Cybersecurity Fundamentals

Cybersecurity: On the Defense

Financial impacts

10 Minutes

Module overview

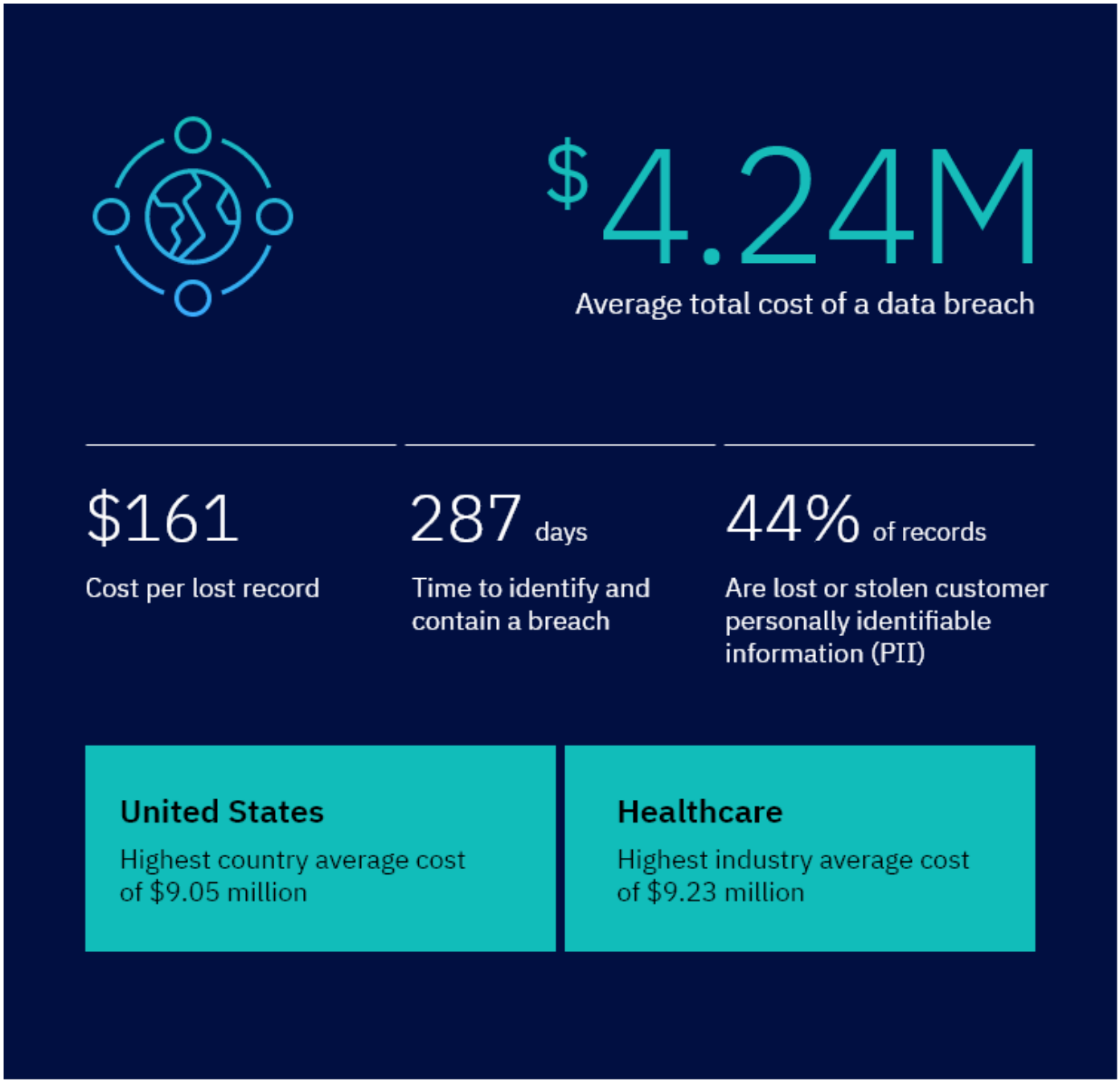
You have learned about the basics of cybersecurity and the various types of threats an organization may face. This module focuses on the "defensive" side of cybersecurity, meaning organizations and their techniques and tools. How do they detect, protect against, and respond to attacks? You will learn about these topics:

- Financial impacts of cyber crime to organizations
- Security maturity
- A security strategy approach that organizations can use to defend against cyber attacks using the 10 Steps to Security by the National Cyber Security Centre
- Common approaches organizations take to:
    - Prevent cyber attacks
    - Detect cyber attacks
    - Respond and recover from cyber attacks
- Key properties for secure communications
- Symmetric and asymmetric cryptography
- Threat intelligence sources and benefits for organizations

Cost of data breaches

First, let's learn about how detrimental cyber attacks can be to organizations and get a better idea about what the cost can be. The cost of cyber crime to organizations can be both hard to predict in advance and very damaging.

The annual **Cost of a Data Breach Report (https://www.ibm.com/security/data-breach)**, conducted by the Ponemon Institute and sponsored by IBM Security, analyzes data breach costs reported by hundreds of organizations around the world and across industries. According to the 2021 report, **the average global total cost of a data breach is $4.24M.** The cost of a data breach has increased by 11.9% since 2015. Review this diagram to learn more key facts about the costs of data breaches. The amounts are in US dollars.



Source: **Cost of a Data Breach Report 2021 (https://www.ibm.com/downloads/cas/OJDVQGRY)**, IBM Security, study conducted by the Ponemon Institute

Data breaches can cause devastating financial losses and affect an organization's reputation for years. The biggest contributor to these costs was lost business. This is something which can linger for years after an attack. In addition, there are regulatory fines and remediation costs that may impact an organization.

EXAMPLE

In Europe, the recent introduction of the General Data Protection Regulation (GDPR) has raised the stakes significantly higher for organizations. The upper limit for fines for negligent organizations is considerably higher than previous laws. In July 2019, the United Kingdom's Information Commissioner's Office tried to fine British Airways £183.39M (approximately USD $240M) for a data breach in 2018. This is the largest proposed fine to date and sets a benchmark for future incidents.

These rising costs from direct impacts and fines act as a key driver for the cybersecurity industry. Over the next few years as other parts of the world adopt similarly tough data standards to Europe, it is likely the number of high profile cases will increase significantly.

Facing the challenge of rising attacks

Hiscox is a global specialist insurer. The **Hiscox Cyber Readiness Report 2021 (https://www.hiscox.com/sites/default/files/content/documents/Hiscox-Cyber-Readiness-Report-2021.pdf)** gauges how prepared businesses are to combat cyber attacks. The annual report surveyed over 6,000 professionals across eight countries who are responsible for their firm's cybersecurity. It found that the cost and number of attacks is on the rise. Here are some **important findings**:

- The proportion of firms reporting attacks rose from 38% in 2020 to 43% in 2021, with many suffering multiple attacks.

- The hackers' favorite targets were the technology, media and telecoms (TMT), financial services, and energy sectors.
- Businesses have radically reoriented their IT budges. The average firm now devotes more than a fifth (21%) of its IT budget to cybersecurity.
- 16% of the firms reporting cyber attacks had to deal with a ransomware demand and just over half of those targeted (58%) paid a ransom, either to recover data or to prevent publication of sensitive information.

You can see cyber attacks are an unavoidable cost of doing business today. Organizations have some way to go before they are cyber ready and they need to develop security strategies.

A good metaphor for a cyber attack is that of a pollutant in the environment. The accumulation of attacks is something everyone must deal with, they cannot be ignored forever, and the problem gets worse with inaction.

Security strategy

10 Minutes

To combat cyber attacks and protect themselves, organizations must outline and implement a security strategy. It is two sides of the same coin: How can the organization mitigate threats as well as increase preparedness for a breach? In this lesson, we'll explore security maturity, ten steps to consider implementing for an organization's security strategy, and additional considerations.

The journey of security maturity

Like individuals, organizations change over time. This is reflected within cybersecurity as a **level of maturity** or experience. It is important for an organization to consider where it is *today* and where it wants to strategically be in the *future* in terms of its journey of security maturity.

Certain organizations may not have focused on cybersecurity and may be immature from a system perspective. Then, there are mature organizations that are typically more "battle hardened" because they have had cybersecurity as a priority for a longer period.

The following table provides examples to help understand how mature an organization's security might be across a few metrics.

Area	Sign of less maturity	Sign of more maturity
Processes	Processes may be ad hoc or not formally documented.	Processes are documented, reviewed, measured, and tested.
Leadership	No or few cybersecurity roles are formally set up. Employees may have cybersecurity as a secondary consideration alongside their core role. Little formal leadership exists.	Clear job descriptions and top-down leadership supports the cybersecurity strategy.
Tools	Little investment in tooling exists. Some cybersecurity tools may be used if they are free or bundled within other software packages.	Cybersecurity tools are procured alongside other software and part of a structured budget.
Culture	Few people think about cybersecurity.	Cybersecurity is a key part of the organization's culture.

> **Note**: Rather than an obvious yes or no, it is important to highlight that cybersecurity maturity is a scale. An organization may show development in one area while not being mature in another area.

CHECK THIS OUT!

If you would like to learn more, here is additional information about five security maturity levels offered and described by NIST's Program Review for Information Security Assistance, or PRISMA.

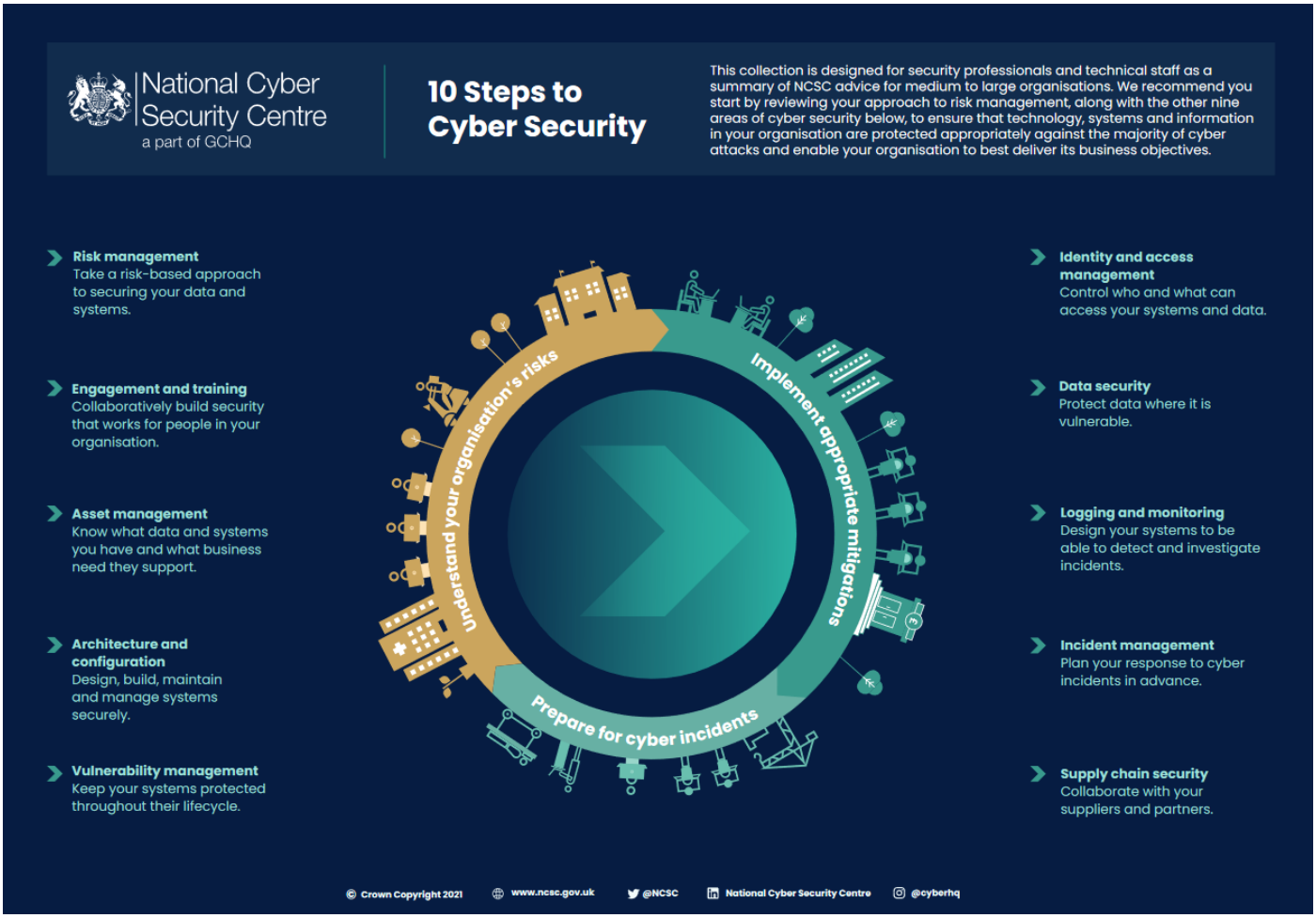
Security Maturity Levels - Program Review for Information Security Assistance (PRISMA) (https://csrc.nist.gov/Projects/Program-Review-for-Information-Security-Assistance/Security-Maturity-Levels)

Starting point for organizations

It can be difficult for organizations to decide where to start with cybersecurity and where to best focus their available resources, such as employees, capital, and time. One approach is to consider following the **10 Steps to Cyber Security (https://www.ncsc.gov.uk/collection/10-steps)** offered by the **The National Cyber Security Centre (https://www.ncsc.gov.uk/)** in the UK. This guidance aims to help organizations manage their cybersecurity risks by breaking down the task of protecting the organization into **10 steps**. Adopting these security measures reduces the likelihood of cyber attacks occurring, and minimizes the impact to an organization when incidents do occur.

It begins with establishing an effective **risk management approach**. This first step and the nine other steps are displayed in the following diagram. You'll learn more about a couple of the steps in more detail in this module, such as **monitoring** and **incident management**.

Enlarge or download this diagram and take a couple of minutes to review the 10 steps so you have an overview.



Download the diagram (https://www.ncsc.gov.uk/files/2021-10-steps-to-cyber-security-infographic.pdf)

Review the online guide of the 10 Steps to Cyber Security (https://www.ncsc.gov.uk/collection/10-steps)

Marketplace for the security industry

Another consideration for organizations starting out with a cybersecurity strategy is that they rarely need to start from scratch or work in isolation to achieve their objectives. Much has been created and developed already! There is a **vast marketplace** in the industry for security products and services. Most large organizations have products from various **cybersecurity vendors**. For example, they may have a data loss prevention system on a database to prevent theft of information produced by one vendor and a firewall produced by another. These many and varied companies each contribute to a vibrant ecosystem supported by a range of standard authorities, charities, and government entities.

Protect against attacks

15 Minutes

An organization's first area of interest within cybersecurity is to **prevent** a successful attack from occurring. In this lesson, we will go over how this can be achieved in practice and some common approaches that organizations take.

What is the goal?

Perfect security in the real world, defined where an attack is *impossible* to complete, is sadly impractical to achieve. While small or simple computer programs can mathematically be assured to perfection, any realistic interconnected system is far too complex. Instead, the emphasis is placed upon making cyber attacks frustratingly difficult. If a defender knows it costs USD $100,000 worth of resources to compromise a system which is only worth USD $80,000 to an attacker, then the attack is unlikely to be attempted and the defense may "work" despite its imperfections.

The goal in cybersecurity is to reduce operational risk to an acceptable level by introducing the correct mixture of people, processes, and technologies.

With the goal in mind, let's examine some overall strategies for how organizations can prevent cyber attacks.

Examine the perimeter

One of the first concepts to consider is that of an **attack surface**. Within cybersecurity, this term means the sum total of an organization's infrastructure and software environment that is exposed where an attacker could choose to attack. Protecting the attack surface was a lot less complicated when organizations had a defined "perimeter" that neatly separated its assets from the outside world. Now, keeping the attack surface *as small as possible* is a basic security measure. This can be done by limiting which services are externally accessible, what devices can be connected, and so on.

> EXAMPLE
>
> Let's say that an organization has a payment record system. It wants employees to be able to access it from a small number of office locations. It is a good security strategy to restrict access to a set number of access points that are required. Any external traffic, such as that from the wider internet, can then be ignored at the perimeter. This simple rule dramatically shrinks the scope of attackers. Rather than having billions of internet protocol (IP) addresses from which to launch an attack, an attacker may be forced to compromise one trusted device and then use that to carry out further attacks. This increases the challenge for the attacker.

Over the last few years, organizations have become more complex with remote access methods, guest wifi, bring your own device (BYOD) policies, and so on. Having a secure perimeter is difficult to achieve. At a minimum, organizations must be aware and monitor their perimeter as part of a larger, comprehensive cybersecurity strategy.

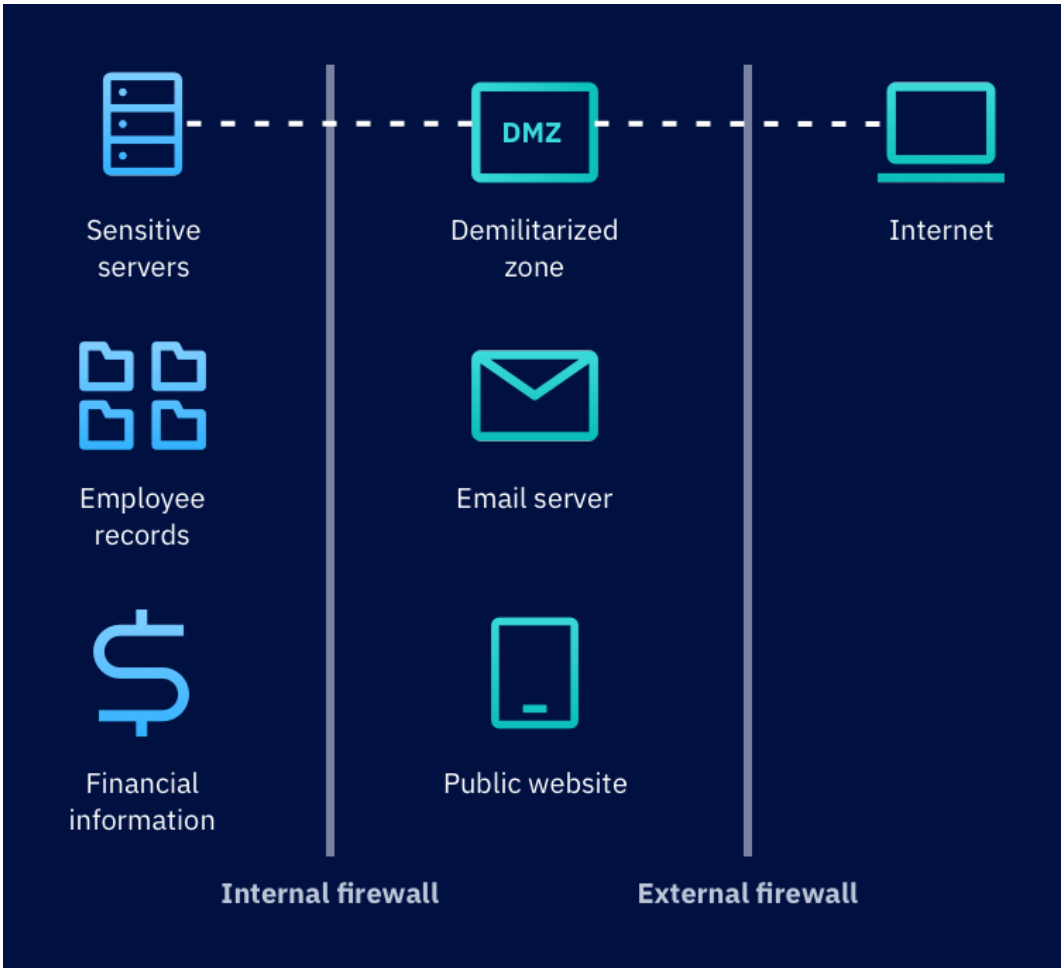
Network segregation

An important approach when designing a more secure system is using a **demilitarized zone** (DMZ). This term is copied from the military. Within networking, it is used to refer to a middle ground area on the network which is partly controlled and managed. Servers in the DMZ may be used by both internal and external applications.

The architecture is often set up so that an external party can access data in the DMZ, but not the sensitive network area. For example, an external customer may be able to place orders for a digital payment system or access email, but not the sensitive company information.

Should one area of an organization's network become impacted during an attack, then the attack does not immediately spread to other more sensitive systems. An attacker who compromises a server in the DMZ would need a second successful attack to move further into the organization.

This diagram shows that a legitimate external user could access the *teal green* servers and applications, but not the more sensitive *blue* servers and applications.



Least privilege

It is important for organizations to decide the levels of permission for applications and individuals within an organization. When doing this, a key element is to introduce the concept of **least privilege**. This means that the fewest permissions are granted to enable a role to be completed.

EXAMPLE

An organization sets up its human resources (HR) database so that managers have read-only access to data for the job roles that they manage. If a particular manager's credentials are stolen by an attacker, then the attacker can only compromise the confidentiality of those specific records. The attacker cannot modify them since they are read-only. They also cannot access applications for other areas of the business.

By introducing this control, the organization has reduced the consequences of a successful attack when compared to a less restricted system. In terms of risk, we are reducing the consequence in this example. You may also hear the military term of a "blast radius" being applied in this context, in which the radius indicates the area of effect from an attack. Reducing permissions is a good way to limit the "blast radius".

Patch and vulnerability management

Patch management is the process of updating software and **vulnerability management** is the process of identifying flaws within software. Over time, older software may have vulnerabilities discovered. Organizations running on outdated software are vulnerable to older exploits. Also, new versions of software can introduce new vulnerabilities. In general, updating software and applications to be the latest version significantly reduces the risk of them being successfully attacked.

When software reaches the end of its life and is no longer supported, managing it becomes a significant issue for security employees. Should a vulnerability be discovered, the software vendor may not issue a remediating patch.

To assess what software is vulnerable to a specific attack, an organization may use a **vulnerability scanner.** This is a piece of software that assesses if there are any vulnerabilities within a server or application. Vulnerability scanners can be network-based to examine vulnerabilities by active testing or they can instead scan static source code for possible errors. Both scanners produce valuable information for identifying flaws before an attacker does.

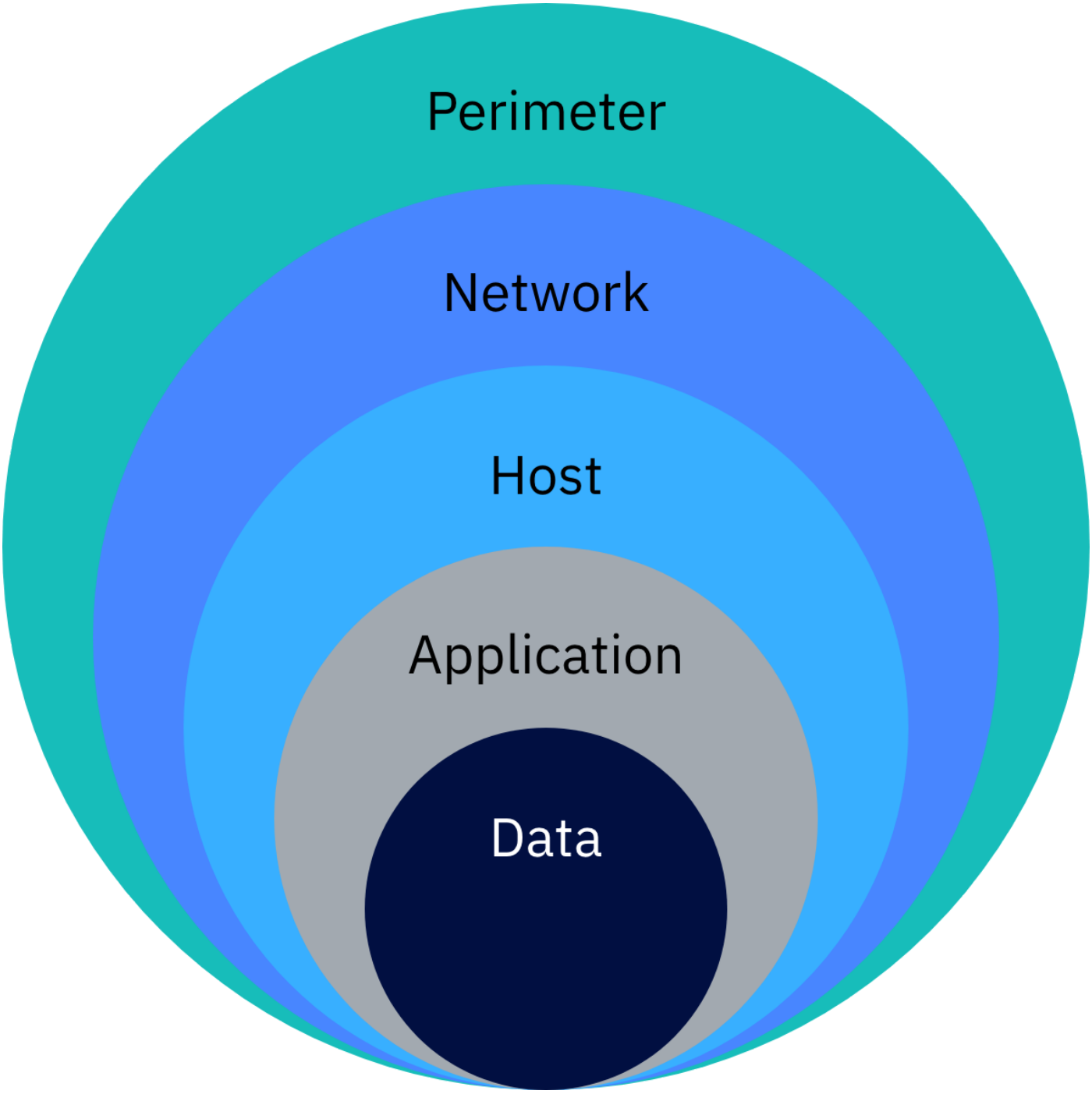
Linked to the idea of vulnerability management is that of **compensating controls**. If a vulnerability is identified for which a patch is not available, then there may be a temporary solution. This could include an application reverting to a previous version or disabling a feature.

Defense in depth

A final key consideration for defense is for organizations to use a layered approach. The term **defense in depth** was originally taken from the military to refer to the idea of not using a single form of defense and instead *layering* them. Within IT, this means an organization may apply network defenses such as firewalls, device defenses such as malware scanners, and place controls around key data by using encryption.

For a successful attack to occur, all layers within the defense would have to be compromised or circumvented, which is quite challenging.

This diagram shows the layering concept for defense in depth.



This is the end of the lesson. Be sure to select the "**I've checked it out**" box to take a mini quiz to check your understanding of this lesson. You will be presented with three questions. This is required for lesson completion.

Detect attacks

10 Minutes

Should an organization's defenses fail to successfully prevent a cyber attack, an organization's next priority is to **detect** the cyber attack. This is ideally done while the attack is in progress or in the best situation, when the breach has yet to occur at all. In this lesson, we'll examine the fundamentals behind attack detection.

Logging

The most important thing for an organization to establish for detecting attacks is a form of **logging**. Logging is the process where actions are accurately recorded in a secure location. Log records should be tamper-proof and act as a permanent record of what has occurred within a network. This logging process can be done on individual machines or applications

While a single log entry may not be highly valuable in isolation, an organization can use a larger collection to track the activities of both legitimate users and attackers.

EXAMPLE

This is an example of a log format used by the Apache web servers:

9.12.156.2 - bob [11/Jan/2020:14:16:34 -0700] "GET /index.html HTTP/1.0" 200 4066

You can see that this log entry describes a user named "bob" who is accessing a specific webpage with the status and time noted.

Network monitoring

In addition to recording events happening on servers, organizations can also monitor communications across their network. This approach is known as **traffic analysis**. Traffic analysis can be used to identify what is being done on a network even in a passive fashion while encryption is being used.

Certain types of malicious software that pivot from device to device can often give themselves away to a good network monitoring solution by being too obvious.

EXAMPLE

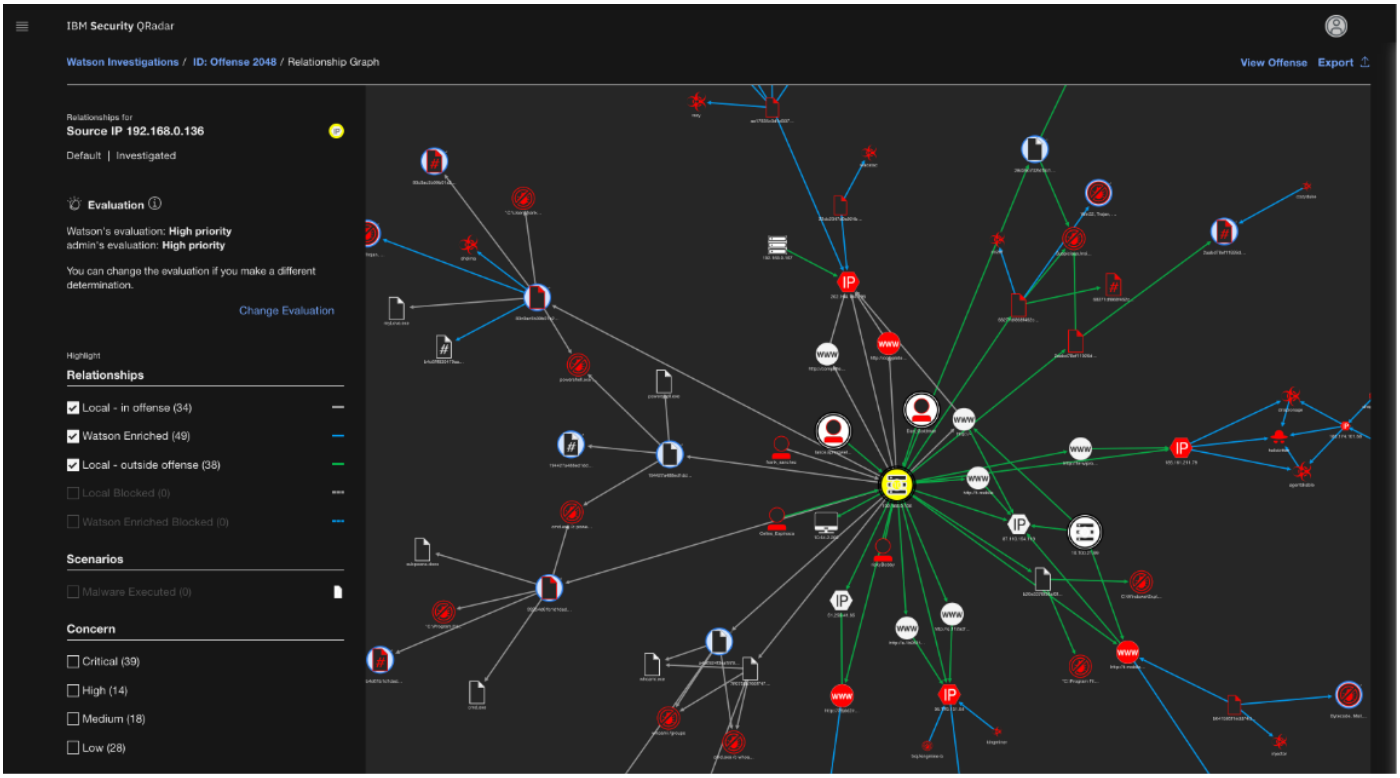
If a device is being used to stream video, then it will have a high bandwidth consumption over an extended period.

By comparison, if a device is downloading a large file, a high demand peak would be seen and then little or nothing after that point.

Security information and event management (SIEM) tools

With all of the information being collected, correlation becomes both highly challenging and rewarding for organizations. A **security information and event management (SIEM)** product collects all of the information throughout the organization's technology infrastructures and aggregates it so the cybersecurity team can identify events and patterns of potential attacks, as well as analyze them.

This is a screen shot of a SIEM service called **IBM QRadar on Cloud (https://www.ibm.com/products/hosted-security-intelligence)**. It is a network security intelligence and analytics software to monitor threats and insider attacks.



EXAMPLE

A cybersecurity team using a SIEM product could decide they want to detect a brute force login attempt for a specific account. They may set a threshold of five failed logins per minute. Should an attacker attempt to compromise an account of the system by working through millions of username or password combinations, the attacker will exceed the threshold and trigger an alert in SIEM, which notifies the cybersecurity team.

Security operations center (SOC)

Often, the group responsible for looking after the security of an organization is a part of the **security operations center (SOC)**. One of the key objectives of the SOC is to detect attacks in progress using SIEMs and other monitoring tools.

Security analysts make up the team of people responsible for assessing an organization's security in the SOC. Should an attack or potential attack be observed, the security analysts will decide how to respond to the situation following organizational procedures.

This photograph shows the Microsoft Cyber Defense Operations Center. It operates 24×7 to defend against cyber threats.

Source: **Microsoft's Cyber Defense Operations Center shares best practices (https://www.microsoft.com/security/blog/2017/01/17/microsofts-cyber-defense-operations-center-shares-best-practices/)**, Microsoft Secure Blog Staff, January 2017

False alarms

One of the fine balancing acts within a SOC is adjusting the sensitivity of certain thresholds. There are several occasions where an alert may trigger when the action is legitimate. This is called a **false positive**, in which an event is recorded as being malicious when it was not.

Confirming if an alert is a false positive is the responsibility of a security analyst. Should an alert trigger too many false positives, it may be worth adjusting the thresholds to be higher.

> EXAMPLE
> A false positive could be caused after an employee returns to work from her holiday and she forgets her password. If the employee tries and guesses her password incorrectly, then her repeated attempts may exceed the threshold and trigger an alert.

Activity

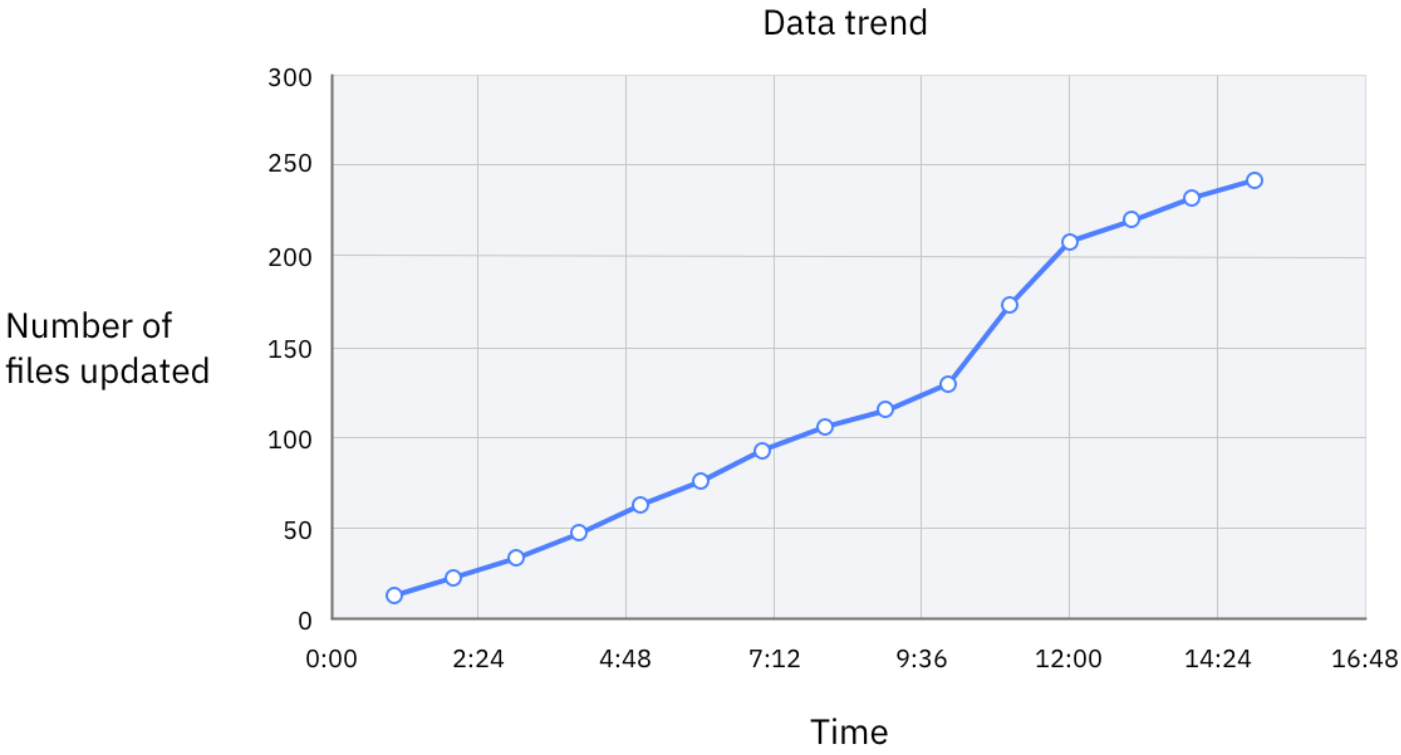
In this activity, you can put on your detective hat to carefully review the following data set! The table shows a record of an organization's **files being altered over a set period of time**, since 12 midnight. From experience, you know that this activity is normally quite predictable with high levels of automation. Can you identify an **interval of time in which there was an unusually high amount of activity**? An unusual amount of changes could indicate unknown or unauthorized activity.

Time	Number of files updated
01:00 AM	12
02:00 AM	23
03:00 AM	33
04:00 AM	47

Time	Number of files updated
05:00 AM	62
06:00 AM	75
07:00 AM	92
08:00 AM	104
09:00 AM	114
10:00 AM	128
11:00 AM	173
12:00 PM	207
13:00 PM	220
14:00 PM	232
15:00 PM	243

When you are ready, click here to reveal the correct answer.

For this data set, there is an unusually high amount of activity between **10:00 AM and 12:00 PM**. You may be able to more easily observe the trend in this visual depiction:



Respond to attacks

15 Minutes

Even with the best defenses, it is inevitable that all organizations will need to **respond** to a cyber attack at some point. Designing systems to be resilient through defined processes and preparation is a vital part of security planning. In this lesson, we'll introduce the basic concepts of incident response.

Introducing incident response

The **SANS Institute (https://www.sans.org/)** provides many educational courses, events, and resources available online. One of the documents they produced is the **Incident Handler's Handbook (https://www.sans.org/reading-room/whitepapers/incident/paper/33901)** by Patrick Kral, which provides a good framework for incident management. Let's briefly review the **six phases** that cybersecurity professionals can use together to respond to an incident.

1. Preparation
• In this phase, an organization should start planning what it will do in the event of an incident. • Typical steps may involve preparing resources and testing procedures.
2. Identification

• The first step to respond to an incident is to detect it. • Once an incident has been confirmed, the process continues to the next phase.
3. Containment
• As soon as an incident is observed, preventing the situation from worsening is the priority. • Steps may include segregating networks or shutting down access routes or certain systems.
4. Eradication
• Like an illness in the human body, certain malware types or attackers must be completely removed in order to be safe. • During the eradication step, devices might be wiped or restored to safe states. • There are countless examples where incomplete eradication results in malware re-emerging, so being thorough is critical.
5. Recovery
• Once the incident is resolved, moving back to standard operation is required. • This may involve removing temporary fixes or restoring certain services.
6. Reflection
• After the incident, it is important to have an opportunity to reflect on not only what caused the incident, but how effective the response was. • Commonly this phase may be referred to as the "lessons learned" phase. However, "lessons identified" may be a better title if changes are not made!

You can see this incident framework provides a good baseline to build upon. Certain forms of attack or incidents might require the expansion of certain stages. For example, a data breach event from a lost storage device might not have many eradication steps, but the recovery process might be longer with a higher number of stakeholders engaged.

Preparing for incidents

As part of standard business activities, many organizations will go through several simulated activities to test their level of preparation. This table explains three types of such tests.

Paper-based tests	**Table-top exercises**	**Live tests**
In this test, security teams are surveyed and asked questions about their level of preparation. This may involve identifying key personnel, ensuring backups are taken, and producing process documents upon request.	This is a more involved test format. In this test, various key personnel are bought together, and the incident response process is simulated end-to-end. This form of testing allows teams to interact with one another and see how the wider scenario would develop.	The most realistic form of testing is to perform an exercise within the live systems. Organizations may shut down key systems to test various failures and how their teams respond.

Business continuity and disaster recovery

Let's examine two key terms that you need to know about with regards to incident response.

1. **Business continuity** is based on an organization’s ability to continue operating despite an incident. This may involve having backup sites to take over the delivery of services or a backup technology to take over should one fail.
2. **Disaster recovery** is based on an organization’s ability to recover from a disaster. A cybersecurity disaster could involve all computers in an organization being wiped or entire databases being deleted. In this recovery planning process, organizations need to be prepared to start with virtually nothing.

Both continuity planning and recovery processes have high levels of overlap with other security functions. While historic concerns were mostly around natural disasters such as floods, earthquakes, or fire, it has become increasing evident that cyber attacks can be equally or more disruptive than their natural counterparts. While a multinational organization is extremely unlikely to have all its sites hit by a power cut simultaneously, a cyber attack that shuts down key global services, such as organizational file shares or domain management systems, is far more plausible.

Benefit of incident response teams

The benefit of incident response teams can be highlighted by the following analysis from the **2019 Cost of a Data Breach Report (https://www.ibm.com/account/reg/us-en/subscribe?formid=urx-42215)** conducted by the Ponemon Institute and sponsored by IBM Security.

Companies studied that had an incident response team and extensive testing of their response plans saved over $1.2 million.

An organization's ability to respond effectively after a data breach was strengthened by the presence of an incident response (IR) team that follows an incident response plan. In this year's research, we found that organizations with an incident response team amplified their cost-savings by also conducting extensive testing of their IR plan, such that the combined effect of the IR team and IR plan testing produced a greater cost savings than any single security process. Those organizations who conducted extensive testing of an IR plan had an average total cost of a breach that was $1.23 million less than those that neither had an incident response team or tested their incident response plan ($3.51 million vs. $4.74 million). Testing the incident response plan, through exercises such as tabletop exercises or simulations of the plan in an environment such as a cyber range, helped teams respond faster and potentially contain the breach sooner.

Activity

It's time for you to design a personal incident response plan! Let's get creative and operational. Imagine your laptop, computer, or tablet has a failure and does not power on anymore. What would your response process be?

Please type your answer to each question in the boxes. Your answers are just for you and are only saved in this course for you. Be sure to click **Save Text**.

1. Your first step could be to **identify** the situation. How would you diagnose what caused the problem? Would you attempt to do this? How quickly would this need to happen?

Save Text Save Text Save Text

2. Your next step could be to determine your steps to **respond**. Would you plan to replace the device? Is there a spare device you could introduce quickly?

Save Text

3. A last step could be to **reflect**. How could you minimize the impact of this situation if it were to occur again in the future?

Save Text

Introducing cryptography

15 Minutes

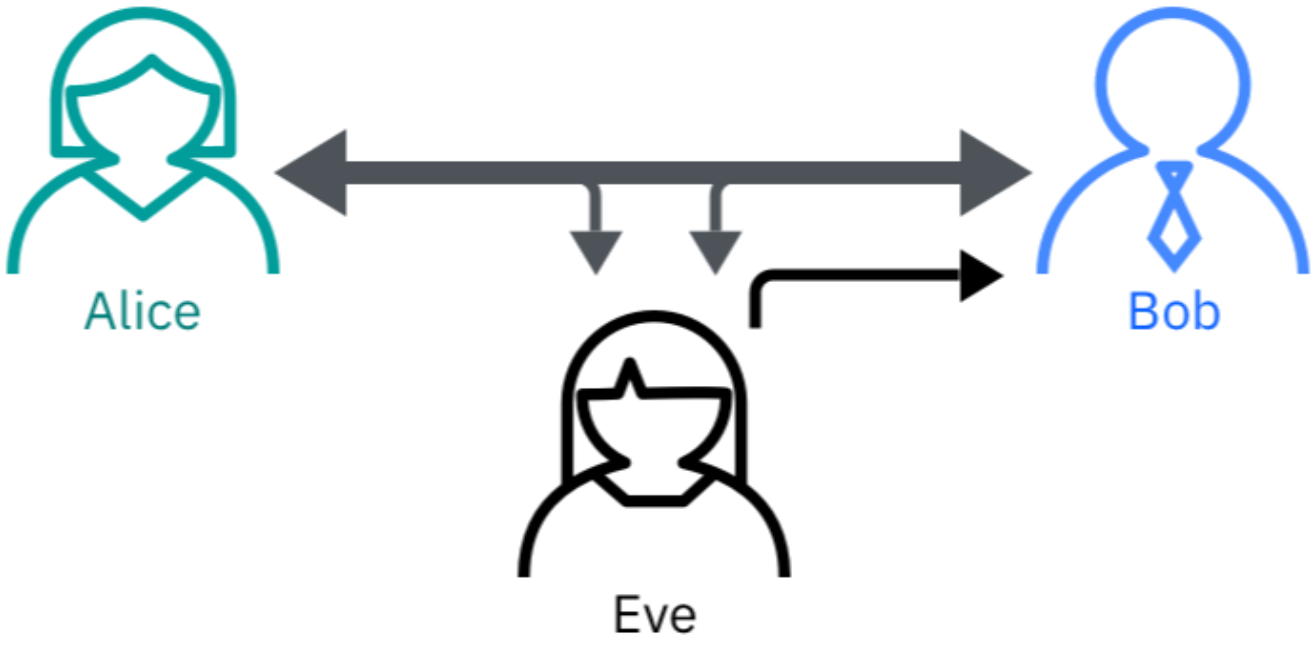
In this lesson, we will introduce the mathematical field of cryptography. Cryptography is fundamental to vital concepts within information security and something all cyber security professionals should have an understanding of to be successful.

Cryptography is defined as the art of writing and solving codes.

At the start of this course, we shared that keeping information **confidential** is one of the key objectives of information security. Keeping and sharing secrets have been challenges that have existed for thousands of years. While methods for achieving this have changed significantly across the years, the objectives have remained broadly the same.

Defining secure communications

Imagine a situation with three participants: **Alice, Bob, and Eve**. These three characters have been used for many years in the field of cryptography to illustrate concepts. Alice and Bob want to communicate securely, and Eve wants to eavesdrop on the exchange, thus her name, "Eve".



There are **three key properties** which must be observed to have reliable secure communications.

Property 1: Confidentiality

Alice can send a message to Bob without Eve being able to understand the contents. This property means that the message is private.

Property 2: Authenticity

Eve cannot send a message to Bob claiming to be Alice. This property relates to ensuring spoofing or impersonation is impossible.

Property 3: Integrity

If Eve modifies a message between Alice and Bob, then the receiver will be able to identify the message has been modified. It is possible to tamper with messages without knowing the contents. For instance, people can talk loudly to disrupt a face to face conversation in a language they do not understand.

These three properties are achieved through a range of mathematical algorithms and other techniques. Historically, this could be locked boxes and wax seals, but for this course, we'll be focusing more on the mathematical options!

Encryption

Encryption is the process by which a message is converted into something that cannot be understood, except by those who have a decryption key to reverse the process. When a message has been converted into an unreadable state it is said to be encrypted. At a high level, there are two forms of encryption in use for the world today: symmetric and asymmetric.

Symmetric encryption

In symmetric encryption, the algorithm for encrypting information uses the **same key** as the decryption process. Symmetric encryption is fast and easy to implement. It relies on both the sender and receiver having access to the same key, kind of like a password or "shared secret", to maintain a private information link.

> **EXAMPLE**
> A simple example is a rotation-based cipher in which characters are increased or decreased by a fixed number of places in the alphabet. The number of places to move forward and backward acts as the key. If the sender is using a key of +1, they rotate characters forwards by 1 and the receiver then uses a -1 rotation to receive the original message. In this cipher, the word "HOLIDAY" is encrypted by +1 shift in the alphabet to be "IPMJEBZ".

H	O	L	I	D	A	Y
I	P	M	J	E	B	Z

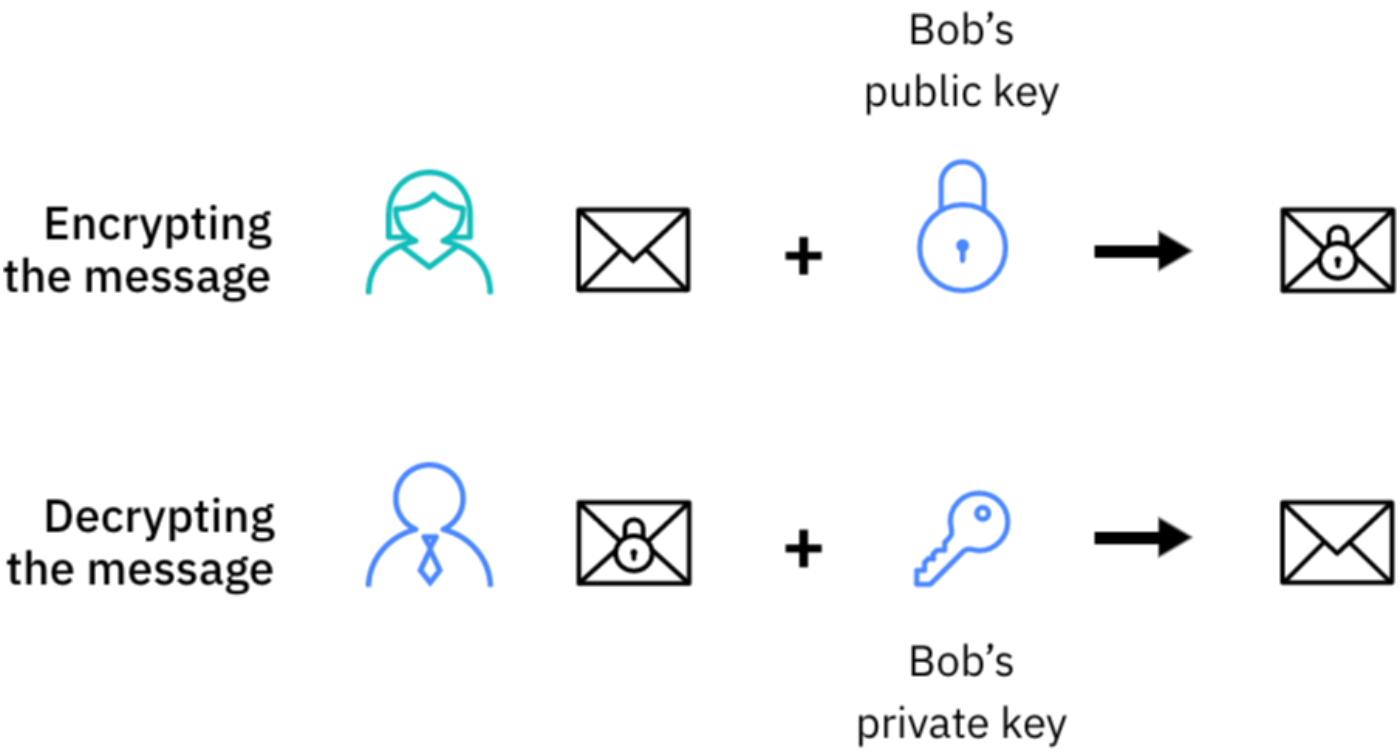
+1

Algorithms in use today that follow symmetric models include versions of the Advanced Encryption Standard (AES). This is likely what your browser is using to see this page securely!

Asymmetric encryption

In asymmetric encryption, the process for encrypting information uses a **different key** to decrypt the information. These keys are known as **public keys** and **private keys**. They are generated simultaneously. Once a public key is generated, you can share it with anyone and everyone. Anyone who has a copy of the public key can encrypt a message, which only the holder of the private key can decrypt.

> EXAMPLE
> In this diagram, Alice is the sender and Bob is the receiver. It represents the transmission process. Alice encrypts a message using Bob's public key. Once the message is encrypted, it can only be decrypted using Bob's private key. The encrypted message is sent to Bob. Bob can then decrypt the message using his private key. It is essential that Bob does not share his private key with anyone, otherwise they would be able to read all of his incoming messages.



The main benefit that asymmetric encryption offers is organizations can communicate securely with an entity that they have not previously exchanged a "key" with. In addition, it can provide assurance that a message is being sent to the right receiver.

> EXAMPLE
> One of the benefits of asymmetric cryptography can be illustrated by online shopping. Customers can buy goods from shops without having to physically go to the location to create a shared, unique, symmetric key.
>
> If symmetric cryptography was the only option, the agreed symmetric key would have to be used to encrypt and decrypt all future transactions between the customer and the shop.
>
> By comparison, using asymmetric cryptography is convenient and saves time since the in-person meeting is not needed. Without this benefit, it would be practically impossible to use online shopping in a secure manner.

Activity

One of the best ways to learn about encryption is to try it yourself! The **CyberChef (https://gchq.github.io/CyberChef/)** tool is a web-based program written by the UK's Government Communication Headquarters (GCHQ) as a tool to help with data processing operations such as encryption. In CyberChef, an encrypted message is the ingredient to "bake" in a recipe by having a series of steps applied to it. Follow these steps.

1. Go to **CyberChef (https://gchq.github.io/CyberChef/)**.
2. Copy and paste this encrypted message in the **Input** field: ftue ue m fqef eqzfqzoq
3. On the left navigation's labelled operations, scroll down to find the **Encryption / Encoding** section and expand it.
4. Select and drag **ROT13** to the empty space in the **Recipe** box. This means that the tool will rotate the alphabet characters forward 13 places in the alphabet. The Auto Bake option is enabled by default, so you will see the **Output** field has changed.
5. Now, click the up and down arrows in the **Amount** filed to see the message change in the **Output** field. You want to decrypt the message. Stop when you find an **Output** message that makes sense as a short sentence in English.

What is the decrypted message? Please type your answer in the box. Your answer is just for you and is only saved in this course for you. Be sure to click **Save Text**.

Your text has been saved. Click "X" to continue.

When you are ready, click here to view the decrypted message.

Visit this **CyberChef web page (https://gchq.github.io/CyberChef/#recipe=ROT13(true,true,true,14)&input=ZnR1ZSB1ZSBtIGZxZWYgZXF6ZnF6b3Eg)** to check your answer.

Introducing threat intelligence

15 Minutes

Historically in military operations, intelligence is often examined as a force multiplier. It allows a commander to use the resources they have for their greatest impact.

> *If you know your enemies and know yourself,*
> *you will not be imperiled in a hundred battles;*
> *if you do not know your enemies but do know yourself,*
> *you will win one and lose one.*
>
> **— The Art of War by Sun Tzu (https://en.wikiquote.org/wiki/Sun_Tzu)**

In the modern world of cybersecurity, understanding your enemies is the domain of threat intelligence.

In this lesson, we'll briefly cover how organizations benefit from staying aware of threat intelligence and sources they commonly use.

What is threat intelligence?

In a pure form, the UK Ministry of Defence defines **intelligence** as, "The directed and co-ordinated acquisition and analysis of information to assess capabilities, intent and opportunities for exploitation by leaders at all levels."

Source: **Joint Doctrine Publication (JDP) 2-00: Understanding and intelligence support to joint operations (https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/311572/20110830_jdp2_00_ed3_with_change1.pdf)**, 3rd edition, August 2011

Then, **cyber threat intelligence** is data collected and analyzed by an organization in order to understand the motives and behavior of cyber attackers. This is a sub-set of the intelligence landscape that we will explore further.

Within cybersecurity, intelligence typically focuses on attacker **tactics, techniques, and procedures (TTPs)** or other **indicators of compromise (IOCs)**. What do these terms mean?

- **Tactics** are the "why" meaning the adversary's tactical goal or reason for performing an action. For example, an adversary may want to increase privileges.
- **Techniques** are the "how" meaning the ways an adversary achieves a tactical goal by performing an action. For example, an adversary may bypass access controls to increase privileges.
- **Procedures** are the specific implementation the adversary uses for techniques. For example, an adversary may use a specific tool or program to increase privileges.
- **Indicators of compromise (IOCs)** are signatures related to attacker activity. For example, certain IP addresses might be associated with threat groups or certain files. The presence of an IOC may indicate that an organization has already been comprised, hence the name.

Benefits of threat intelligence

Organizations can benefit from threat intelligence across the following broad areas.

Providing a warning	• A key benefit of threat intelligence is it allows organizations to prepare for attacks. • Certain geopolitical or technical developments have the potential to change an organization's risk profile quite rapidly. • Having some advance notice enables organizations to better prepare their defenses to stop an attack from occurring at all.
Providing indicators of compromise (IOCs)	• Threat intelligence aids detection activities by providing indicators of compromise. • These could be certain IP addresses used by attackers, file hashes, or domains. • A defender within an organization can search for these signs and add detection rules to alert when they are detected.
Providing context	• Should an organization discover they were attacked from an unknown location or group, the organization can use intelligence sources to start understanding the attacker. • Context can include helpful pieces of information to aid attribution and guidance on what to expect next.
Learning from peers	• There are some things best learned from others. • Organizations may share information about how attackers attacked them, how they defended themselves, and how effective their approaches were. • These shared stories are an excellent method of strengthening the whole industry.

Sources of threat intelligence

Gathering and developing threat intelligence can be a complex undertaking. Organizations may engage in primary research in which they investigate themselves or collect secondary information from another source. Here are some common threat intelligence sources that organizations utilize.

Threat exchange platforms	• There are a number of online platforms that allow cybersecurity professionals to access databases of gathered information and analysis. • These can range from free platforms to others which are provided on a subscription model or to closed industry groups. • One example is the **IBM X-Force Exchange platform (https://exchange.xforce.ibmcloud.com/)**.

Conferences	• Conferences are a good method for cybersecurity professionals to share the latest developments in the industry. • Certain researchers hold off making discoveries public in order to get a larger burst of publicity at an event. • There are also opportunities to gather information from informal conversations at conferences and networking. • Examples of conferences include **Black Hat (https://www.blackhat.com/)**, **RSA Conference (https://www.rsaconference.com/)**, and **CYBERUK (https://www.ncsc.gov.uk/section/cyberuk/overview)**.
Articles and news	• Certain media outlets devote a significant amount of effort to covering developments within the IT world. One example is **Security Intelligence (https://securityintelligence.com/)**. • As certain security issues have become more high profile, the amount of coverage has increased significantly. • There is also a good collection of smaller sites in addition to traditional media outlets who cater to a more specialist audience. Examples of blogs include **Krebs on Security (https://krebsonsecurity.com/)** and **Graham Cluley (https://www.grahamcluley.com/)**.
Product vendors	• Organizations such as Microsoft, Google, and Apple, who produce large amount of software, frequently produce periodic security advisories relating to their products. • These notices can include very important information and are essential reading for system administrators.

Job roles

Within the world of cyber threat intelligence, job roles can typically be divided into two areas: production and interpretation.

- On the **production** side, there is a range of job roles involved in the collection and enrichment of information. Some of these roles are technically-focused, such as those involved with developing scanners or web crawlers, or conducting software analysis. Other roles might involve more subterfuge and infiltrating criminal gangs and marketplaces. Finally, there are roles involved in translation, linguistic analysis, and psychometrics (the science of measuring mental capacities and processes). All of these roles collect information and produce intelligence from it.
- On the **interpretation** side, unless intelligence development is done "in house" or by commission, it is very rare that intelligence will tell analysts everything they would like. Security analysts may receive several warnings relating to a range of topics. They then need to review the findings and decide the best course of action to recommend. Interpretation must take unique, organizational attributes into account such as proprietary or confidential information to be effective. There isn’t a one-size-fits-all model!

Key takeaway

In conclusion, threat intelligence allows organizations to act in a systematic and planned way rather than using estimations or relying on standards. This means defenses are designed to meet the attacks they will experience rather than designing defenses to meet an industry or regulatory standard. This is particularly important for organizations that operate in a complex or anomalous way for which regulations are often insufficient guidance.

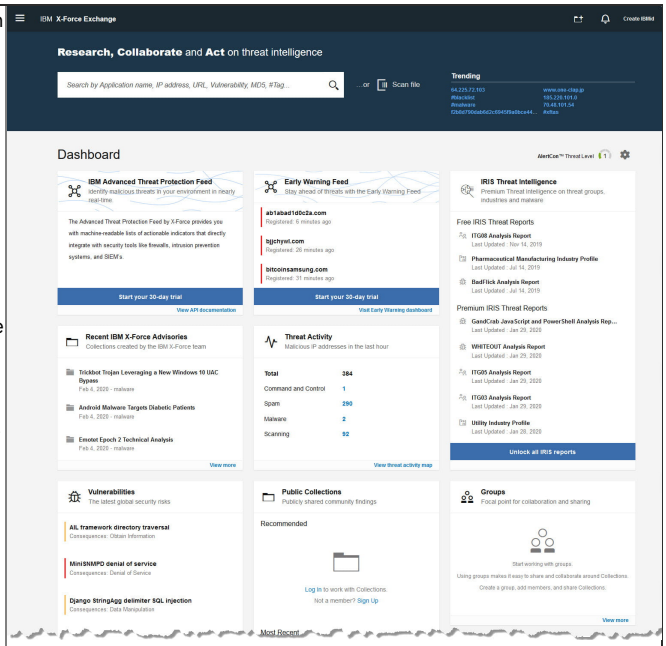
Activity

Let's pretend you are on a security team and have been asked to produce a threat intelligence brief to summarize what has happened in the past 24 hours. Try and look up some information on the **IBM X-Force Exchange platform (https://exchange.xforce.ibmcloud.com/)**.

Please type your answer in the box. Your answer is just for you and is only saved in this course for you. Be sure to click **Save Text**.

What information would you provide today? What is the latest intelligence, advisories, threat activities, and so on?

Check out the threat activity map in the **Threat Activity** section!



Go to the **IBM X-Force Exchange platform (https://exchange.xforce.ibmcloud.com/)**.

Your text has been saved. Click "X" to continue.