat Reports

ITG08 Analysis Report
Last Updated : Nov 14, 2019

Pharmaceutical Manufacturing Industry Profile
Last Updated : Jul 15, 2019

BadFlick Analysis Report
Last Updated : Jul 15, 2019

Premium IRIS Threat Reports

Enfourks Analysis Report
Last Updated : Dec 10, 2019

ChChes Analysis Report
Last Updated : Dec 3, 2019

Retail Industry Profile
Last Updated : Nov 26, 2019

ITG06 Analysis Report
Last Updated : Nov 21, 2019

Hive0052 Analysis Report
Last Updated : Nov 21, 2019

Recent IBM X-Force Advisories

Collections created by the IBM X-Force team

New Monero Cryptominer Discovered
Dec 13, 2019 - malware

Anchor Targeting PoS Systems
Dec 13, 2019 - malware

Threat Activity

Malicious IP addresses in the last hour

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

THREAT INTELLIGENCE PROVIDERS (cont.)

تاعت ال Windows

✓Vendor websites—proprietary threat intelligence is not always provided at cost.

- 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).

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).

- 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)
  - ➢ Malware Information Sharing Project (MISP) (misp-project.org/feeds)
  - ➢ Spamhaus (spamhaus.org/organization)
  - ➢ VirusTotal (virustotal.com)

SECURITY CONTROL FUNCTIONAL TYPES (cont.)

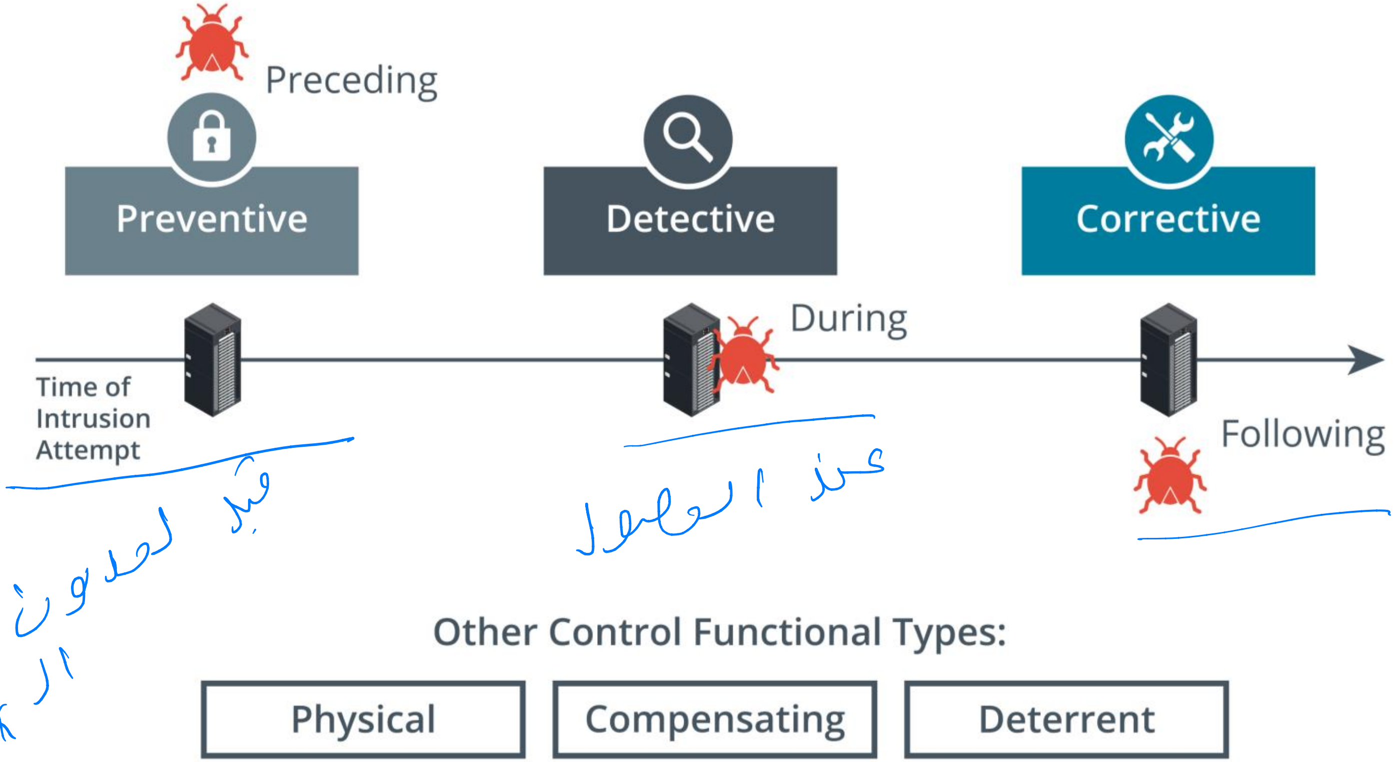
- Security controls can also be classified in types according to the **goal** or **function** they perform (cont.)

تصحيح

✓ 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.

يقلل الـ مخاطر الـ atakk

SECURITY CONTROL FUNCTIONAL TYPES (cont.)



قبل الحدوث ال attack

عند الحصول

بعد

Other Control Functional Types:

Physical

Compensating

Deterrent

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) 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.