02- Explaining Threat Actors and Threat Intelligence

Outlines

2.1- Explain Threat Actor Types and Attack Vectors

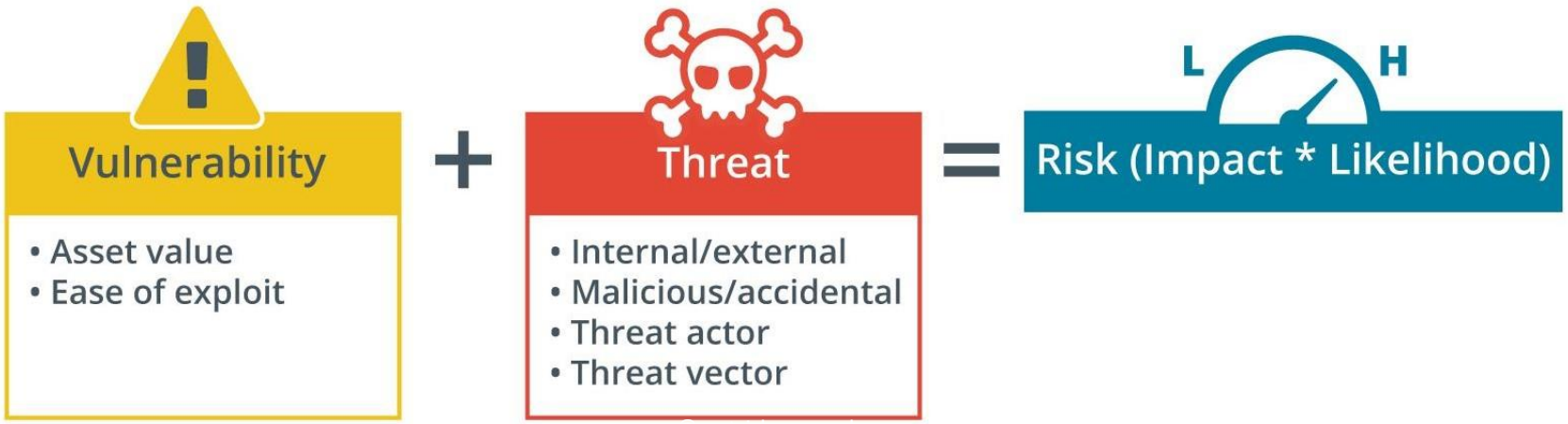
2.2- Explain Threat Intelligence Sources

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.
  - كجزء من التقييم الأمني والمراقبة، يجب على الفرق الأمنية تحديد الطرق التي يمكن من خلالها مهاجمة أنظمتها.
  - تتضمن هذه التقييمات نقاط الضعف والتهديدات والمخاطر



VULNERABILITY, THREAT, AND RISK (cont.)

- **Vulnerability**
  - ✓ is a weakness that could be triggered accidentally or exploited intentionally to cause a security breach.
    هي نقطة ضعف يمكن أن تحدث عن طريق الخطأ أو يتم استغلالها عمدًا للتسبب في اختراق أمني.
  - ✓ **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

VULNERABILITY, THREAT, AND RISK (cont.)

- **Threat**
  - ✓ 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**.
  - ✓ هو احتمال قيام شخص ما أو شيء ما باستغلال ثغرة أمنية وخرق الأمان.وقد يكون التهديد مقصودًا أو غير مقصود.يُطلق على الشخص أو الشيء الذي يشكل التهديد اسم ممثل التهديد أو وكيل التهديد.يمكن الإشارة إلى المسار أو الأداة التي يستخدمها ممثل التهديد الخبيث باسم ناقل الهجوم
- **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.

هو احتمالية وتأثير (أو نتيجة) جهة التهديد التي تستغل الثغرة الأمنية.لتقييم المخاطر، يمكنك تحديد الثغرة الأمنية ثم تقييم احتمالية استغلالها من خلال تهديد والتأثير الذي قد يحدثه استغلال ناجح.

ATTRIBUTES OF THREAT ACTORS

- **Internal/External**
  - ✓ **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.

ممثل أو وكيل التهديد الخارجي هو الذي ليس لديه حساب أو وصول مصرح به إلى النظام المستهدف.يجب أن يتسلل التهديد الخارجي الضار إلى نظام الأمان باستخدام البرامج الضارة و/أو الهندسة الاجتماعية.لاحظ أن جهة فاعلة خارجية قد ترتكب هجومًا عن بعد أو داخل مقر الشركة (عن طريق اقتحام المقر الرئيسي للشركة، على سبيل المثال).إن جهة التهديد هي التي يتم تعريفها على أنها خارجية، وليست طريقة الهجوم.وعلى العكس من ذلك، فإن جهة التهديد الداخلية (أو الداخلية) هي الجهة التي تم منحها أذونات على النظام.ويعني هذا عادةً موظفًا، ولكن التهديد الداخلي يمكن أن ينشأ أيضًا من المقاولين وشركاء الأعمال.

ATTRIBUTES OF THREAT ACTORS (cont.)

- **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.
  - ✓ النية تصف ما يأمل المهاجم في تحقيقه من الهجوم، في حين أن الدافع هو سبب المهاجم لارتكاب الهجوم.يمكن أن يكون الدافع وراء التهديد الخبيث هو الجشع أو الفضول أو نوع من التظلم، على سبيل المثال.يمكن أن يكون القصد تخريب النظام وتعطيله أو سرقة شيء ما.يمكن أن تتناقض النوايا والدوافع الخبيثة مع الجهات الفاعلة والوكلاء التهديديين العرضيين أو غير المقصودين.تمثل جهات التهديد غير المقصودة حوادث وإغفالات وأخطاء أخرى.

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.
  - ✓ ولتقييم النوايا والقدرة بشكل كامل، من المفيد تحديد فئات مختلفة من الجهات التهديدية.قراصنةيصف الهاكر الفرد الذي لديه المهارات اللازمة للوصول إلى أنظمة الكمبيوتر من خلال وسائل غير مصرح بها أو غير معتمدة.في الأصل، كان الهاكر مصطلحًا محايدًا للمستخدم الذي تفوق في الكمبيوترالبرمجة وإدارة أنظمة الكمبيوتر.كان اختراق النظام علامة على المهارة التقنية والإبداع.يتم استخدام مصطلحات القبعة السوداء (غير المصرح بها) والقبعة البيضاء (المصرح بها) للتمييز بين هذه الدوافع.

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.
  - ✓ وبطبيعة الحال، بين الأسود والأبيض تكمن بعض ظلال اللون الرمادي.قد يحاول متسلل القبعة الرمادية (شبه مرخص) العثور على نقاط الضعف في منتج أو شبكة دون الحصول على موافقة المالك؛ لكنهم قد لا يحاولون استغلال أي نقاط ضعف يجدونها.قد يسعى أصحاب القبعة الرمادية إلى الحصول على تعويض طوعي من نوع ما (مكافأة الأخطاء)، لكنهم لن يستخدموا برمجية إكسبلويت كوسيلة للابتزاز.يسعى متسلل القبعة البيضاء دائمًا إلى الحصول على إذن لإجراء اختبار اختراق للأنظمة الخاصة والمملوكة.

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.
  - ✓طفل النص هو شخص يستخدم أدوات القرصنة دون أن يفهم بالضرورة كيفية عملها أو أن يكون لديه القدرة على صياغة هجمات جديدة.
  - ✓قد لا يكون لهجمات الأطفال النصية هدف محدد أو أي هدف معقول بخلاف جذب الانتباه أو إثبات القدرات التقنية.

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.
  - ✓الصورة التاريخية للهاكر هي صورة الشخص المنعزل، الذي يتصرف كفرد مع القليل من الموارد أو التمويل.وفي حين أن مثل هذا "المتسلل المنفرد" لا يزال يمثل تهديدًا يجب أخذه في الاعتبار، فمن المرجح الآن أن تعمل الجهات الفاعلة في مجال التهديد كجزء من نوع ما من الفريق أو المجموعة.ويعني جهد الفريق التعاوني أن هذه الأنواع من الجهات التهديدية قادرة على تطوير أدوات متطورة واستراتيجيات جديدة.تستخدم مجموعة من الناشطين في مجال القرصنة، مثل Anonymous أو WikiLeaksأو LulzSec، الأسلحة السيبرانية لتعزيز أجندة سياسية.قد يحاول المتسللون الحصول على معلومات سرية ونشرها في المجال العام، أو تنفيذ هجمات رفض الخدمة ((DoS، أو تشويه مواقع الويب

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.

الجهات الحكومية والتهديدات المستمرة المتقدمة

لقد طورت معظم الدول خبرة في مجال الأمن السيبراني وستستخدم الأسلحة السيبرانية لتحقيق الأهداف العسكرية والتجارية.
تمت صياغة مصطلح التهديد المستمر المتقدم (APT) لفهم التهديدات المستمرة المتقدمة السلوك الذي يقوم عليه الأنواع الحديثة من الخصوم السيبرانيين.

بدلاً من التفكير في إصابة الأنظمة بفيروس أو حصان طروادة، تشير التهديدات المستمرة المستمرة إلى قدرة الخصم المستمرة على اختراق أمان الشبكة - للحصول على الوصول والحفاظ عليه - باستخدام مجموعة متنوعة من الأدوات والتقنيات.

وقد تورطت الجهات الحكومية في العديد من الهجمات، لا سيما على أنظمة شبكات الطاقة والصحة.

إن أهداف الجهات الحكومية هي في المقام الأول التجسس وتحقيق ميزة استراتيجية، ولكن ليس من المستغرب أن تستهدف الدول -كوريا الشمالية مثالاً جيدًا- الشركات لتحقيق مكاسب تجارية بحتة.

ATTACK VECTORS

- 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.

✓ناقل الهجوم هو المسار الذي يستخدمه ممثل التهديد للوصول إلى نظام آمن.في معظم الحالات، يعني الحصول على حق الوصول القدرة على تشغيل تعليمات برمجية ضارةعلى الهدف.الوصول المباشر - هذا نوع من الهجوم الفعلي أو المحلي، حيث يمكن لممثل التهديد استغلال محطة عمل غير مؤمّنة، أو استخدام قرص تمهيد لمحاولة تثبيت أدوات ضارة، أو سرقة جهاز، على سبيل المثال.الوسائط القابلة للإزالة - يقوم المهاجم بإخفاء البرامج الضارة على محرك أقراص USBصغير أو بطاقة ذاكرة ويحاول خداع الموظفين لتوصيل الوسائط بجهاز كمبيوتر أو كمبيوتر محمول أو هاتف ذكي. بالنسبة لبعض عمليات الاستغلال، قد يكون توصيل الوسائط ببساطة كافيًا لتشغيل البرامج الضارة، في كثير من الحالات، قد يطلب المهاجم من الموظف فتح ملف في تطبيق ضعيف أو تشغيل برنامج إعداد

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.

✓البريد الإلكتروني - يرسل المهاجم مرفق ملف ضار عبر البريد الإلكتروني، أو عبر أي نظام اتصالات آخر يسمح بالمرفقات، ويحتاج المهاجم إلى استخدام تقنيات الهندسة الاجتماعية لإقناع المستخدم أو خداعه لفتح المرفق.عن بعد ولاسلكي - يحصل المهاجم إما على بيانات اعتماد للوصول عن بعد أو اتصال لاسلكي بالشبكة أو يخترق بروتوكولات الأمان المستخدمة للمصادقة، وبدلاً من ذلك، ينتحل المهاجم موردًا موثوقًا به، مثل نقطة الوصول، ويستخدمه لتنفيذ عملية جمع بيانات الاعتماد ثم يستخدم تفاصيل الحساب المسروق للوصول إلى الشبكة

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.

✓الويب ووسائل التواصل الاجتماعي - قد يتم إخفاء البرامج الضارة في ملفات مرفقة بالمنشورات أو يتم تقديمها كتنزيلات، وقد يتمكن المهاجم أيضًا من اختراق موقع ما بحيث يصيب تلقائيًا برنامج المتصفح الضعيف (التنزيل من محرك الأقراص).السحابة - تقوم العديد من الشركات الآن بتشغيل جزء من خدمات شبكتها أو جميعها عبر سحابات يمكن الوصول إليها عبر الإنترنت، ويحتاج المهاجم فقط إلى العثور على حساب أو خدمة أو مضيف واحد ببيانات اعتماد ضعيفة للوصول، ومن المرجح أن يستهدف المهاجم الحسابات المستخدمة للتطوير. الخدمات السحابية أو إدارة الأنظمة السحابية، وقد يحاولون أيضًا مهاجمة مزود الخدمة السحابية ((CSPكوسيلة للوصول إلى النظام الضحية.

2.1- Explain Threat Actor Types and Attack Vectors

2.2- Explain Threat Intelligence Sources

THREAT RESEARCH SOURCES

- 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.

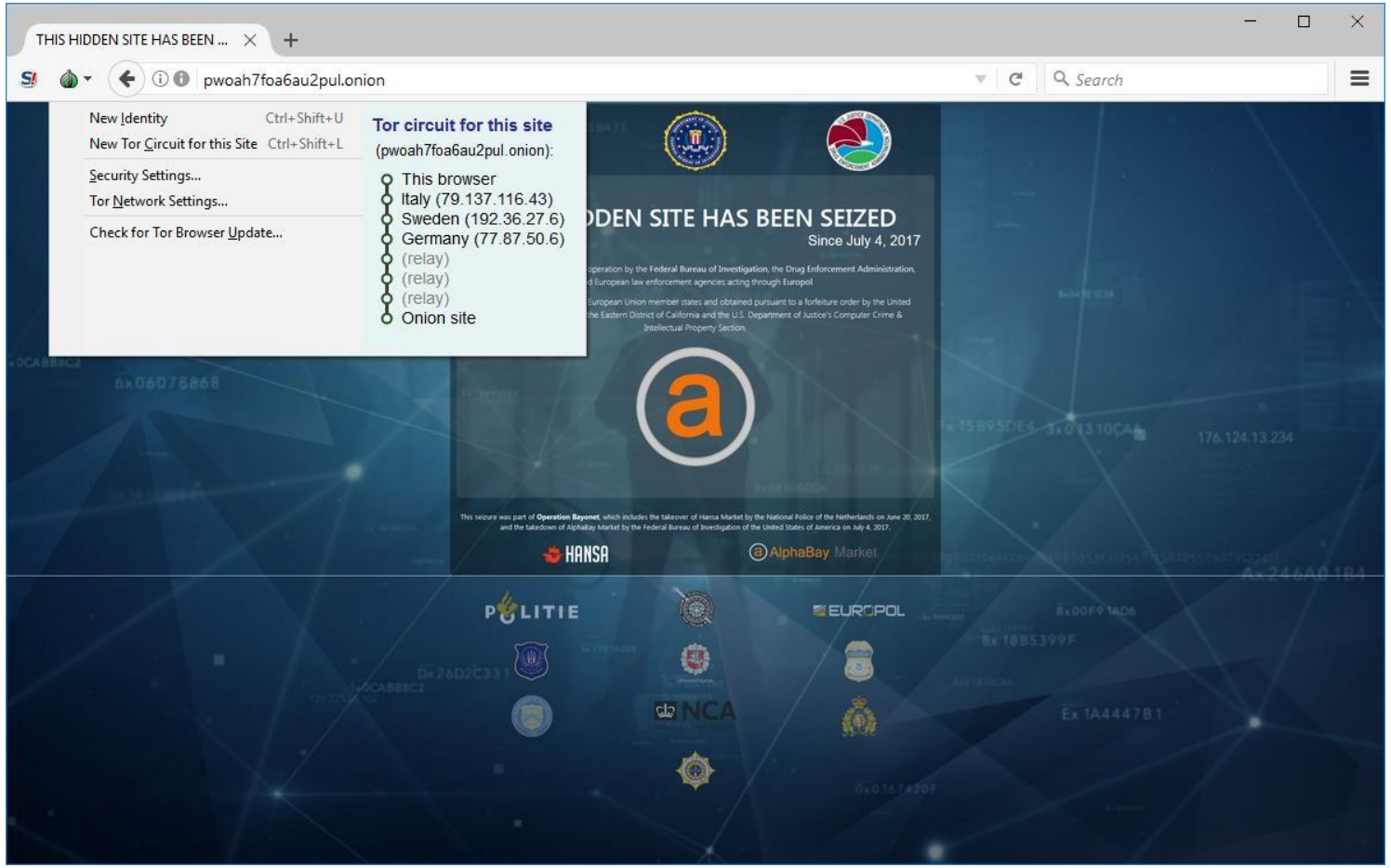
- أبحاث التهديدات هي جهود جمع معلومات استخباراتية مضادة تحاول من خلالها الشركات الأمنية والباحثون اكتشاف التكتيكات والتقنيات والإجراءات ((TTPsالخاصة بالخصوم السيبرانيين المعاصرين.هناك العديد من الشركات والمؤسسات الأكاديمية العاملة في مجال أبحاث الأمن السيبراني الأولية.يستمد موفرو الحلول الأمنية المزودون بجدار الحماية ومنصات مكافحة البرامج الضارة الكثير من البيانات من شبكات عملائهم.نظرًا لأنهم يساعدون العملاء في عمليات الأمن السيبراني، فهم قادرون على تحليل ونشر TTPsومؤشراتها.تقوم هذه المنظمات، أيضًا بتشغيل شبكات العسل لمحاولة مراقبة كيفية تفاعل المتسللين مع الأنظمة الضعيفة.

THREAT RESEARCH SOURCES (cont.)

- 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.

المصدر الرئيسي الآخر لمعلومات التهديد هو شبكة الإنترنت المظلمة.شبكة الويب العميقة هي أي جزء من شبكة الويب العالمية لا تتم فهرسته بواسطة محرك بحث.يتضمن ذلك الصفحات التي تتطلب التسجيل، والصفحات التي تحظر فهرسة البحث، والصفحات غير المرتبطة، والصفحات التي تستخدم DNSغير قياسي، والمحتوى المشفر بطريقة غير قياسية.توجد في شبكة الويب العميقة مناطق تم إخفاؤها عمدًا عن الوصول إلى المتصفح "العادي".

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.

- الشبكة المظلمة - شبكة تم إنشاؤها كتراكب للبنية التحتية للإنترنت بواسطة برامج، مثل Onion Router (TOR)أو Freenetأو I2P، والتي تعمل على إخفاء هوية الاستخدام ومنع طرف ثالث من معرفة وجود الشبكة أو تحليل أي منها. النشاط الذي يحدث عبر الشبكة، يستخدم التوجيه البصلي، على سبيل المثال، طبقات متعددة من التشفير والمرحلات بين العقد لتحقيق إخفاء الهوية.
- الويب المظلم - المواقع والمحتوى والخدمات التي لا يمكن الوصول إليها إلا عبر شبكة مظلمة، على الرغم من وجود محركات بحث على الويب المظلم، إلا أن العديد من المواقع مخفية عنها، وغالبًا ما يكون الوصول إلى موقع الويب المظلم عبر عنوان URLالخاص به متاحًا فقط عبر "الكلام الشفهي". لوحات الإعلانات.

THREAT INTELLIGENCE PROVIDERS

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

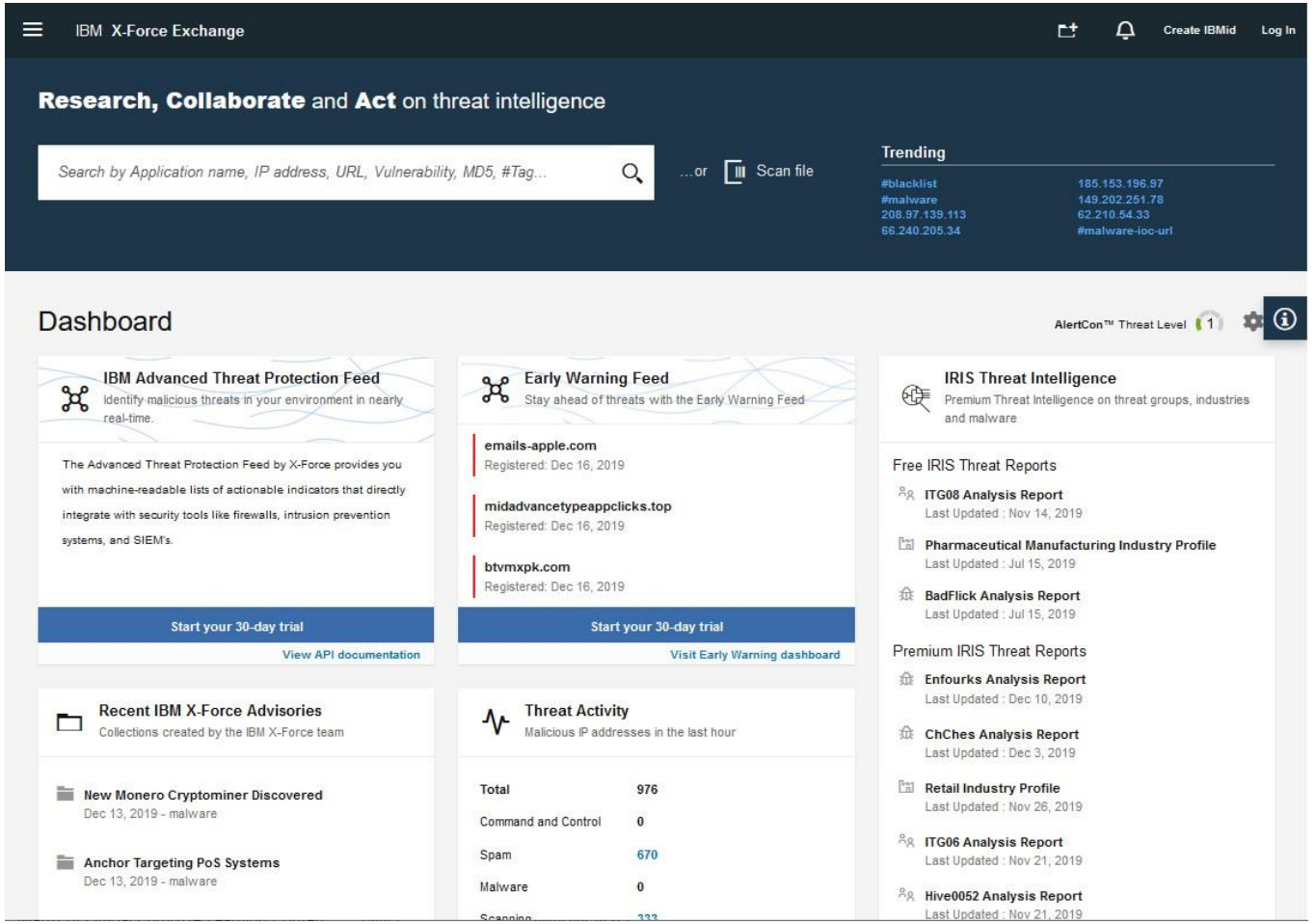
✓ Closed/proprietary—the threat research is made available as a **paid subscription** to a commercial threat intelligence platform.

- 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.

- يتم توفير منصات وموجزات معلومات التهديدات كواحد من ثلاثة نماذج تجارية مختلفة:مغلق/ملكي — يتم توفير أبحاث التهديدات كاشتراك مدفوع لمنصة تجارية لاستخبارات التهديدات.سيقوم موفر الحلول الأمنية أيضًا بتوفير الأبحاث الأكثر قيمة مبكرًا لمشتركي النظام الأساسي في شكل مدونات وتقارير تقنية وندوات عبر الإنترنت.

- Some examples of such platforms include:
  - **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.)



THREAT INTELLIGENCE PROVIDERS (cont.)

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

✓المواقع الإلكترونية للموردين - لا يتم دائمًا توفير المعلومات المتعلقة بالتهديدات الخاصة مقابل التكلفة.

- 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.

- يقوم بائعو جميع أنواع الأجهزة الأمنية والبرمجيات بتوفير كميات هائلة من أبحاث التهديدات عبر مواقعهم الإلكترونية كفائدة عامة لعملائهم.

- 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).

✓تم إنشاء مراكز مشاركة المعلومات العامة/الخاصة - في العديد من الصناعات الحيوية، لمشاركة معلومات التهديدات وتعزيز أفضل الممارسات

- 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.

- هذه موارد خاصة بقطاعات محددة للشركات والوكالات العاملة في الصناعات الحيوية، مثل إمدادات الطاقة أو الأسواق المالية أو الطيران. في حالة عدم وجود تغطية من قبل ISAC، قد تجتمع مجموعات وجمعيات الصناعة المحلية معًا لتقديم الدعم المتبادل.

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.

✓الذكاء مفتوح المصدر (OSINT) - تدير بعض الشركات خدمات استخبارات التهديدات على أساس مفتوح المصدر، وتحصل على دخل من الاستشارات وليس مباشرة من النظام الأساسي أو الجهود البحثية.

- 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)