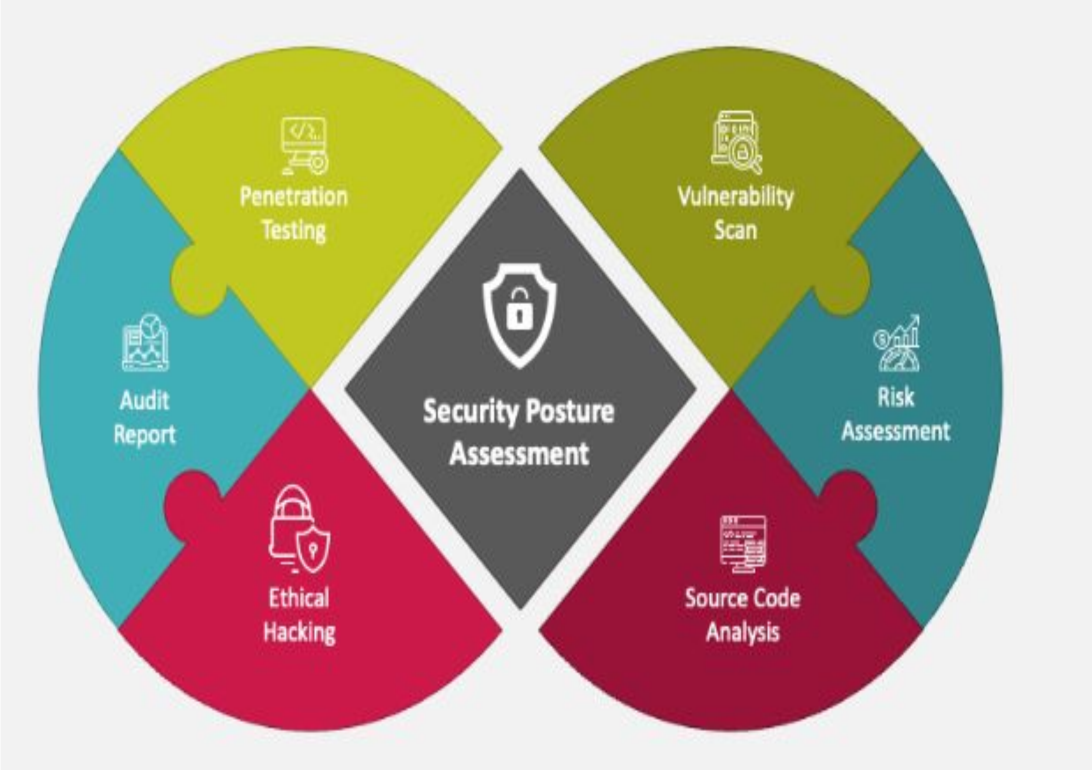
Cyber Security Attacks and Defense Strategies

Yuri Diogenes, Erdal Ozkaya

Unit-01-Security Posture



What is Security Posture?

Unit-01-Security Posture

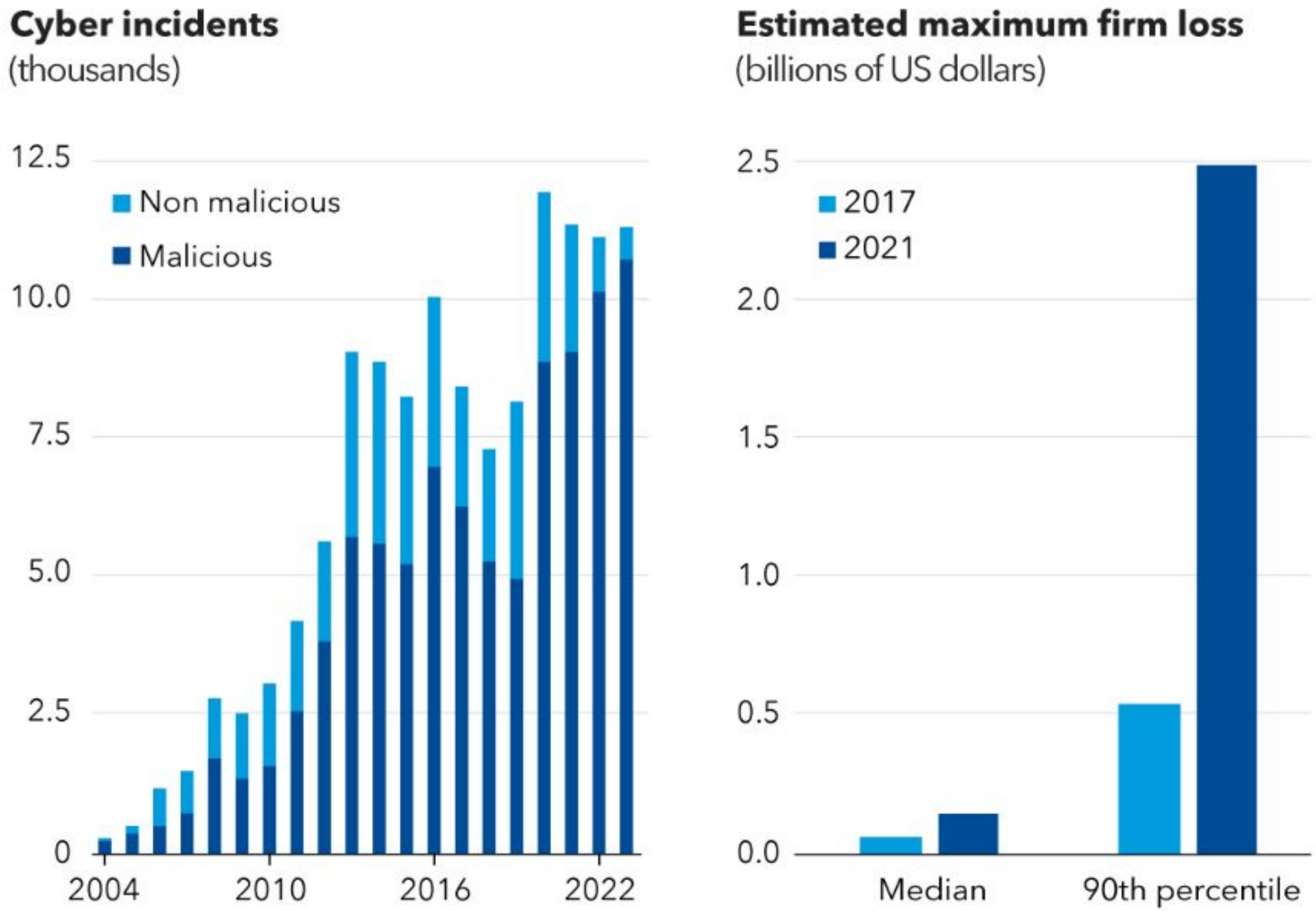
An organization's security posture is its readiness and ability to identify, respond to and recover from security threats and risks.

Why Strong Security Posture is important?

Unit-01-Security Posture

- Protection Against Cyber Attacks
- Adaptability to Future Attacks
- Effective Incident Response and Recovery
- Cost Savings in a Data Breach

Unit-01-Security Posture



Sources: Advisen Cyber Loss Data; Capital IQ; and IMF staff calculations.

Security Posture

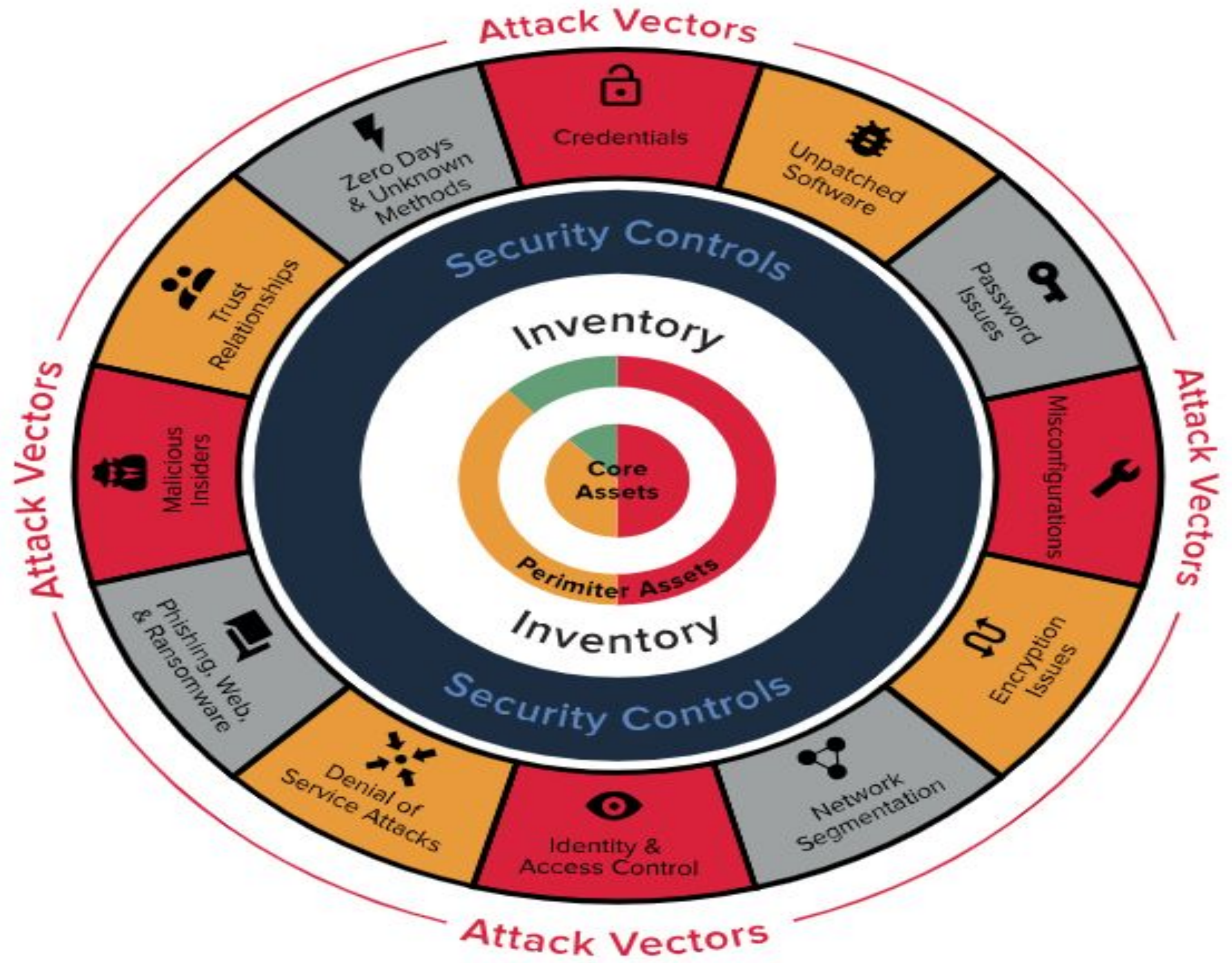
Security posture refers to an organization's overall cybersecurity strength and how well it can predict, prevent and respond to ever-changing cyberthreats.

An organization's security posture includes its networks, information security, network security, data security and internet security, as well as penetration testing, vendor risk management, vulnerability management, data breach prevention, security awareness training for employees to prevent social engineering attacks and other security controls.

A company's security posture, however, isn't static. Rather, it is constantly changing to respond to new vulnerabilities and threats in the cybersecurity landscape. As such, enterprises are transitioning from fragmented tools and outdated security frameworks to end-to-end security postures that can protect against these new security threats and vulnerabilities.

Now a days organizations around the globe are realizing how important it is to continually invest in security. This investment will ensure that the company stays competitive in the market.

Security Posture



Security Posture

An **attack vector** is a pathway or method used by a hacker to illegally access a network or computer in an attempt to exploit system vulnerabilities.

Attack Vector vs Attack Surface?

How Do Hackers Exploit Attack Vectors?

Common type of Attack Vectors?

How a strong security posture protects companies

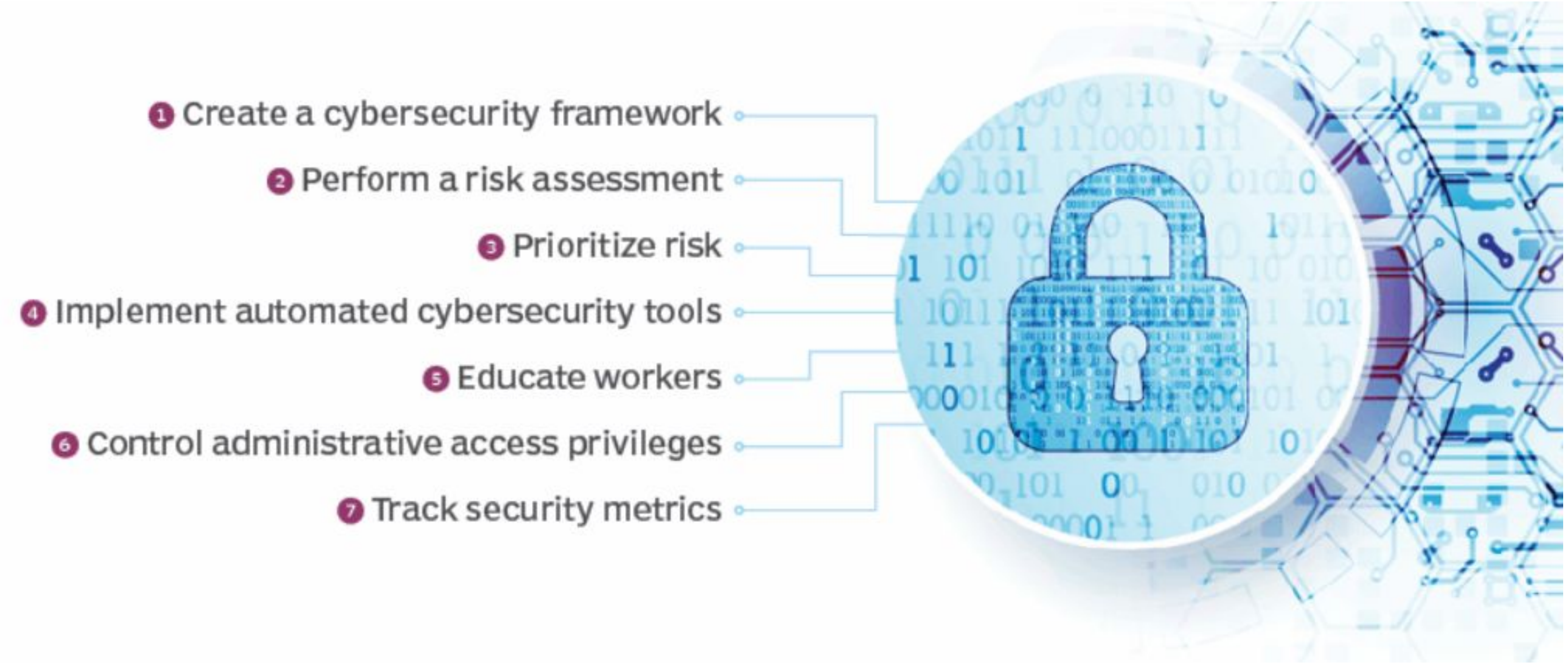
A strong security posture aims to protect organizations against cybersecurity threats by detecting and preventing malware intrusions -- like ransomware -- and data breaches. It also prevents the theft of intellectual property.

For example, a company that requires employees, third-party vendors and customers to use two-factor authentication or multifactor authentication -- or at least cycle through complex passwords -- to log in to its website can keep corporate data safe.

In addition, implementing firewall, antivirus and antimalware tools as part of a strong security posture can make it difficult for cybercriminals to break into its network and steal sensitive data. This strategy helps deter cyber attacks.

Implementing anti-phishing and email security tools as part of a comprehensive security posture can help a company stop spam from making its way to users' inboxes. These tools also scan messages and remove any malicious content before forwarding them to the company's mail server.

How a strong security posture protects companies



1 Create a cybersecurity framework
2 Perform a risk assessment
3 Prioritize risk
4 Implement automated cybersecurity tools
5 Educate workers
6 Control administrative access privileges
7 Track security metrics

Strategies to strengthen security posture

Organizations are constantly faced with a variety of security issues, such as how to reduce vast attack surfaces; how to secure their networks, devices, endpoints and other IT assets and how to keep hackers from breaching their systems. There are many ways companies can enhance their security policies to meet these challenges, including the following:

Create a cybersecurity framework. Companies should align their security requirements with the goals and objectives of the business.

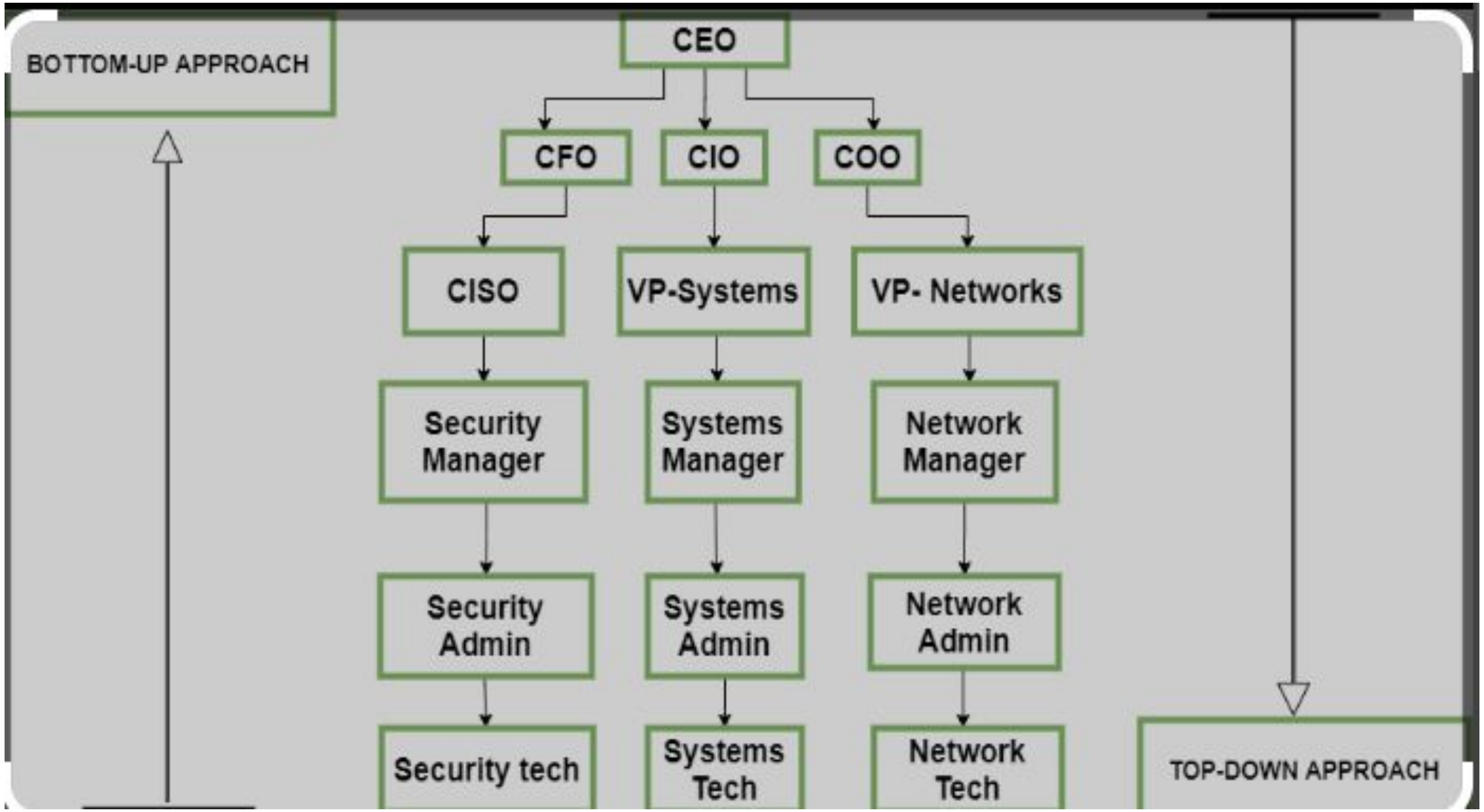
Perform a risk assessment. A cybersecurity risk assessment identifies the level of vulnerability across an organization's assets. The results enable organizations to determine what they need to do to improve their security postures.

Prioritize risk. After identifying the asset vulnerabilities, enterprises should then rank them based on the overall risk they pose to the business and determine what to work on first.

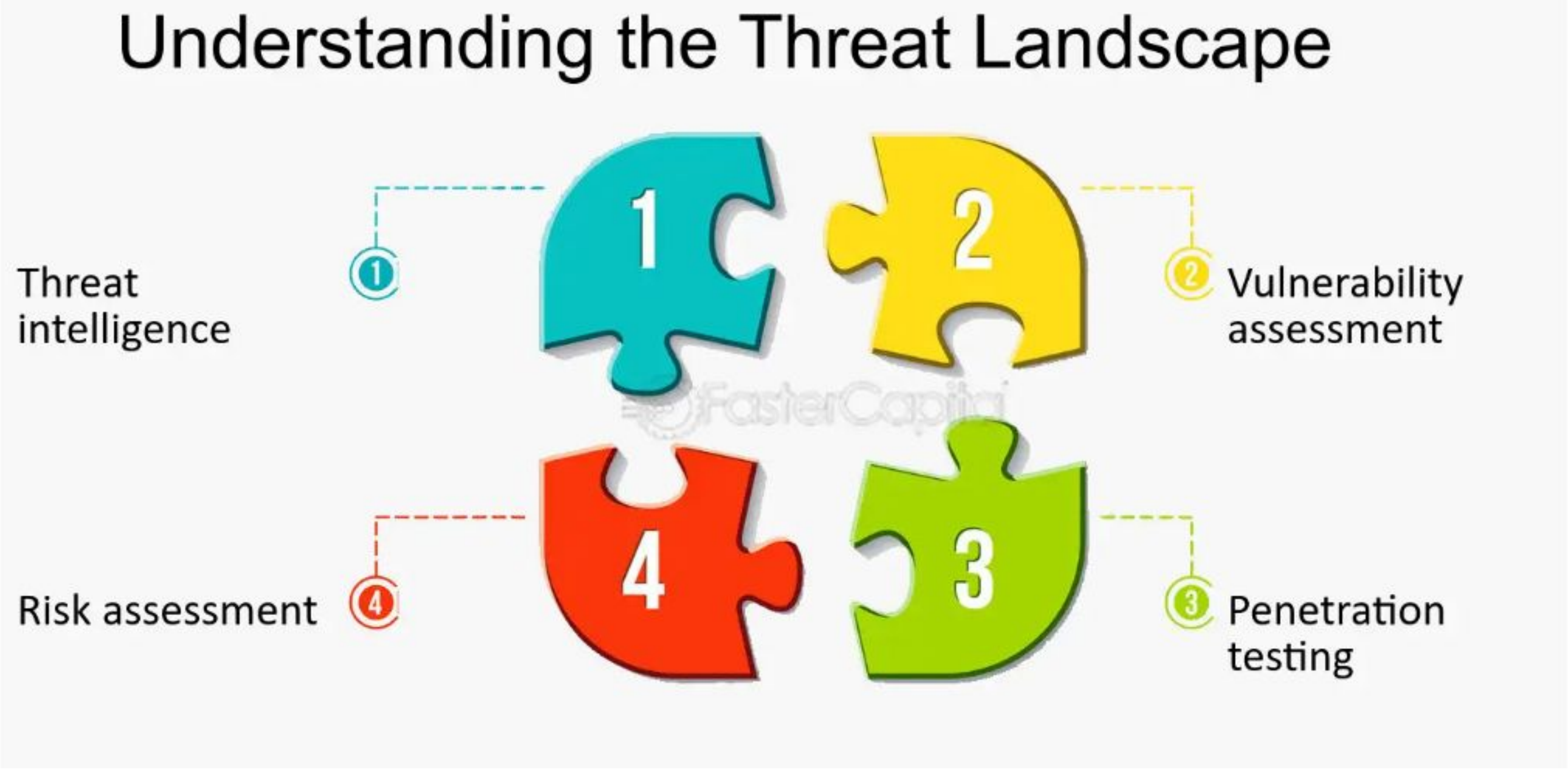
Implement automated cybersecurity tools. Using automated tools can help reduce incident response times and prevent hackers from infiltrating the network.

Control administrative access privileges. Organizations should only grant administrative access privileges to a small group of employees, like security teams. Letting too many people modify hardware and operating system settings can be disastrous to companies' security postures

Approaches to Information Security Implementation



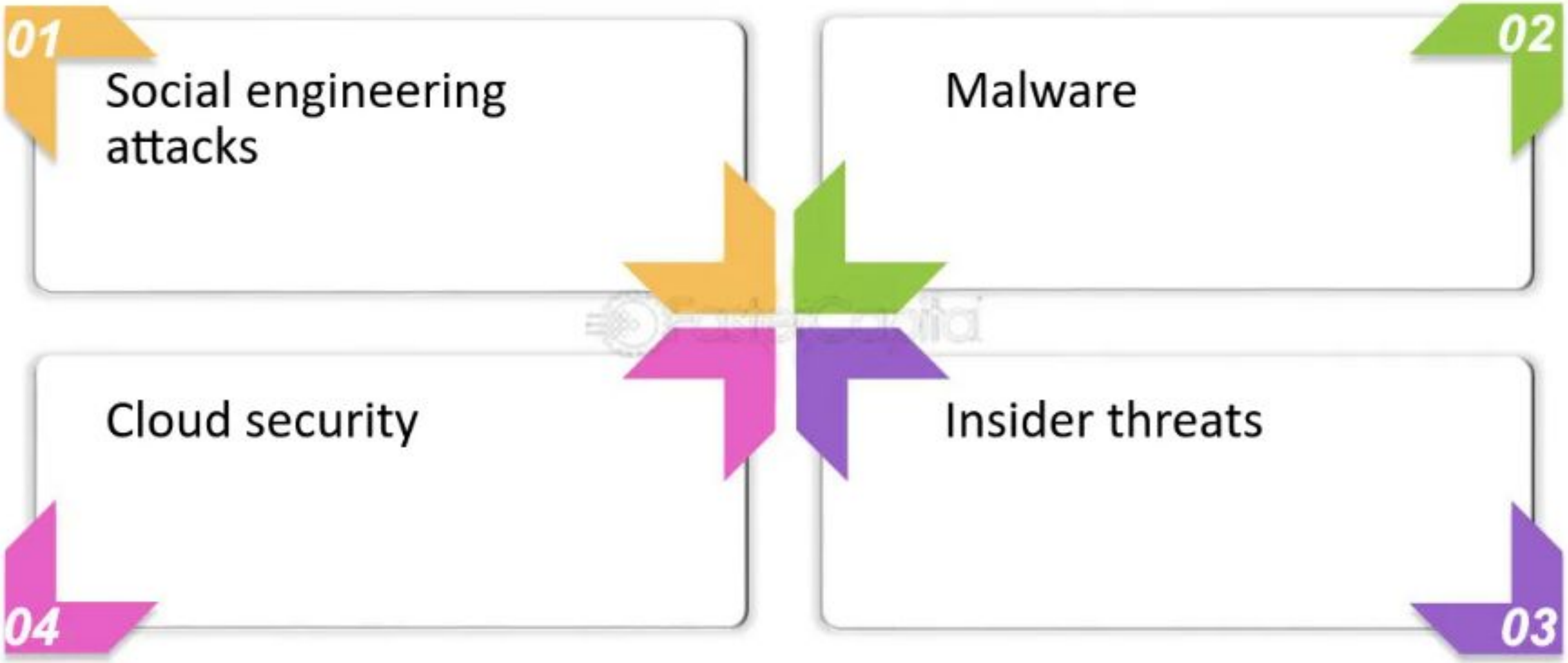
Current Threat Landscape



Understanding the Threat Landscape

1. Threat intelligence
2. Vulnerability assessment
3. Penetration testing
4. Risk assessment

Current Threat Landscape



01 Social engineering attacks

02 Malware

03 Insider threats

04 Cloud security

The Current Threat landscape

With the prevalence of always-on connectivity and advancements in technology that are available today, the threats are evolving rapidly to exploit different aspects of these technologies. Any device is vulnerable to attack, and with **Internet of Things** (**IoT**) this became a reality.

In October 2016, a series of Distributed Denial of Service (DDoS) attacks were launched against DNS servers, which caused some major web services to stop working, such as GitHub, PayPal, Spotify, Twitter, and others.

This was possible due to the amount of insecure IoT devices around the world. While the use of IoT to launch a massive cyber attack is something new, the vulnerabilities in those devices are not. As a matter of fact, they've been there for quite a while.

The **Chief Executive Officer** (**CEO**) may even ask: what do the vulnerabilities in a home device have to do with our company? That's when the **Chief Information Security Officer** (**CISO**) should be ready to give an answer. Because the CISO should have a better understanding of the threat landscape and how home user devices may impact the overall security that this company needs to mitigate. The answer comes in two simple scenarios, remote access and **Bring your Own Device** (**BYOD**).

The Current Threat landscape

With the prevalence of always-on connectivity and advancements in technology that are available today, the threats are evolving rapidly to exploit different aspects of these technologies. Any device is vulnerable to attack, and with **Internet of Things** (**IoT**) this became a reality.

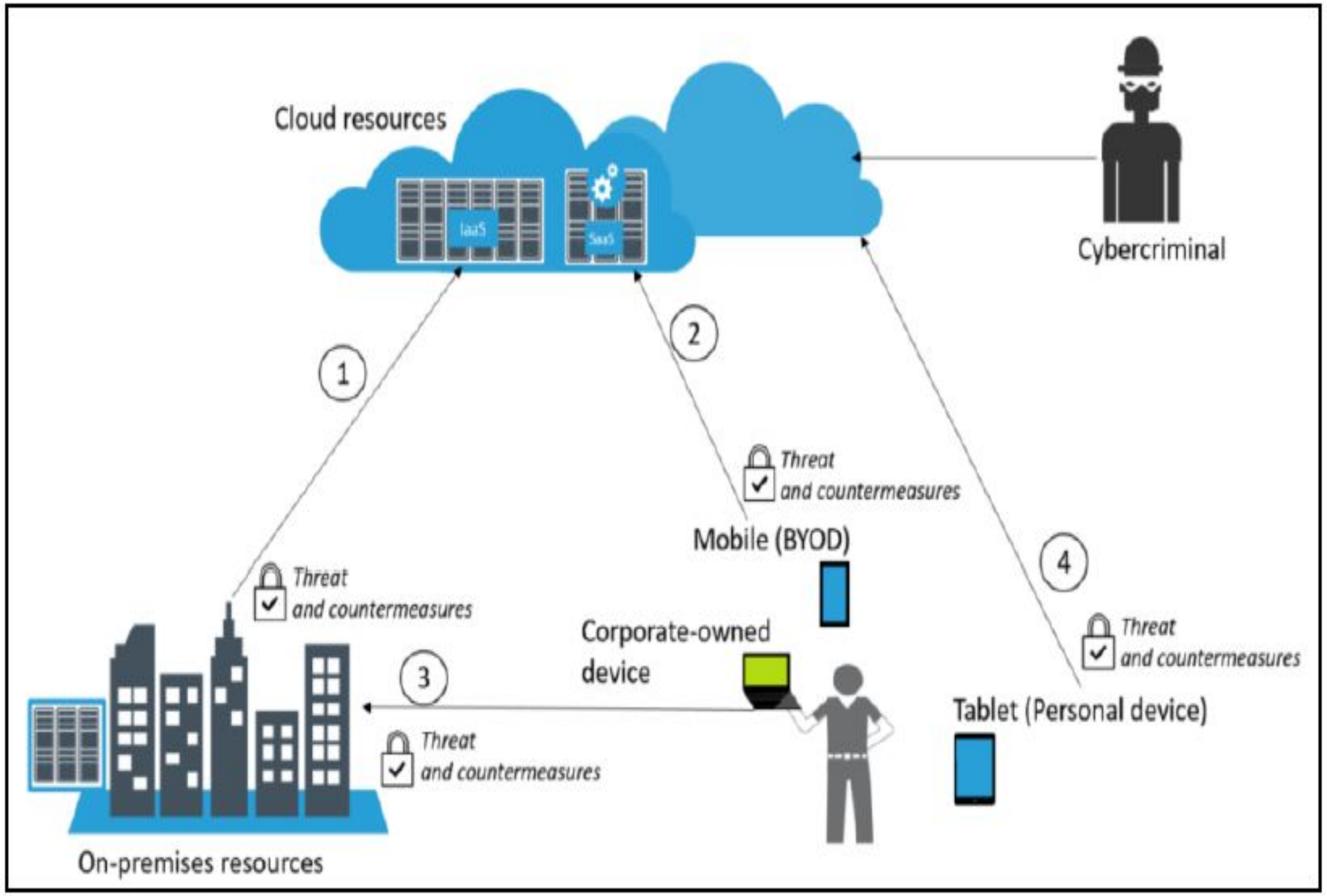
In October 2016, a series of Distributed Denial of Service (DDoS) attacks were launched against DNS servers, which caused some major web services to stop working, such as GitHub, PayPal, Spotify, Twitter, and others.

This was possible due to the amount of insecure IoT devices around the world. While the use of IoT to launch a massive cyber attack is something new, the vulnerabilities in those devices are not. As a matter of fact, they've been there for quite a while.

Connectivity between on-premises and cloud (1)
Connectivity between BYOD devices and cloud (2)
Connectivity between corporate-owned devices and on-premises (3)
Connectivity between personal devices and cloud (4)

The current threat landscape

- Connectivity between on-premises and cloud (1)
- Connectivity between BYOD devices and cloud (2)
- Connectivity between corporate-owned devices and on-premises (3)
- Connectivity between personal devices and cloud (4)



In all scenarios, there is also another important element that appears constantly, which is cloud computing resources. The reality is that nowadays you can't ignore the fact that many companies are adopting cloud computing. The vast majority will start in a hybrid scenario, where **Infrastructure as a Service** (**IaaS)** is their main cloud service. Some other companies might opt to use **Software as a Service** (**SaaS**) for some solutions. For example, **Mobile Device Management** (**MDM**), as shown in scenario **(2)**. You may argue that highly secure organizations, such as the military may have zero cloud connectivity. That's certainly possible, but commercially speaking, cloud adoption is growing and will slowly dominate most of the deployment scenarios

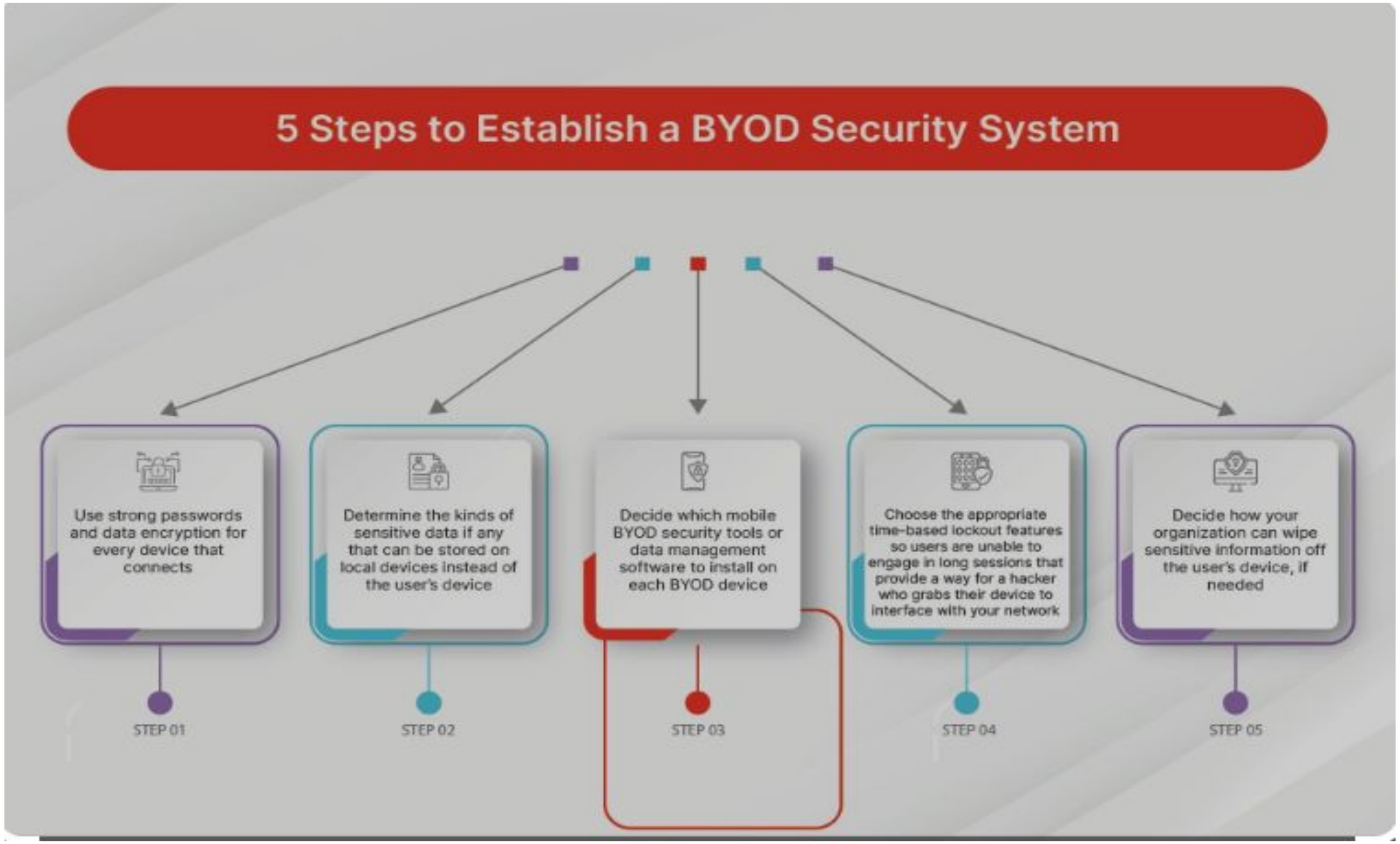
On-premise security is critical, because it is the core of the company, and that's where the majority of the users will be accessing resources. When an organization decides to extend their on-premise infrastructure with a cloud provider to use IaaS **(1)**, the company needs to evaluate the threats for this connection and the countermeasure for these threats through a risk assessment.

Personal Device used in (4) case: Yes, this is a personal device with no direct connectivity with on-premise resources. However, if this device is compromised, the user could potentially compromise the company's data in the following situations:

- Opening a corporate email from this device
- Accessing corporate SaaS applications from this device
- If the user uses the same password (8) for his/her personal email and his corporate account, this could lead to account compromise through brute force or password guessing

BYOD

BYOD, or bring your own device, refers to corporate IT policy that determines when and how employees, contractors and other authorized end users can use their own laptops, smartphones and other personal devices on the company network to access corporate data and perform their job duties.



5 Steps to Establish a BYOD Security System

STEP 01: Use strong passwords and data encryption for every device that connects

STEP 02: Determine the kinds of sensitive data if any that can be stored on local devices instead of the user's device

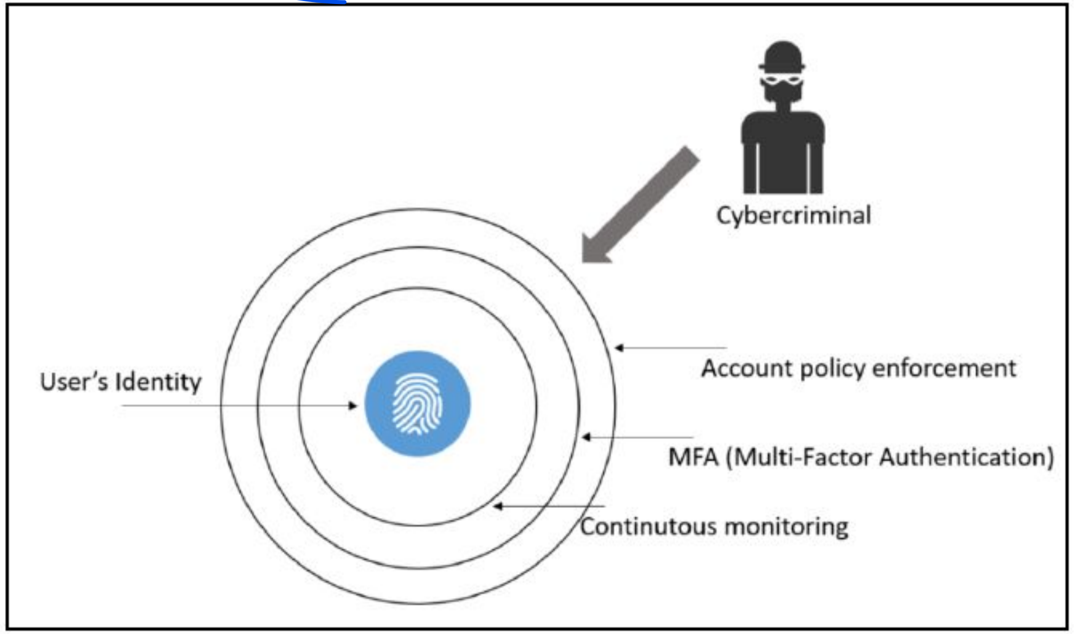
STEP 03: Decide which mobile BYOD security tools or data management software to install on each BYOD device

STEP 04: Choose the appropriate time-based lockout features so users are unable to engage in long sessions that provide a way for a hacker who grabs their device to interface with your network

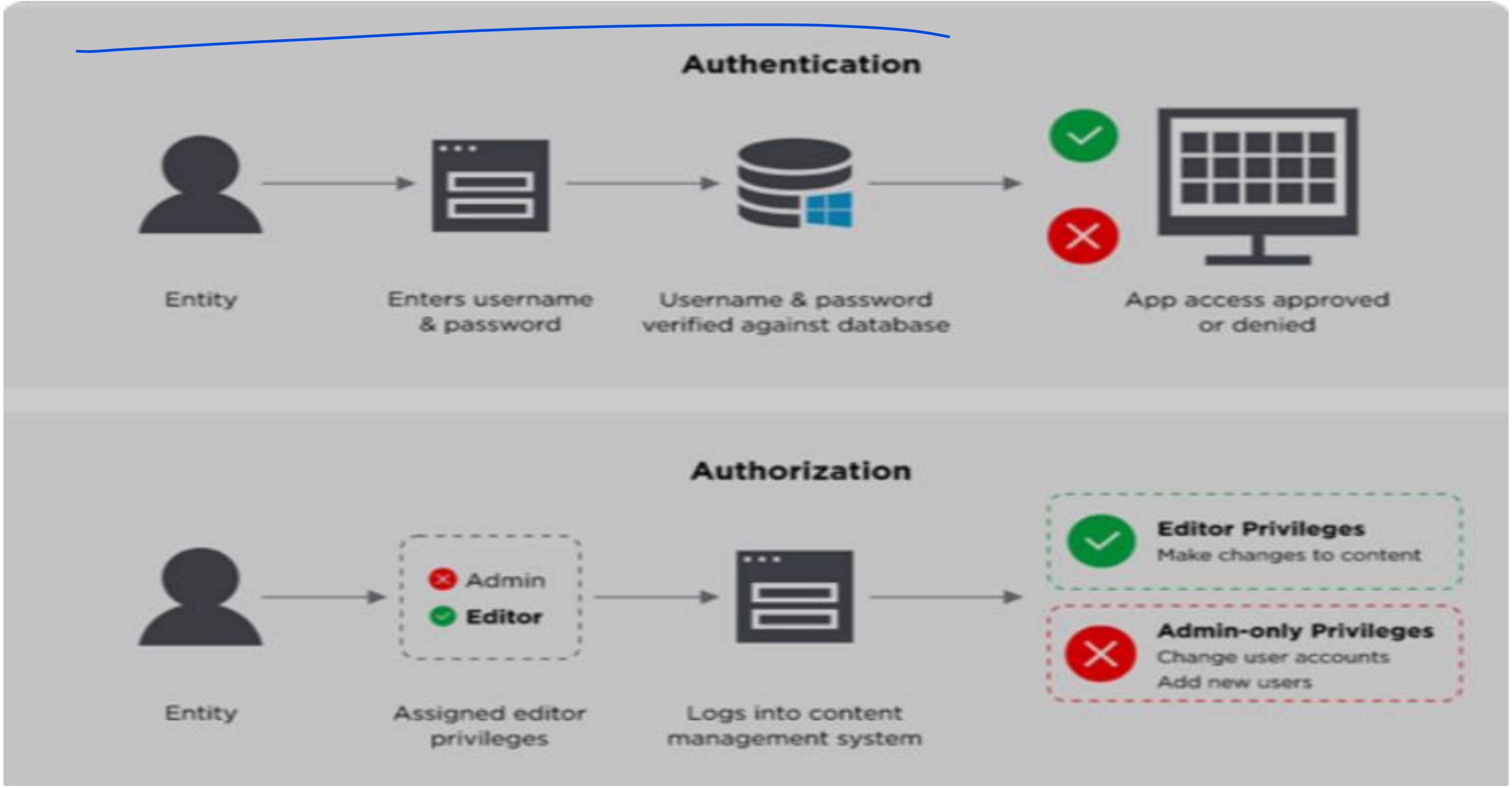
STEP 05: Decide how your organization can wipe sensitive information off the user's device, if needed

The Credentials –authentication and authorization

- The industry agreed that a user's identity is the new perimeter.
- A comprehensive Identity Security approach includes ***authenticating*** every identity accurately, ***authorizing*** each identity with the proper permissions and providing ***access*** for that identity to privileged assets in a structured manner
- This requires security controls specifically designed to authenticate and authorize individuals based on their job and need for specific data within the network.



The Credentials –authentication and authorization


Authentication
Entity
Enters username & password
Username & password verified against database
App access approved or denied
Authorization
Entity
Admin
Editor
Assigned editor privileges
Logs into content management system
Editor Privileges
Make changes to content
Admin-only Privileges
Change user accounts
Add new users

What is MFA?

- Multi-factor Authentication (MFA) is an authentication method that requires the user to provide two or more verification factors to gain access to a resource such as an application, online account, or a VPN.
- MFA is a core component of a strong identity and access management (IAM) policy.
- Rather than just asking for a username and password, MFA requires one or more additional verification factors, which decreases the likelihood of a successful cyber attack.

What is MFA is important?

- The main benefit of MFA is it will enhance your organization's security by requiring your users to identify themselves by more than a username and password.
- While important, usernames and passwords are vulnerable to brute force attacks and can be stolen by third parties.
- Enforcing the use of an MFA factor like a thumbprint or physical hardware key means increased confidence that your organization will stay safe from cyber criminals.

Applications-APPS

Applications are the entry point for the user to consume data and to transmit, process, or store information onto the system.
Apps are evolving rapidly and the adoption of SaaS-based apps is on the rise. However, there are inherited problems with this amalgamation of apps.

Here are two key examples:

- Security: How secure are these apps that are being developed in-house and the ones that you are paying for as a service?

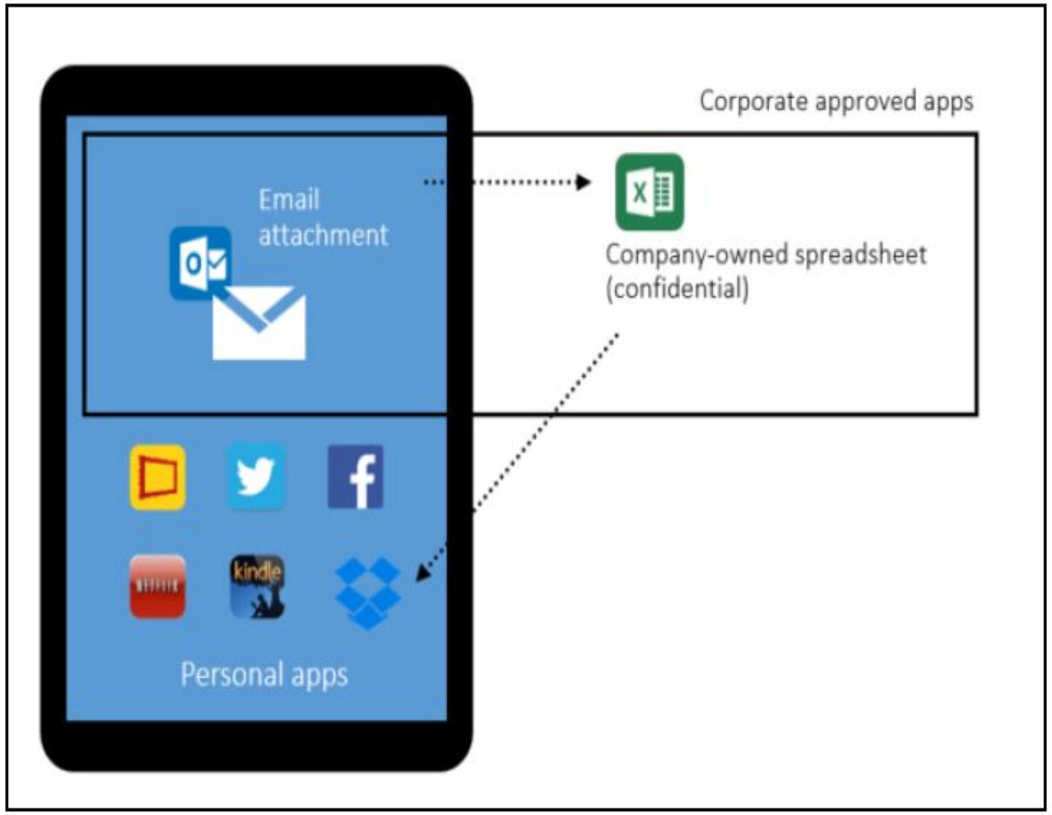
- Company-owned versus personal apps: Users will have their own set of apps on their own devices (BYOD scenario).

How do these apps jeopardize the company’s security posture and can they lead to a potential data breach?

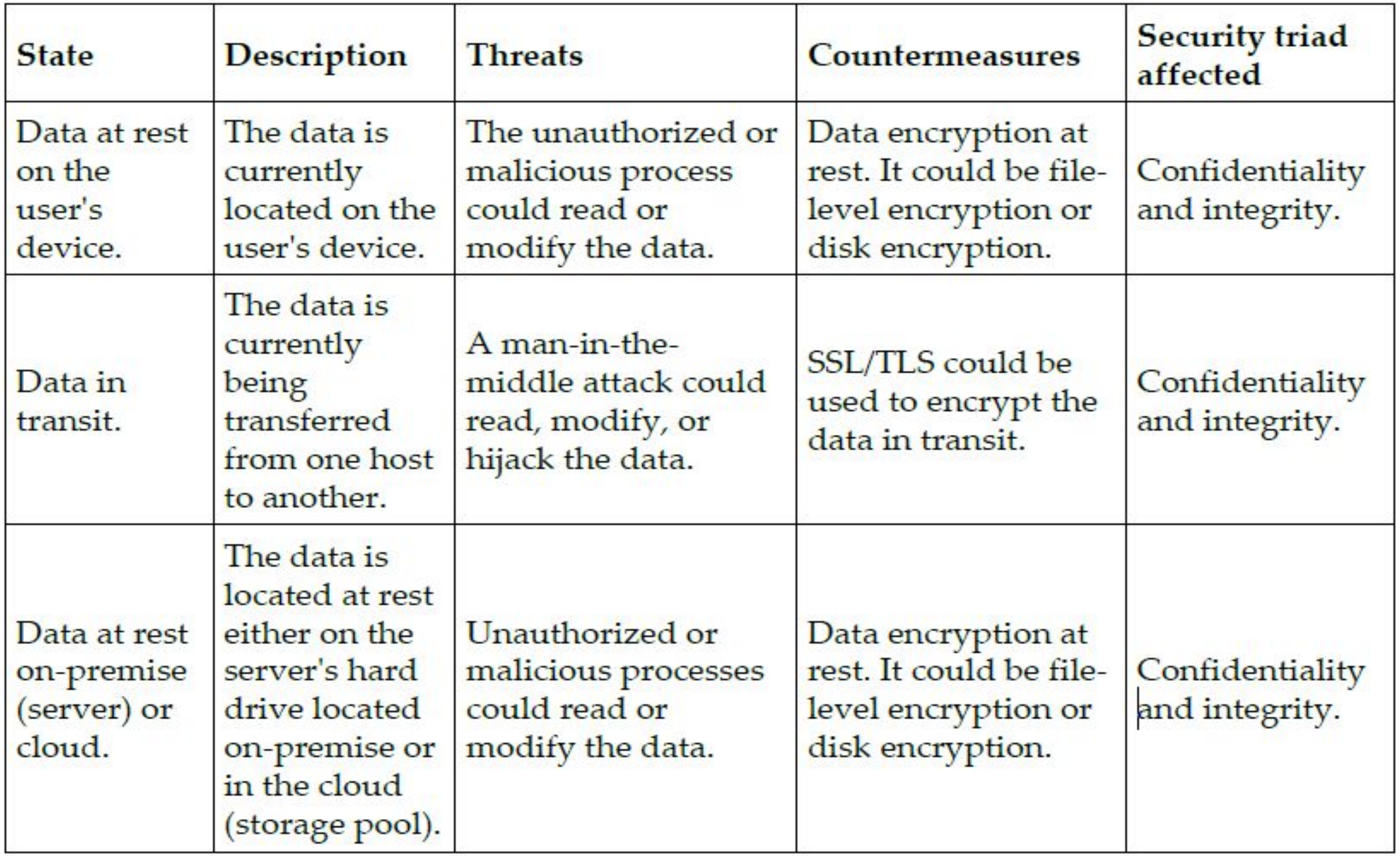
According to Kaspersky Global IT Risk Report 2016 (13), 54 percent of businesses perceive that the main IT security threats are related to inappropriate sharing of data via mobile devices. It is necessary for IT to gain control of the apps and enforce security policies across devices (company-owned and BYOD).

Apps

In this case, if the user downloads the excel spreadsheet onto his/her device and uploads it to a personal Dropbox cloud storage and the spreadsheet contains the company's confidential information, the user has now created a data leak without the company's knowledge or the ability to secure it.



Data

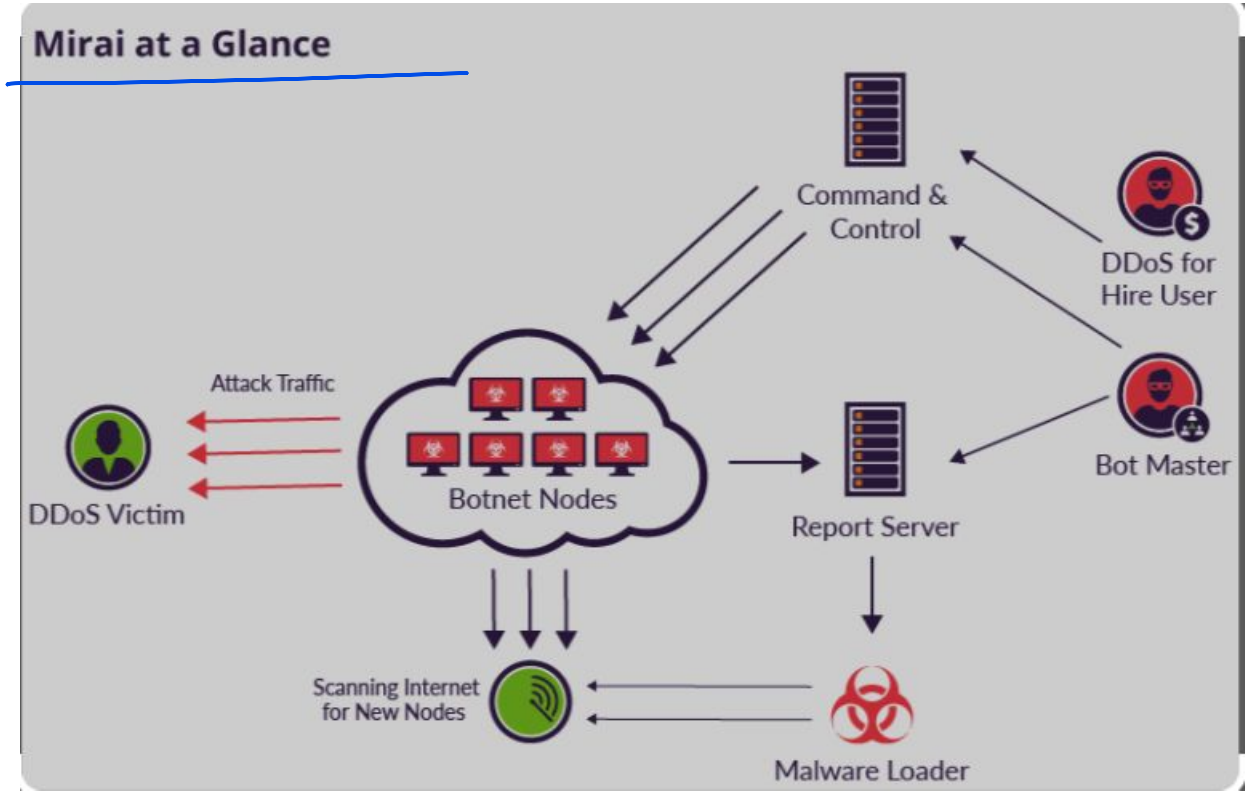


State	Description	Threats	Countermeasures	Security triad affected
Data at rest on the user's device.	The data is currently located on the user's device.	The unauthorized or malicious process could read or modify the data.	Data encryption at rest. It could be file-level encryption or disk encryption.	Confidentiality and integrity.
Data in transit.	The data is currently being transferred from one host to another.	A man-in-the-middle attack could read, modify, or hijack the data.	SSL/TLS could be used to encrypt the data in transit.	Confidentiality and integrity.
Data at rest on-premise (server) or cloud.	The data is located at rest either on the server's hard drive located on-premise or in the cloud (storage pool).	Unauthorized or malicious processes could read or modify the data.	Data encryption at rest. It could be file-level encryption or disk encryption.	Confidentiality and integrity.

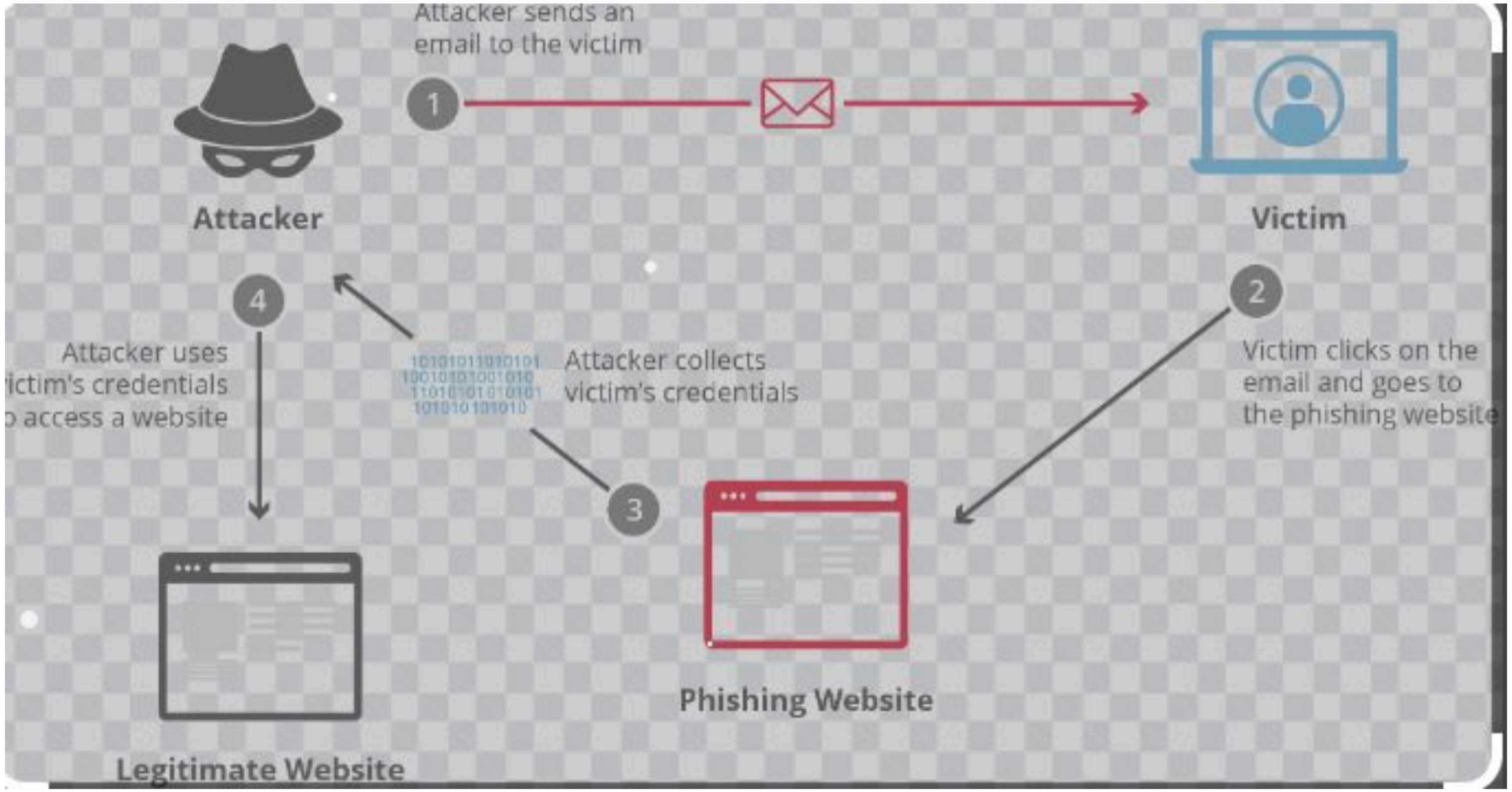
Cybersecurity Challenges

1. IoT Attacks
2. Cloud Attacks
3. Phishing Attacks
4. ~~Cryptocurrency and Blockchain Attacks~~
5. ~~Mobile Banking Malware~~
6. AI Attacks
7. Insider Attacks
8. Social Engineering Attack
9. The Man in the Middle Attack

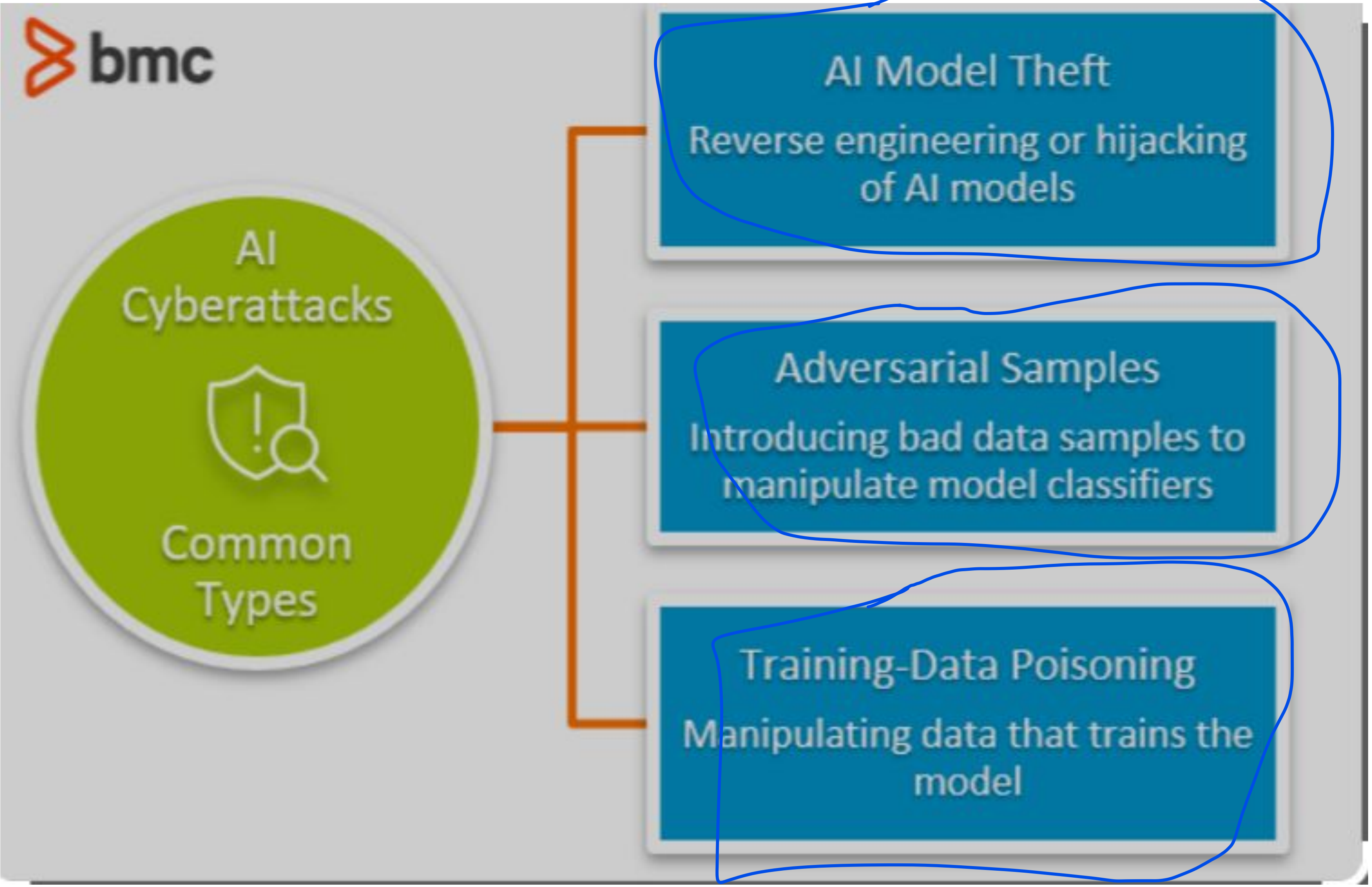
IOT Attacks-Mirai Botnet



Phishing Attack



AI Attack



AI Model Theft

Reverse engineering or hijacking of AI models

Adversarial Samples

Introducing bad data samples to manipulate model classifiers

Training-Data Poisoning

Manipulating data that trains the model

Old techniques and broader results

According to Kaspersky Global IT Risk Report 2016 (14), the top causes for the most costly data breaches are based on old attacks that are evolving over time, which are in the following order:

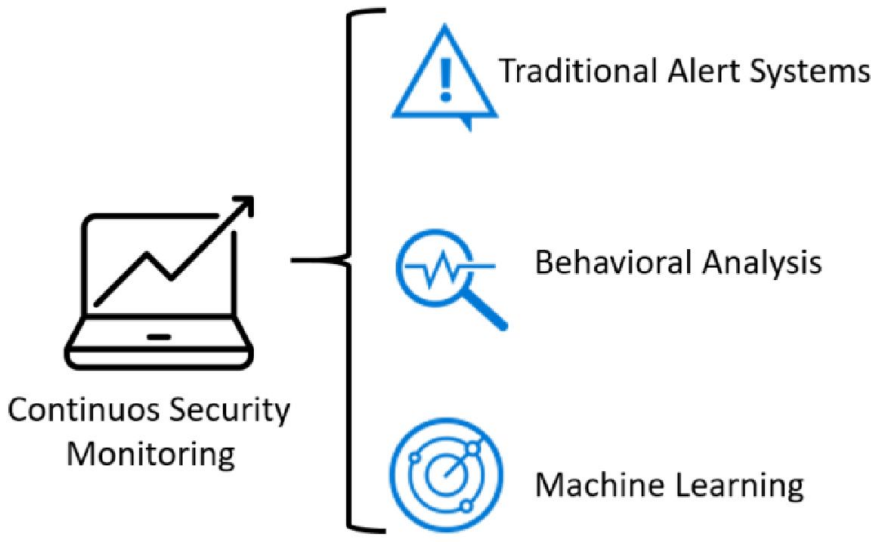
- Viruses, malware, and trojans
- Lack of diligence and untrained employees
- Phishing and social engineering
- Targeted attack
- Crypto and ransomware

The shift in the threat landscape

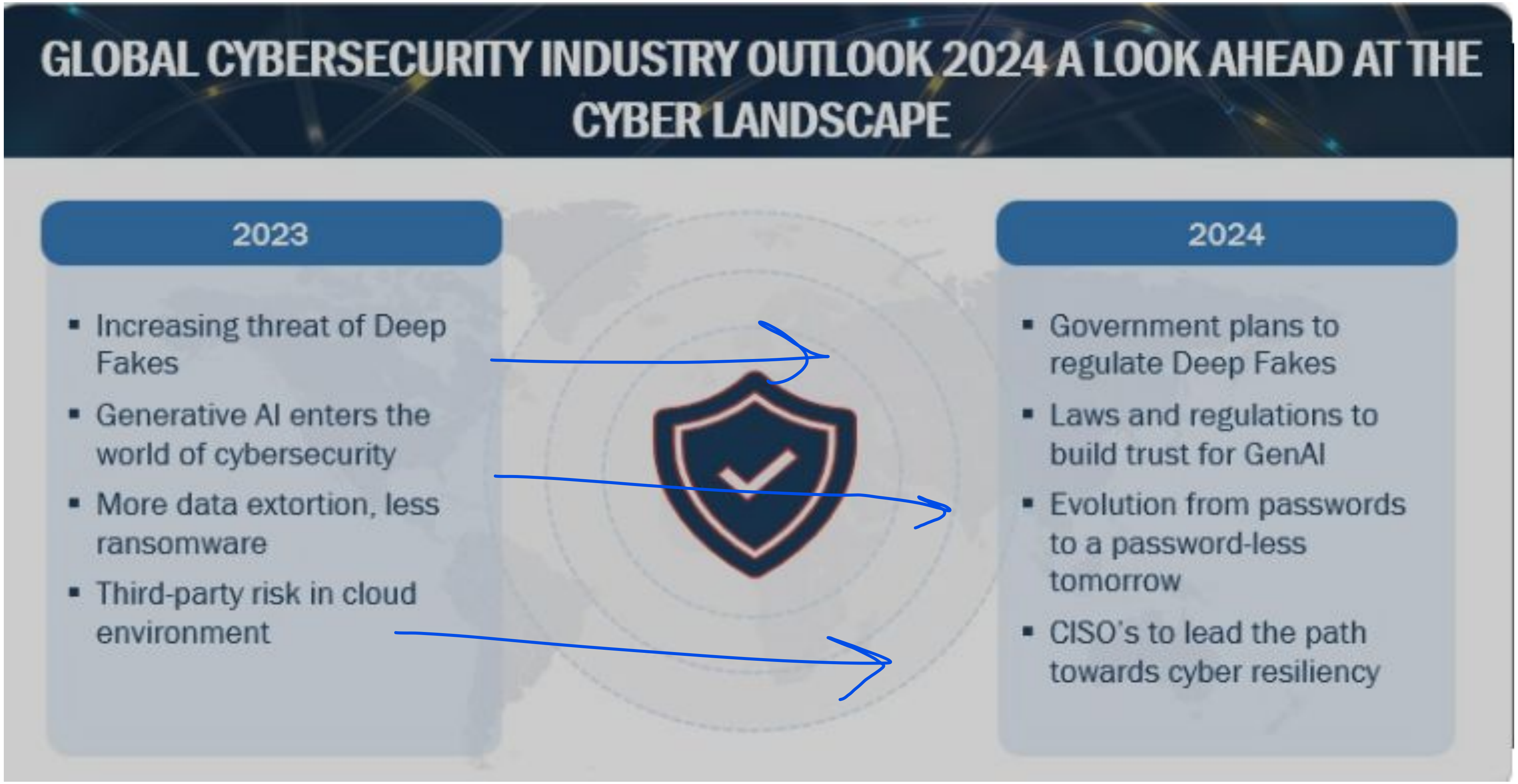
In 2016, a new wave of attacks also gained mainstream visibility, when CrowdStrike reported that it had identified two separate Russian intelligence-affiliated adversaries present in the United States Democratic National Committee (DNC) network (19).

According to their report, they found evidence that two Russian hacking groups were in the DNC network: Cozy Bear (also classified as APT29) and Fancy Bear (APT28). Cozy Bear was not a new actor in this type of attack, since evidence has shown that in 2015 they were behind the attack against the Pentagon email system via spear phishing attacks.

This type of scenario is called Government-sponsored cyber attacks, but some specialists prefer to be more general and call it data as a weapon, since the intent is to steal information that can be used against the hacked party. The private sector should not ignore these signs.



The shift in the threat landscape



GLOBAL CYBERSECURITY INDUSTRY OUTLOOK 2024 A LOOK AHEAD AT THE CYBER LANDSCAPE

2023

- Increasing threat of Deep Fakes
- Generative AI enters the world of cybersecurity
- More data extortion, less ransomware
- Third-party risk in cloud environment

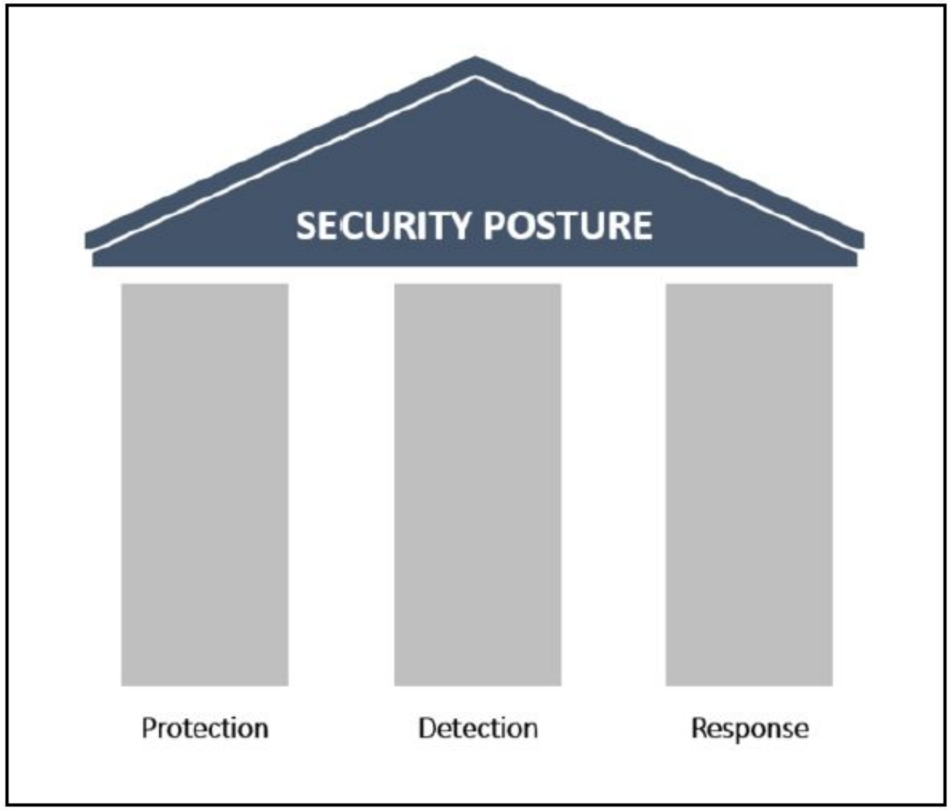
2024

- Government plans to regulate Deep Fakes
- Laws and regulations to build trust for GenAI
- Evolution from passwords to a password-less tomorrow
- CISO's to lead the path towards cyber resiliency

Enhancing your security posture

It is also important to enable IT and security operations to quickly identify an attack, by enhancing the detection system.

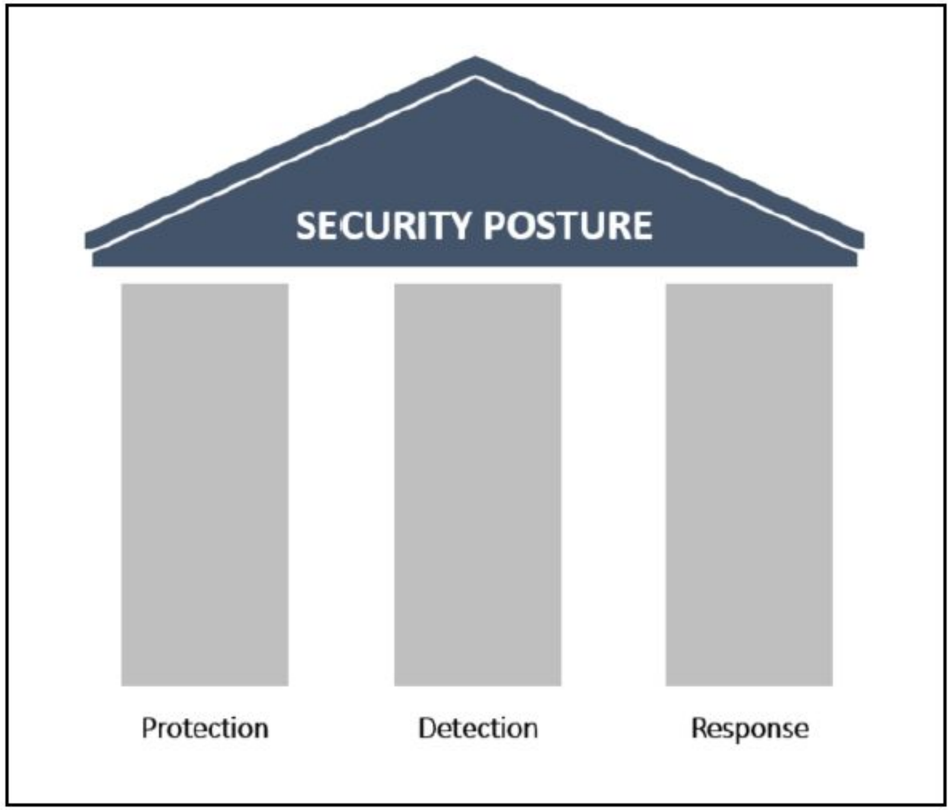
Last but certainly not least, it is necessary to reduce the time between infection and containment by rapidly responding to an attack by enhancing the effectiveness of the response process.



Enhancing your security posture

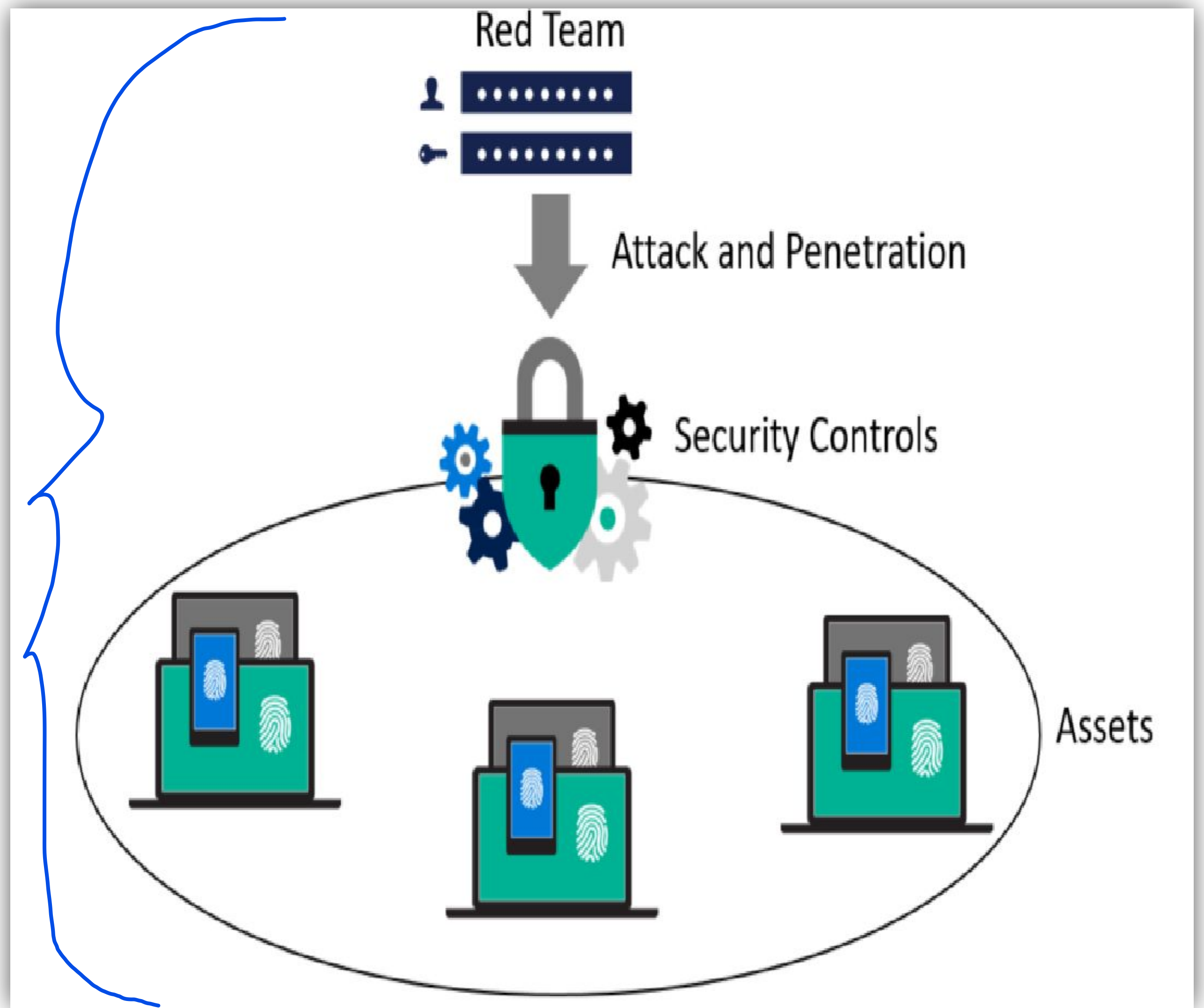
Three Pillars

1. Protection
2. Detection
3. Response



The Red and Blue Team

- In the cybersecurity field, the adoption of the Red Team approach also helped organizations to keep the assets more secure.
- The Red Team must be composed of highly trained individuals, with different skill sets and they must be fully aware of security trends and attacks are taking place.
- Red Team must have coding skills to create their own exploit and customize it to exploit relevant vulnerabilities.



Red Team Workflow

The Red Team and Blue Team

Red Team Metrics:-

- **MTTC(Mean Time to Compromise)**
- **MTTP(Mean Time to Privilege Escalation)**

Blue Team Metrics:-

- **ETTD(Estimated Time to Detection)**
- **ETTR(Estimated Time to Recovery)**

Tasks done by Blue Team

- Save Evidence
- Validate the Evidence
- Engage whoever is necessary to Engage
- Triage the incident
- Scope the breach
- Create a Remediation Plan
- Execute the Plan

Chapter 2: Incident Response Process

Security Incidents:-

- User clicks an email attachment and executes malware
  -Malware communicates with external servers
- DDOS attack
  -Botnet attack
- Confidential Information is stolen
  -thief wants money or it goes public
- User installs peer-peer software and allows external access to internal servers

Roles and Responsibilities:-

- Incident Response Team
  -Specialized group, Trained or Tested
- IT security management
  -Corporate Support
- Compliance officers
  -Intricate knowledge of compliance rules
- Technical Staff
- User Community

Chapter 2: Incident Response Process

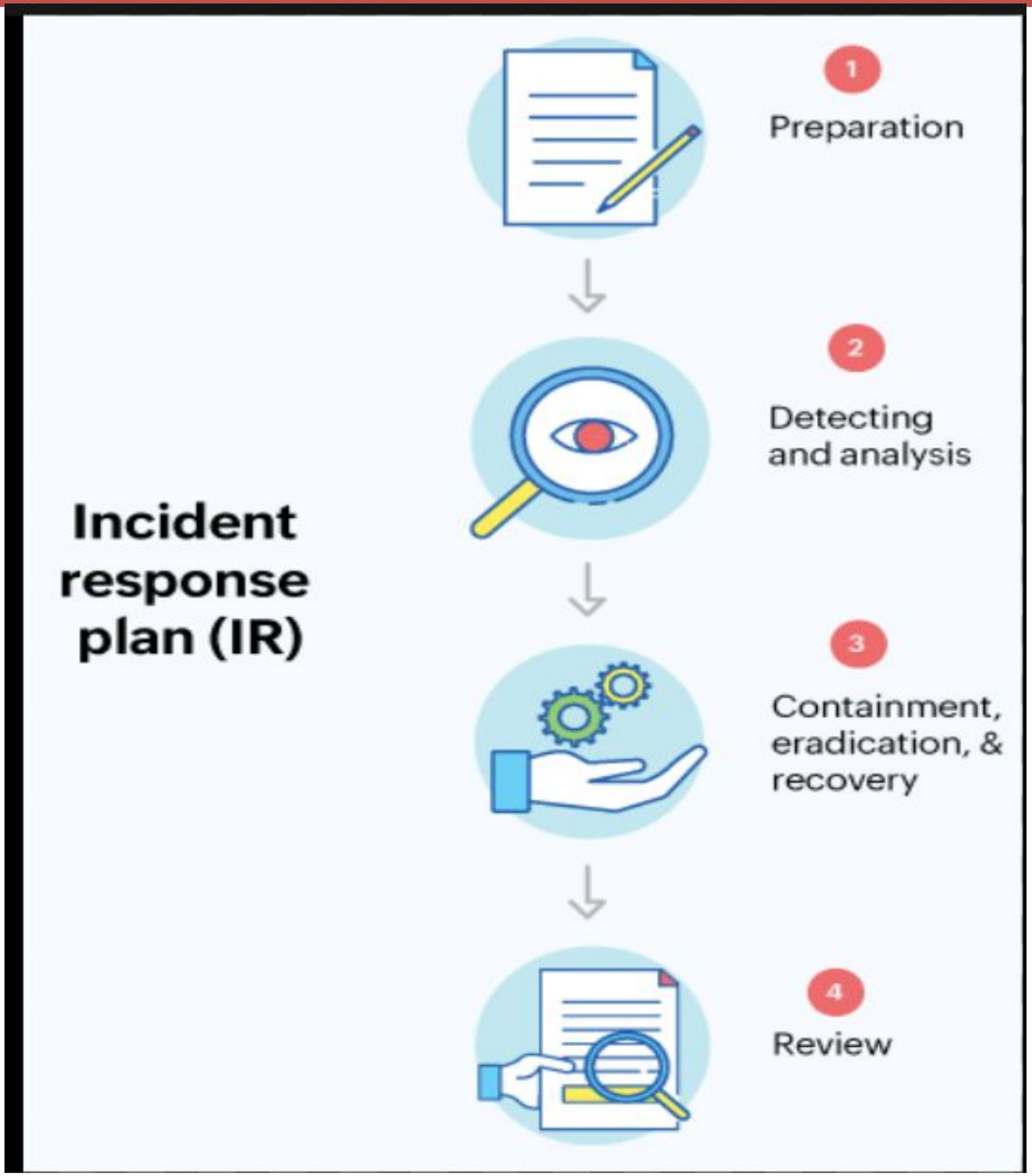
National Institute of Standards and Technology(NIST)-computer security incident handling guide

Incidence Response Lifecycle:

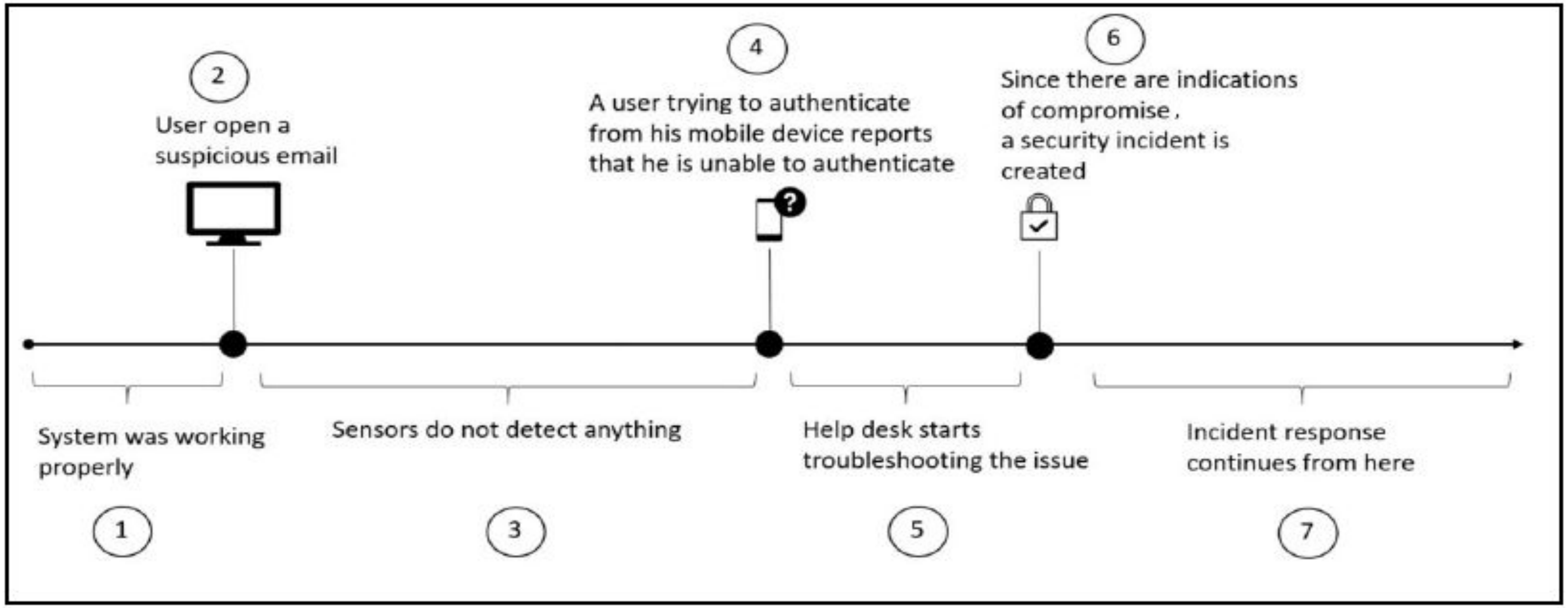
- Preparation
- Detection and Analysis
- Containment, Eradication and Recovery
- Post Incident Activity

Chapter 2: Incident Response Process

Incident response (IR) is the process by which an organization handles a data breach or cyberattack. It is an effort to quickly identify an attack, minimize its effects, contain damage, and remediate the cause to reduce the risk of future incidents.

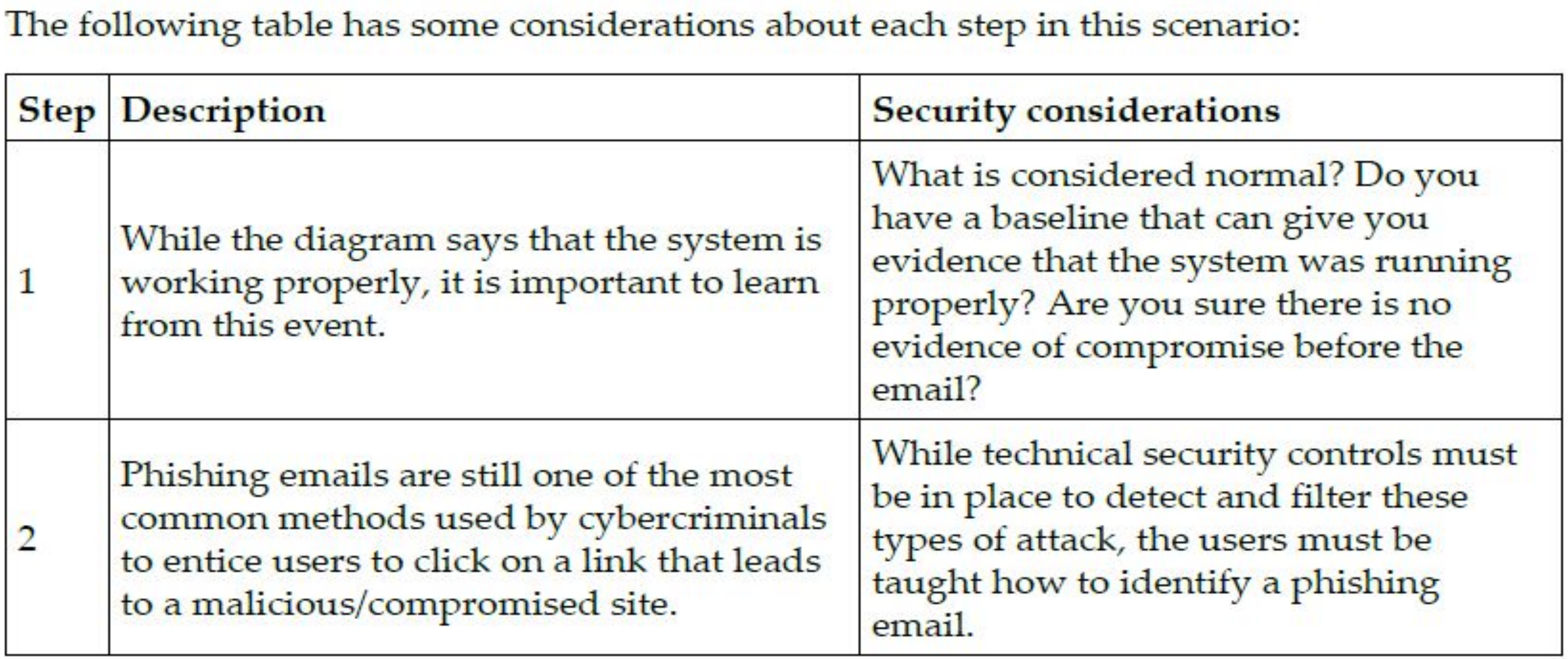

Incident response plan (IR)
1
Preparation
2
Detecting and analysis
3
Containment, eradication, & recovery
4
Review

2.1 Reasons to have IR process in place.


2
User open a suspicious email
4
A user trying to authenticate from his mobile device reports that he is unable to authenticate
6
Since there are indications of compromise ,
a security incident is created
System was working properly
1
Sensors do not detect anything
3
Help desk starts troubleshooting the issue
5
Incident response continues from here
7

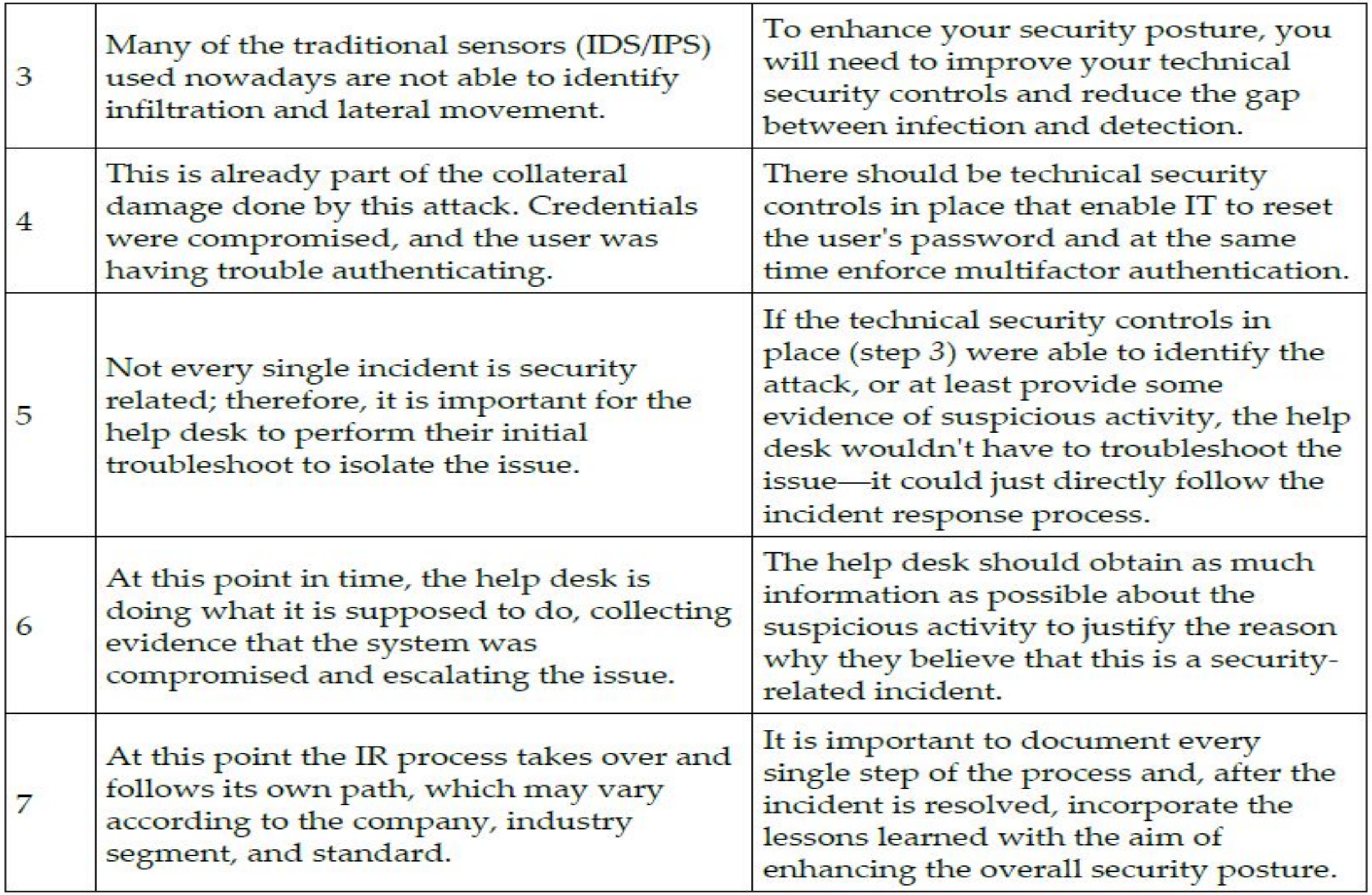
The following diagram has a timeline of events(2) that leads the help desk to escalate the issue and start the incident response process:

Chapter 2: Incident Response Process



The following table has some considerations about each step in this scenario:

Step	Description	Security considerations
1	While the diagram says that the system is working properly, it is important to learn from this event.	What is considered normal? Do you have a baseline that can give you evidence that the system was running properly? Are you sure there is no evidence of compromise before the email?
2	Phishing emails are still one of the most common methods used by cybercriminals to entice users to click on a link that leads to a malicious/compromised site.	While technical security controls must be in place to detect and filter these types of attack, the users must be taught how to identify a phishing email.



3	Many of the traditional sensors (IDS/IPS) used nowadays are not able to identify infiltration and lateral movement.	To enhance your security posture, you will need to improve your technical security controls and reduce the gap between infection and detection.
4	This is already part of the collateral damage done by this attack. Credentials were compromised, and the user was having trouble authenticating.	There should be technical security controls in place that enable IT to reset the user's password and at the same time enforce multifactor authentication.
5	Not every single incident is security related; therefore, it is important for the help desk to perform their initial troubleshoot to isolate the issue.	If the technical security controls in place (step 3) were able to identify the attack, or at least provide some evidence of suspicious activity, the help desk wouldn't have to troubleshoot the issue—it could just directly follow the incident response process.
6	At this point in time, the help desk is doing what it is supposed to do, collecting evidence that the system was compromised and escalating the issue.	The help desk should obtain as much information as possible about the suspicious activity to justify the reason why they believe that this is a security-related incident.
7	At this point the IR process takes over and follows its own path, which may vary according to the company, industry segment, and standard.	It is important to document every single step of the process and, after the incident is resolved, incorporate the lessons learned with the aim of enhancing the overall security posture.

Guidelines to be adhered:

- All IT personnel should be trained to know how to handle a security incident.
- All users should be trained to know the core fundamentals about security in order to perform their job more safely, which will help avoid getting infected.
- There should be integration between their help desk system and the incident response team for data sharing.
- If in the above given scenario if no **indication of compromise** (**IoC**) was found in step *6*. In this case, the help desk would easily keep troubleshooting the issue. What if at some point things started to work normally again? Is this even possible? Yes, it is!
- Incident response process in place to be compliant with regulations that are applicable to the industry in which they belong. For example, FISMA requires federal agencies to have procedures in place to detect, report, and respond to a security incident.

Creating an Incident Response Process

1. Establish the Objective

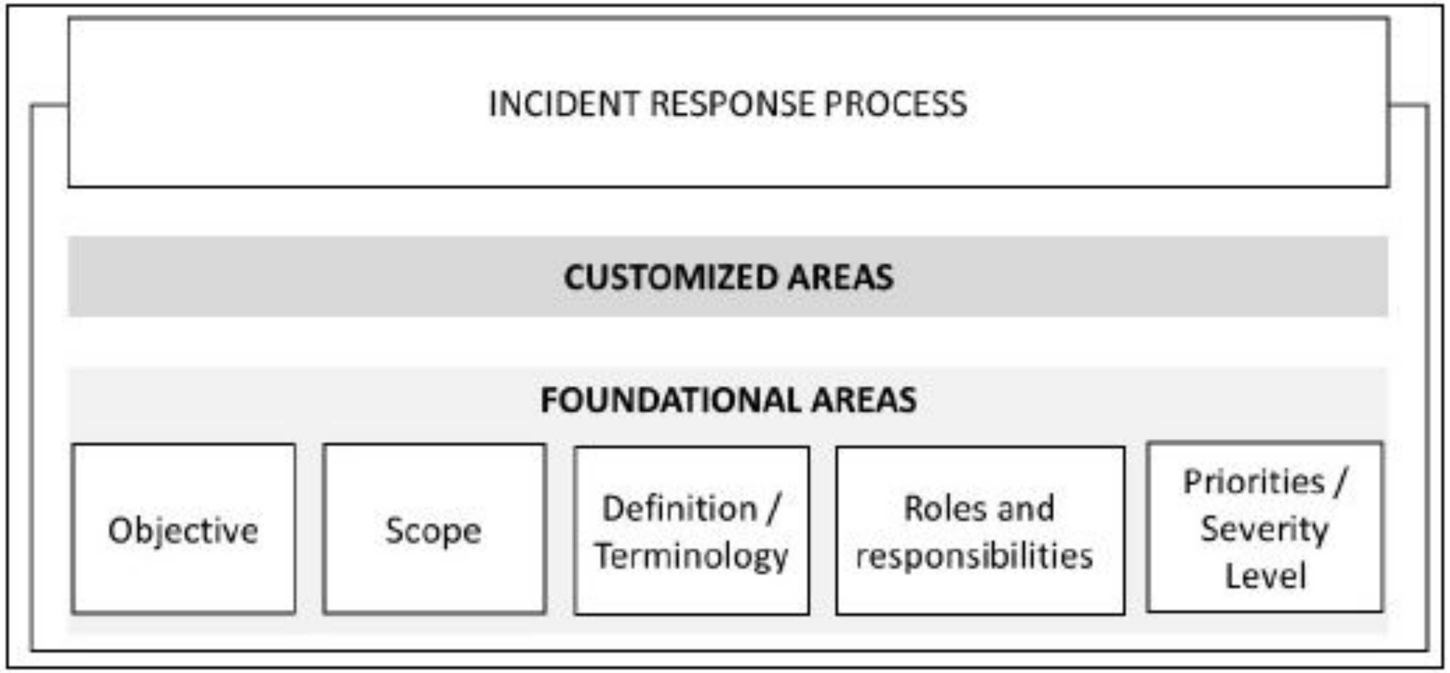
- What's the purpose of this process?
- What is the process is going to accomplish?

2. Scope

- To whom does the process apply?
- Whether it is a company wide process or not?

3. Definition/Terminology

Companies create different set of terminologies, relevant terminologies to security incident must be documented.



INCIDENT RESPONSE PROCESS
CUSTOMIZED AREAS
FOUNDATIONAL AREAS
Objective
Scope
Definition / Terminology
Roles and responsibilities
Priorities / Severity Level

Foundational Areas of Incident Response Process

Creating an Incident Response Process

4. Roles and Responsibilities

- Without proper level of authority , the entire process is at risk.
- Who has the authority to confiscate a computer in order to perform further investigation?

5. Priority and Security Level

- What defines a critical incident?
- How are you going to distribute your manpower when an incident occurs?
- Should you allocate more resources to incident "A" versus incident "B"?
- Why?

Priority and Security Level

Functional impact of the incident in the business: The importance of the affected system for the business will have a direct effect on the incident's priority. All stakeholders for the affected system should be aware of the issue, and will have their input in the determination of priorities.

Type of information affected by the incident: Every time you deal with PII, your incident will have high priority; therefore, this is one of the first elements to verify during an incident.

Recoverability: After the initial assessment, it is possible to give an estimate of how long it will take to recover from an incident. Depending on the amount of time to recover, combined with the criticality of the system, this could drive the priority of the incident to high severity.

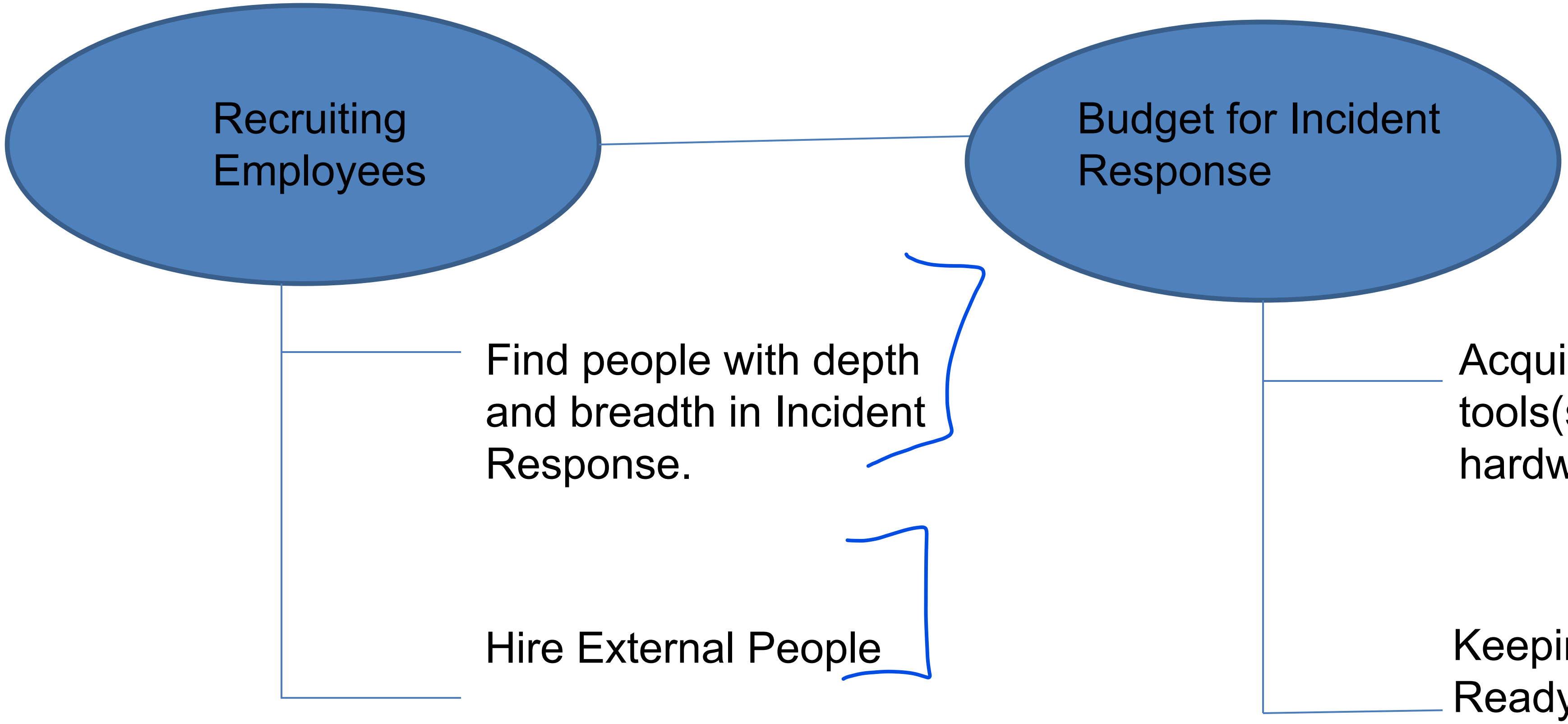
Also very important to answer below questions:

1. Customer's personal identifiable Information(PII) was leaked.
2. How will the company communicate this to the media?

Incident Response Team

- The format of the team will vary according to the company size, budget, and purpose.
- A large company may want to use a distributed model, where there are multiple incident response teams with each one having specific attributes and responsibilities.
- This model can be very useful for organizations that are geodispersed, with computing resources located in multiple areas.
- Other companies may want to centralize the entire incident response team in a single entity. This team will handle incidents regardless of the location.

Incident Response Team



Recruiting Employees

- Find people with depth and breadth in Incident Response.
- Hire External People

Budget for Incident Response

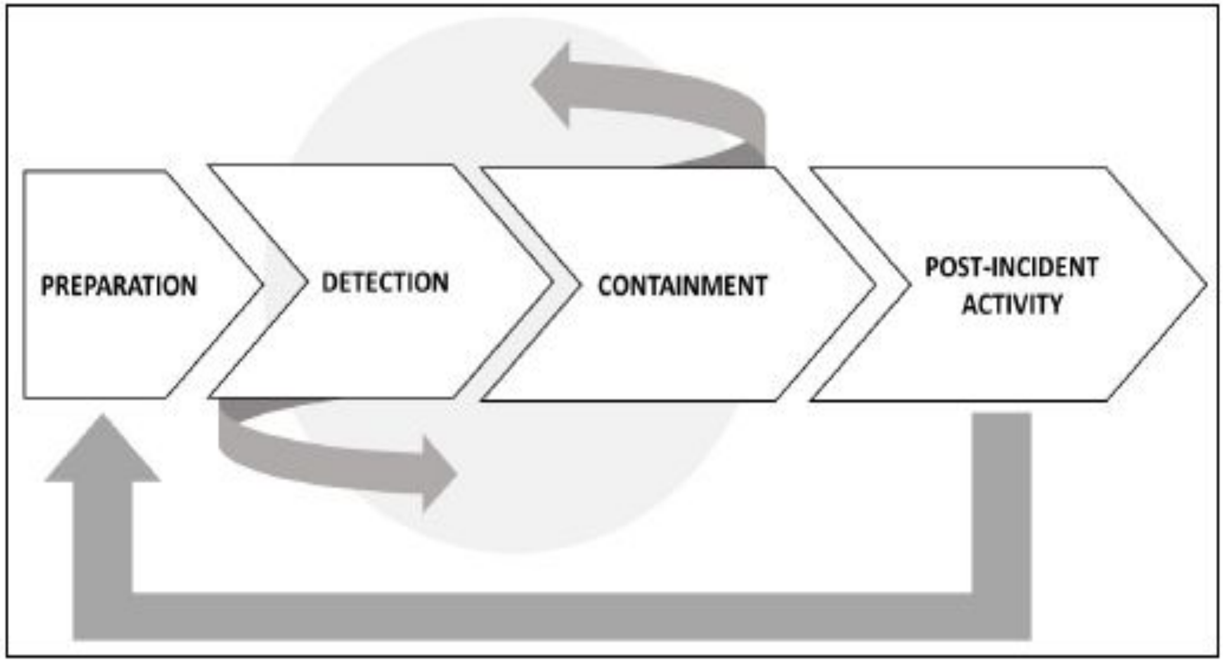
- Acquisition of proper tools(software) and hardware
- Keeping the workforce Ready. Outsourcing the Incident Response process

SLA for Incident Response

service-level agreement (SLA) that meets the severity levels that were established previously. During this phase, you should also define the team coverage, assuming the need for 24-hour operations.

- Shifts: How many shifts will be available for 24-hour coverage?
- Team allocation: Based on this shift, who is going to work on each shift, including full-time employees and contractors?
- On-call process: It is recommended that you have on-call rotation for technical and management roles in case the issue needs to be escalated.

Incident Response Cycle



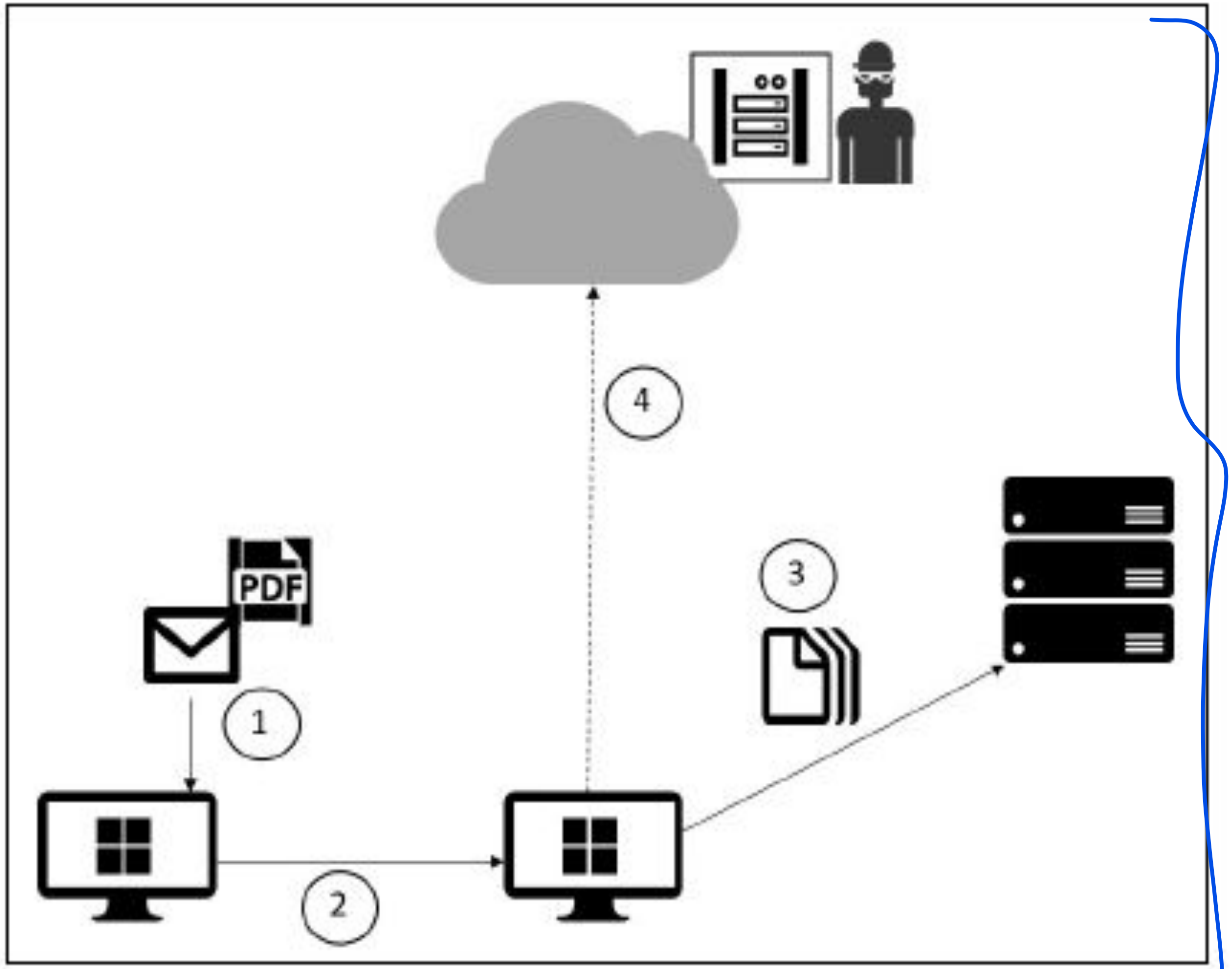
Preparation phase is the implementation of other security controls:

- Endpoint protection
- Malware protection
- Network security

Preparation phase is not static, will receive input from Post-Incident Activity

The DETECTION and CONTAINMENT phase could have multiple interactions within the same incident. Once the loop is over, you will move on to the post-incident activity phase.

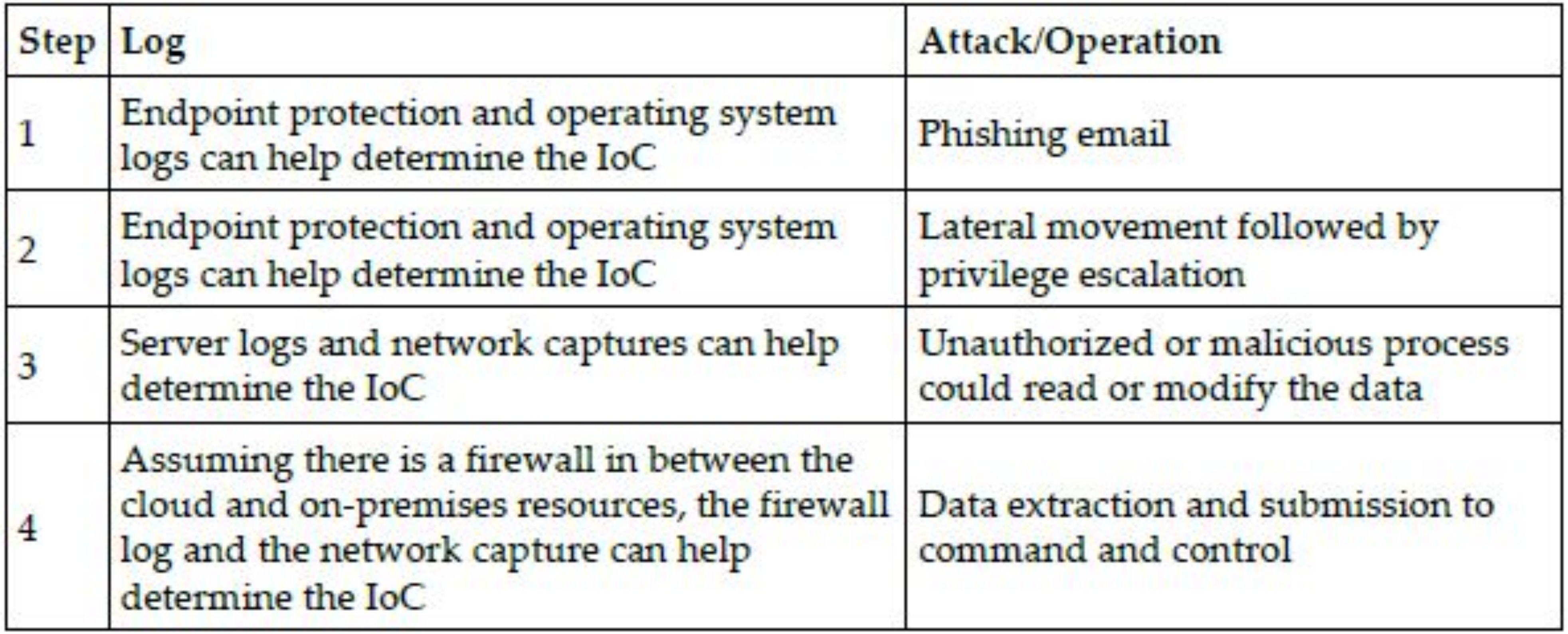
Handling the Incidence



Handling the incidence includes:

- Detection and containment phases.
- Detection system must be aware of the attack Vectors.
- Learning more about new threats, behaviors.
- Alert incase of suspicious activity
- Security awareness training for the user.
- Gathering information from different sources

Rules of Digital Evidence



Step	Log	Attack/Operation
1	Endpoint protection and operating system logs can help determine the IoC	Phishing email
2	Endpoint protection and operating system logs can help determine the IoC	Lateral movement followed by privilege escalation
3	Server logs and network captures can help determine the IoC	Unauthorized or malicious process could read or modify the data
4	Assuming there is a firewall in between the cloud and on-premises resources, the firewall log and the network capture can help determine the IoC	Data extraction and submission to command and control

Explanation of above diagram

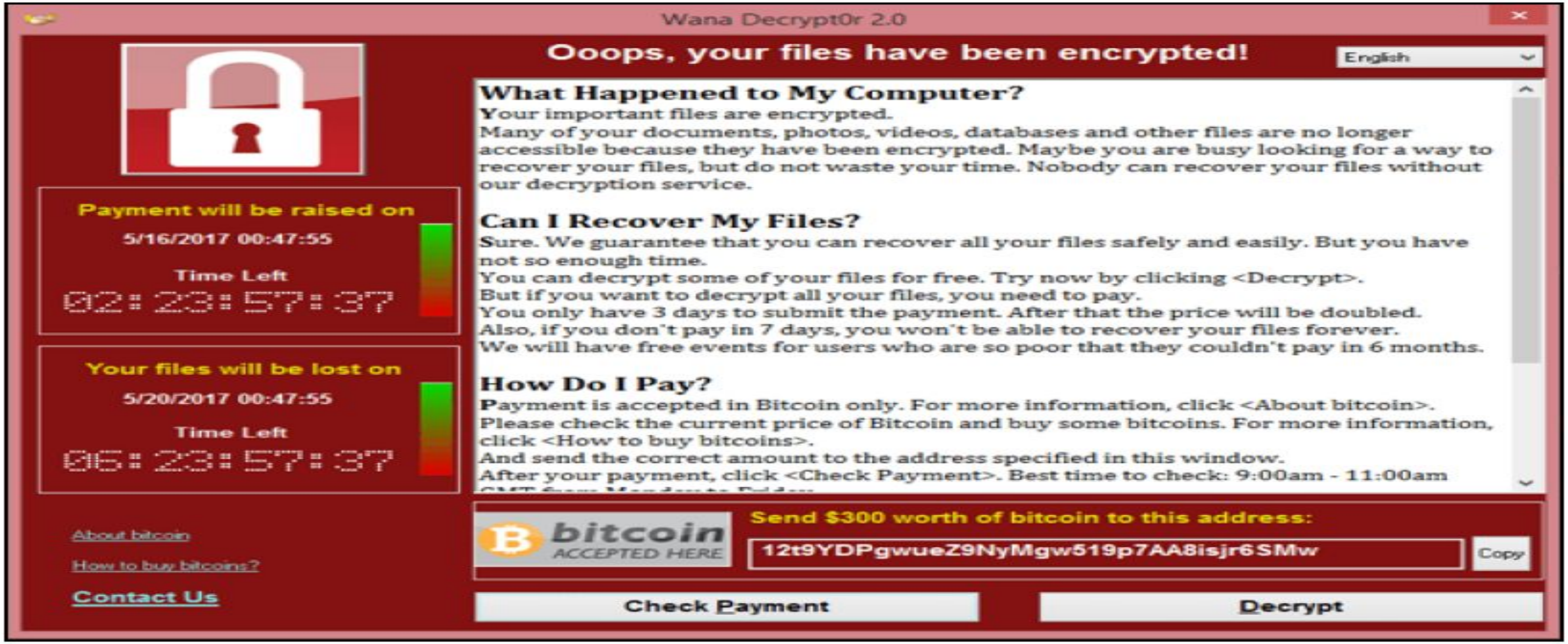
Best Practices to optimize incident handling

- System profile
- Network profile/baseline
- Log-retention policy
- Clock synchronization across all systems

~~Post-incident activity~~

Real-world scenario

Let's use the WannaCry outbreak as a real-world example, using the fictitious company Diogenes & Ozkaya Inc. to demonstrate the end-to-end incident response process.



Ooops, your files have been encrypted!

Payment will be raised on

5/16/2017 00:47:55

Time Left

02:23:57:37

Your files will be lost on

5/20/2017 00:47:55

Time Left

06:23:57:37

What Happened to My Computer?

Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.

Send $300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Post-incident activity

After an initial assessment and confirmation of the issue (detection phase), the security team was engaged and an incident was created. Since many systems were experiencing the same issue, they raised the severity of this incident to high. They used their threat intelligence to rapidly identify that this was a ransomware outbreak, and to prevent other systems from getting infected, they had to apply the MS17-00(3) patch.

At this point, the incident response team was working on three different fronts:

- Try to break the ransomware encryption
- Try to identify other systems that were vulnerable to this type of attack
- Working to communicate the issue to the press.
- The incident response team worked with antimalware vendor to break the encryption and gain access to the data again.

Post-incident activity

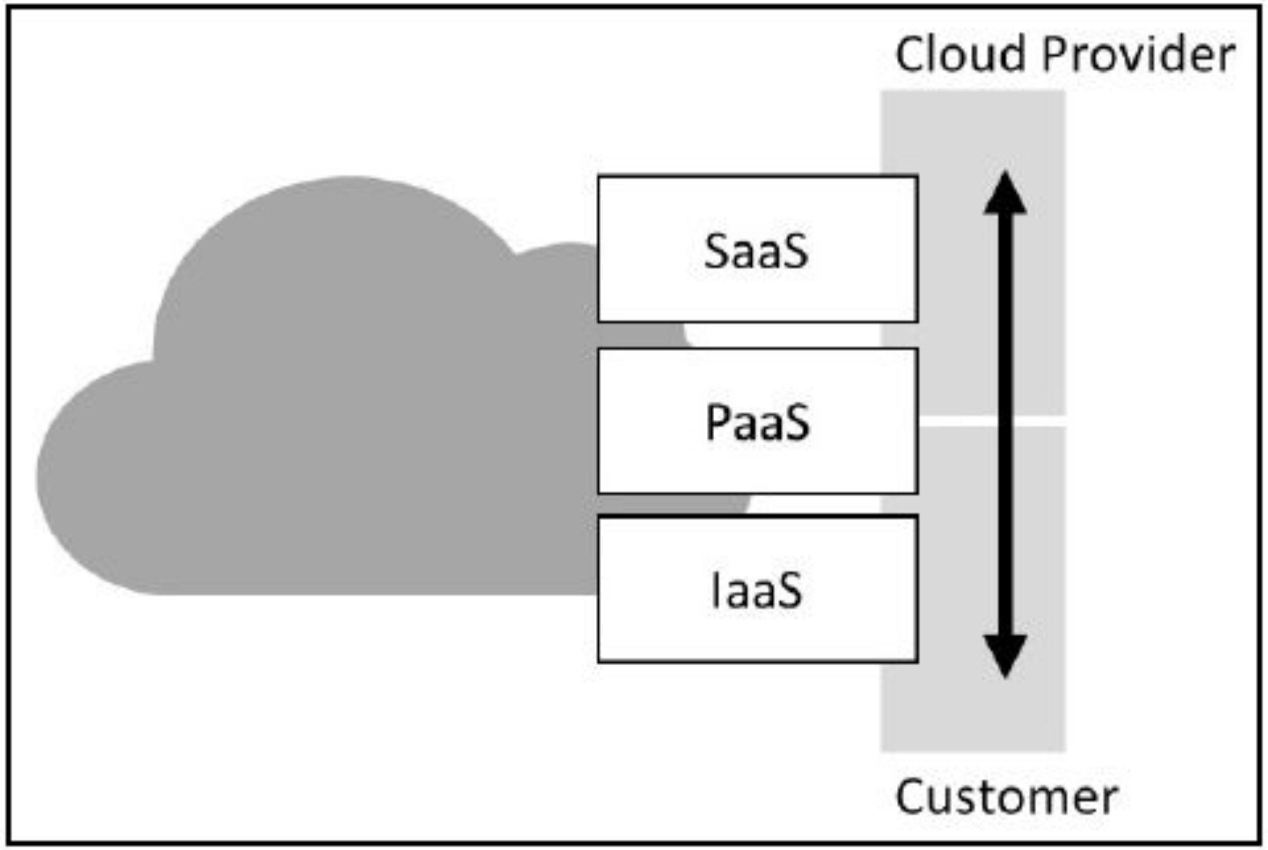
Lessons Learned

“Incident is not finished when the issue is resolved, It is the just beginning of a whole different level of work that needs to be done for every single incident”

This documentation will be used as a base to answer the following questions:

Who identified the security issue? A user or the detection system?
Was the incident opened with the right priority?
Did the security operations team perform the initial assessment correctly?
Is there anything that could be improved at this point?
Was the data analysis done correctly?
Was the containment done correctly?
Is there anything that could be improved at this point?
How long did it take to resolve this incident?

Incident Response in the cloud



- For Software as a Service (SaaS), most of the responsibility is on the Cloud Provider; in fact, the customer's responsibility is basically to keep his or her infrastructure on premises protected (including the endpoint that is accessing the cloud resource).
- For Infrastructure as a Service (IaaS),most of the responsibility lies on the customer's side, including vulnerability and patch management

Updating your IR process to include cloud

- Preparation:- you need to update the contact list to include the cloud provider contact information, on-call process, and so on.
- Detection: Depending on the cloud model that you are using, you want to include the cloud provider solution for detection in order to assist you during the investigation .
- Containment: Revisit the cloud provider capabilities to isolate an incident in case it occurs, which will also vary according to the cloud model that you are using.
- For example, if you have a compromised VM in the cloud, you may want to isolate this VM from others in a different virtual network and temporarily block access from outside.

QUIZ