



BỘ LAO ĐỘNG - THƯƠNG BINH VÀ XÃ HỘI
TỔNG CỤC GIÁO DỤC NGHỀ NGHIỆP
DIRECTORATE OF VOCATIONAL EDUCATION AND TRAINING

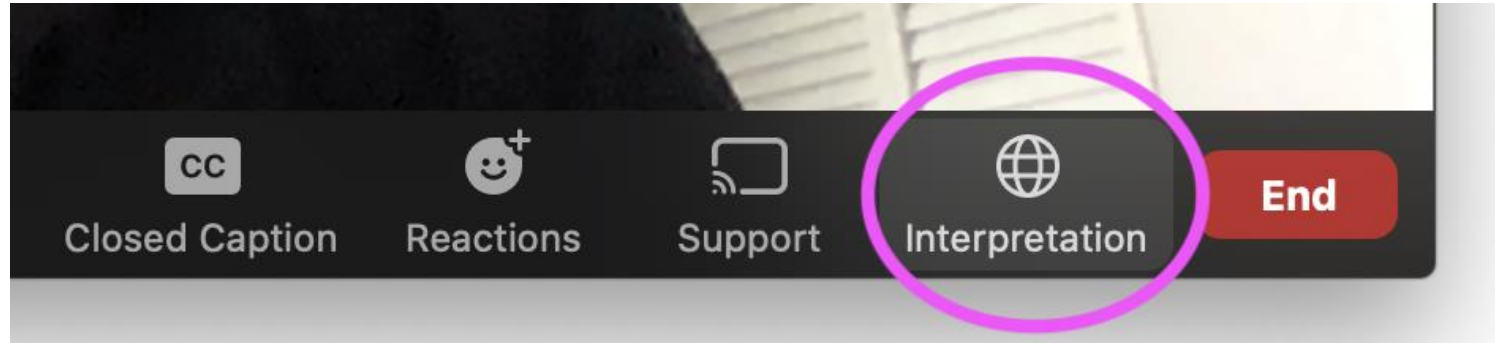
Emerging trends in the cybersecurity landscape

Webinar Two

Saturday 26 August



Please ensure you're on the right interpretation channel on Zoom



Webinar Agenda

Start	End	Duration	Session Title	Facilitator
09:00	09:15	15	Introduction to webinar	Michael Barton
09:15	09:40	25	Cyber security threats + QA	Michael Barton
09:40	10:00	20	Discussion on threats within Vietnam	Michael Barton
10:00	10:30	30	Creating a cyber security policy + QA	Michael Barton
10:30	10:50	20	Cloud Based Security/ plan + QA	Michael Barton
10:50	11:30	40	Demo on RMIT cyber prevention tools	Michael Barton
11:30	11:50	20	Industry Guest Speaker	Nguyễn Quốc Cường
11:50	12:00	10	Conclusion and Wrap up	Michael Barton

EDUCATING STAFF AND USERS TO RISKS AND DANGERS

By looking at how your business uses IT, you can:

- understand and identify the types of IT risks
- understand the impact of risks on your business
- manage risks using policies and procedures
- conduct regular staff training to further lower risk from potential threats.



1. KEY STAFF EDUCATION TOPICS

Education topics should align with your end-user security policy. The top topics staff need to know about are:

- How to choose a strong password
- How to avoid clicking on links or open attachments in a suspect, unsolicited or unexpected email
- How to spot scam and phishing emails
- Never to respond to emails requesting personal, financial information and passwords
- Where and how to store sensitive information
- How to avoid reusing passwords or sharing user accounts unsafely
- How to keep devices secure
- How to respond to a suspected or actual security incident or data breach.

2. CYBER SECURITY POLICY

A staff cyber security policy coupled with training can do more to keep your workplace computers safe than any single piece of software.

The policy should guide staff and volunteers to using the internet and other communications technologies appropriately, covering topics such as:

- which uses of email and internet are acceptable
- how to handle sensitive data
- keeping equipment secure
- how to use the internet safely
- what to do if working off-site.
- You should run through it with new staff and train them in the safe use of technology.

CREATE A CYBER SECURITY POLICY

- If your business doesn't have a cyber security policy, you could be leaving yourself open to cyberattacks.
- Create a cyber security policy to protect your business and plan how you would respond if an incident occurred.



WHAT IS A CYBER SECURITY POLICY?

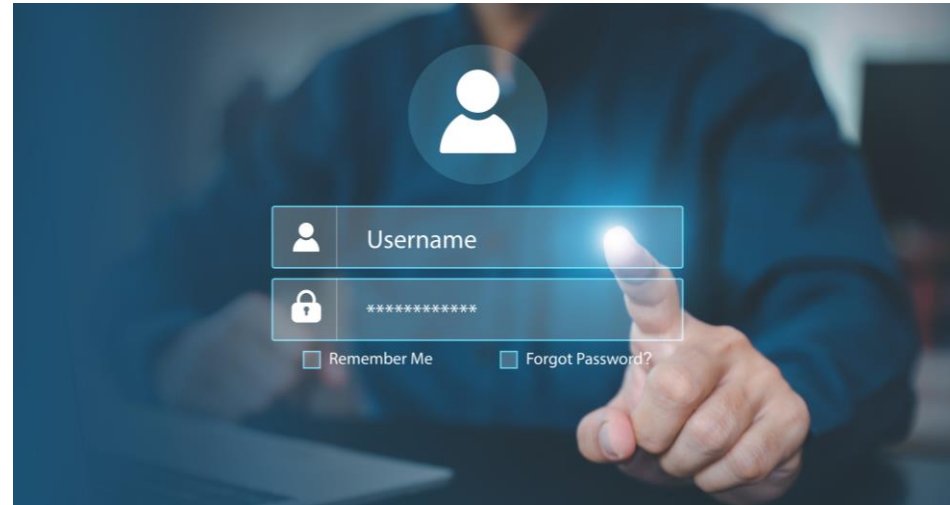
- technology and information assets that you need to protect
- threats to those assets
- rules and controls for protecting them and your business
- the type of business information that can be shared and where it can be shared
- acceptable use of devices and online materials
- handling and storage of sensitive material

When developing your cyber security policy consider the following steps...

1. SET PASSWORD REQUIREMENTS

Your cyber security policy should explain:

- requirements to create strong passphrases
- how to store passphrases correctly
- how often you need to update passphrases
- the importance of having unique passphrases for different logins



2. OUTLINE EMAIL SECURITY MEASURES

Include guidelines on:

- when it's appropriate to share your work email address
- only opening email attachments from trusted contacts and businesses
- blocking junk, spam and scam emails
- identifying, deleting and reporting suspicious-looking emails.



3. SAFE USE OF EMAIL

There are a few simple rules for safely opening email:

- Be cautious of any email that asks you for passwords, log in information or personal details (especially banking details!)
- Check that the sender's email address is legitimate
- Only open attachments or click on links from people you know
- If you're unsure, ask for help
- Know who your IT support person is in case of an emergency
- Email isn't a good way to send sensitive information, and in the case of some information
 - for example when you're dealing with Student Records – you're required to use a secure messaging system instead.

4. EXPLAIN HOW TO HANDLE SENSITIVE DATA

When it comes to handling sensitive data, outline:

- when staff may share sensitive data with others
- ways they should store physical files with sensitive data, such as in a locked room or drawer
- ways to properly identify sensitive data
- ways to destroy any sensitive data when it is no longer needed



5. SET RULES AROUND HANDLING TECHNOLOGY

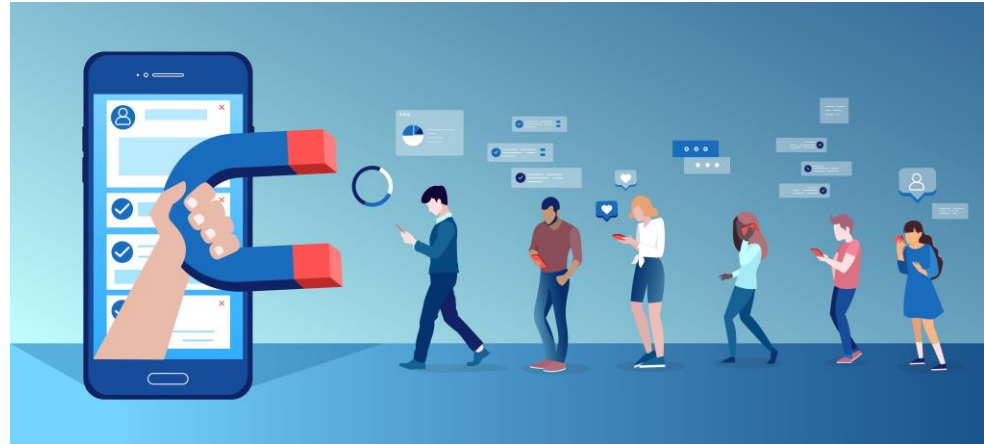
Rules around technology should include:

- where employees can access their devices such as a business laptop away from the workplace
- how to store devices when they aren't in use
- how to report a theft or loss of a work device
- how system updates such as IT patches and spam filter updates will be rolled out to employee devices
- when to physically shut down computers and mobile devices if not in use
- the need to lock screens when computers and devices are left unattended
- how to protect data stored on devices like USB sticks
- restrictions on use of removable devices to prevent malware being installed
- the need to scan all removable devices for viruses before they may be connected to your business systems

6. SET STANDARDS FOR SOCIAL AND INTERNET ACCESS

The standards for social media and internet access may include:

- what is appropriate business information to share on social media channels
- what is appropriate for staff to sign when using their work email account
- guidelines around which websites and social media channels are appropriate to access during work hours



7. PREPARE FOR AN INCIDENT

If a cyber security incident occurs, you should minimize the impact and get back to business as soon as possible. You'll need to consider:

- how to respond to a cyber incident
- what actions to take
- staff roles and responsibilities for dealing with a cyber attack



PREPARE A CYBER SECURITY INCIDENT RESPONSE PLAN

Prepare and prevent

- Prepare your business and employees to be ready to handle cyber incidents.
- Develop policies and procedures to help employees understand how to prevent an attack and to identify potential incidents.
- Identify the assets that are important to your business – financial, information and technology assets.
- Consider the risks to these and the steps you need to take to reduce the effects of an incident.
- Create roles and responsibilities so everyone knows who to report to if an incident occurs, and what to do next.

PREPARE A CYBER SECURITY INCIDENT RESPONSE PLAN

Check and detect

Check and identify any unusual activities that may damage your business information and systems.
Unusual activity may include:

- accounts and your network not accessible
- passwords no longer working
- data is missing or altered
- your hard drive runs out of space
- your computer keeps crashing
- your customers receive spam from your business account
- you receive numerous pop-up ads

PREPARE A CYBER SECURITY INCIDENT RESPONSE PLAN

Identify and assess

- Find the initial cause of the incident and assess the impact so you can contain it quickly.
- Determine the impact the incident has had on your business.
- Determine its effects on your business and assets if not immediately contained.



PREPARE A CYBER SECURITY INCIDENT RESPONSE PLAN

Respond

- Limit further damage of the cyber incident by isolating the affected systems. If necessary, disconnect from the network and turn off your computer to stop the threat from spreading.
- Remove the threat.
- Recover from the incident by repairing and restoring your systems to business as usual.



PREPARE A CYBER SECURITY INCIDENT RESPONSE PLAN

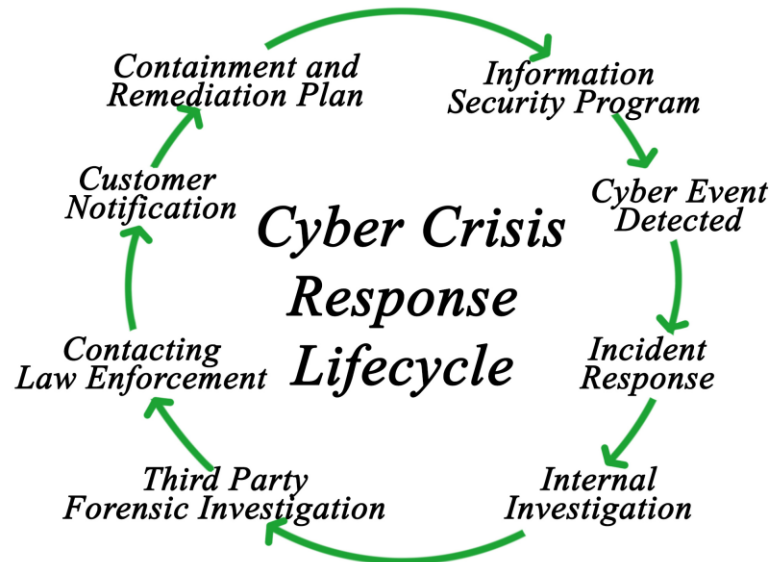
Review

- Identify if any systems and processes need improving and make those changes.
- Evaluate the incident before and after, and any lessons learnt.
- Update your cyber security incident response plan based on the lessons learnt so you can improve your business response.



8. KEEP YOUR POLICY UP-TO-DATE

You should develop, review and maintain your cyber security policy on a regular basis.



LET'S LOOK AT SOME CASE STUDIES FROM:

- Uber
- Target
- SolarWinds

STEP 1:

DON'T PANIC



A cyber attack can certainly be classified as a disaster scenario, and a clear mind is needed to navigate a solution. Once you and your team adopt a problem-solving attitude, you will be able to respond to the breach in a logical and organized way.

Call Inceptus at (239) 673-8130 for any assistance.

STEP 2:

DO NOT PAY A RANSOM



If a cyber attacker demands a ransom, it may be tempting and easier to pay it to regain control of your network, but often times, it may lead to future attacks.

Only pay a ransom if there is no other way to recover your data. A much easier solution is to invest in an Endpoint Detection and Response solution that can stop ransomware before it can be executed.

STEP 4:

USE BACKUP SERVERS



If you have backup servers available and undamaged from the attack, switch to them immediately. The biggest reason this step fails is that organizations fail to test their data restoration process.

If your organization does not have backup servers, avoid the temptation to switch off your servers and workstations. While this may seem to be a viable solution, it will not help to fix the damage.

STEP 3:

FORM A RESPONSE TEAM



To address any damage caused by the cyber attack, you will need a capable and experienced response team. Your team should be comprised of IT staff members, either contracted or in-house, who will investigate the attack and work to resolve it. HR should be included if your employees have been impacted by the attack. Public Relations representatives should be included to best explain the attack to your customers. Always include legal counsel since breaches can have a number of legal implications.

STEP 5:

ISOLATE THE BREACH



If your organization is hit with a cyber breach, it is imperative that you minimize the number of affected systems. You will need to isolate where the breach occurred and stop it from infecting other systems. Once the breach has been suspended, your response team can test other portions of the network to see if they have been compromised as well.

STEP 6:

INVESTIGATE & MANAGE



Upon investigation, you may find that the damage affects numerous portions of your organization. HR, response team members will need to be address any impact on your employees. If your customers or the public were affected, PR staff will need to control the damage done to your reputation. The attack may even cause legal ramifications, and as such your business's lawyers may need to be involved.

STEP 8:

CONTACT CLIENTS



The PR members on your response team need to reach out to all clients who have been impacted by the breach as soon as possible. For security purposes, your clients may need to change their passwords or PIN numbers if their private information was compromised.

STEP 7:

DOCUMENT



As your response team is investigating the attack, ensure that they are documenting both their process and their findings. From this evidence, you will be able to ascertain the vulnerability that allowed the attack to be successful, and thus fortify it going forward.

STEP 9:

PREVENT FUTURE ATTACKS



If your team is unable to effectively secure your organization's IT, you may need to partner with an outside cyber security company. Outsourcing your cyber security needs to an Managed Security Services Provider (MSSP) can be cheaper and they are often more effective than most IT teams.

IMPORTANT CONTACT INFORMATION

INCEPTUS	(239) 673-8130 soc@inceptussecure.com	Help with remediation efforts
IT CONTACT		Help with remediation
LEGAL COUNSEL		Help with breach notification and reporting
PR CONTACT		Help with client notification
HR CONTACT		Help with employee
LOCAL LAW ENFORCEMENT		May be required for insurance claims
FBI FIELD OFFICE	http://www.fbi.gov/	Report any Cyber

PRIVACY ISSUES IN THE MODERN ERA

Internet Privacy Issues: Tracking, Hacking and Trading



1. SPYING AND SNOOPING

- When you are online, you are spied by a number of trackers for various purposes.
- Trackers keep a record of your search history and track all your online activities through various means. This provides them a clear picture of who you are and your interests, which is a breach of online privacy policy and makes you a public property.
- Most of the time, this tracking is for advertisement purposes only and it allows advertisers to show ads according to your taste and interests.
- Sometimes this information is used by cybercriminals to carry out unauthorized and illegal activities risking your online existence.

2. INFORMATION MISHANDLING

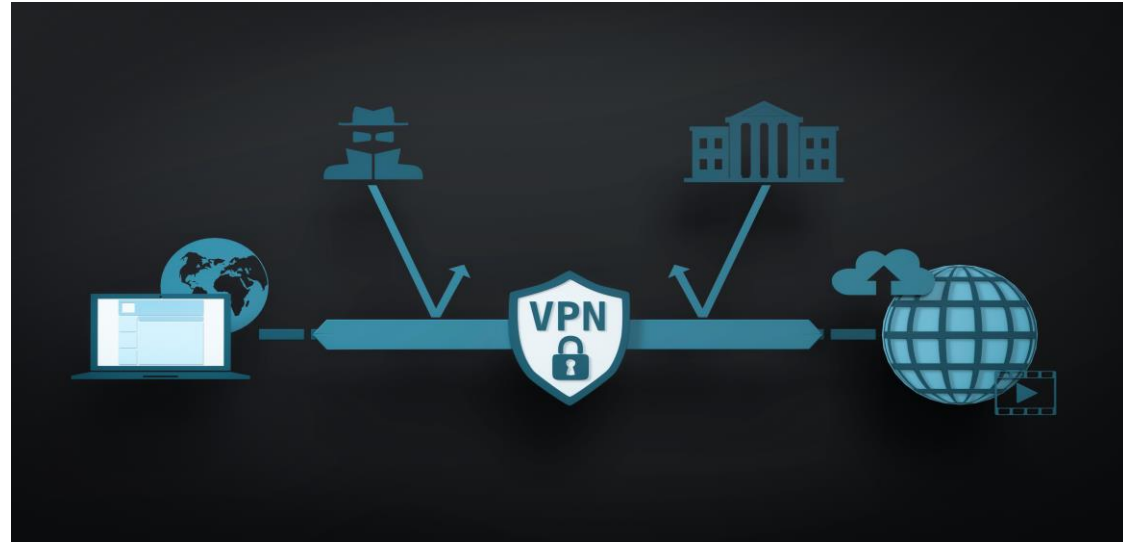
- There are various sites on the internet that need your personal information to get access to their services.
- These sites often store cookies and save your personal information and later use it for various purposes. Most of the time this information is not encrypted and can be accessed by anyone.
- This mishandling of personal information may lead to serious consequences.
- The modern trend of e-banking and e-business portals have multiplied the risks associated with online privacy. By sharing your bank details and crucial files on the internet, you are paving ways for burglars and making yourself vulnerable to cybercriminals.

3. LOCATION TRACKING

- Most of internet users proudly upload their social media posts highlighting their current location along with tagging friends and family members.
- It's fun and exciting to share your life events with friends and family, but this data does not remain restricted to your expected audience only.
- This same data is stored on the social media site you are using and stays there forever, often without you knowing (though you may have given consent through a terms and services agreement).
- Along with social media apps, Google Maps and other apps also ask for your location and by turning on your location you are providing first-hand information to the world about where exactly you are and what your next move is, which is certainly risky and insecure.

4. WAYS TO PROTECT AGAINST ONLINE PRIVACY THREATS

- Use a VPN
- Conduct Safe Browsing
- Keep Your System Up-to-Date
- Use Anti-Virus
- Adjust Your Settings on Social Media
- Keep social media posts to a minimum
- Use cloud services for day to day work



CLOUD SECURITY AND MALWARE

An overview of cloud security



WHY IS CLOUD SECURITY IMPORTANT?

As companies continue to migrate to the cloud, understanding the security requirements for keeping data safe has become critical.

While third-party cloud computing providers may take on the management of this infrastructure, the responsibility of data asset security and accountability doesn't necessarily shift along with it.



WHAT ARE SOME CLOUD SECURITY CHALLENGES?

- **Lack of visibility**

It's easy to lose track of how your data is being accessed and by whom, since many cloud services are accessed outside of corporate networks and through third parties.

- **Multitenancy**

Public cloud environments house multiple client infrastructures under the same umbrella, so it's possible your hosted services can get compromised by malicious attackers as collateral damage when targeting other businesses.

- **Access management and shadow IT**

While enterprises may be able to successfully manage and restrict access points across on-premises systems, administering these same levels of restrictions can be challenging in cloud environments. This can be dangerous for organizations that don't deploy bring-your-own device (BYOD) policies and allow unfiltered access to cloud services from any device or geolocation.

- **Compliance**

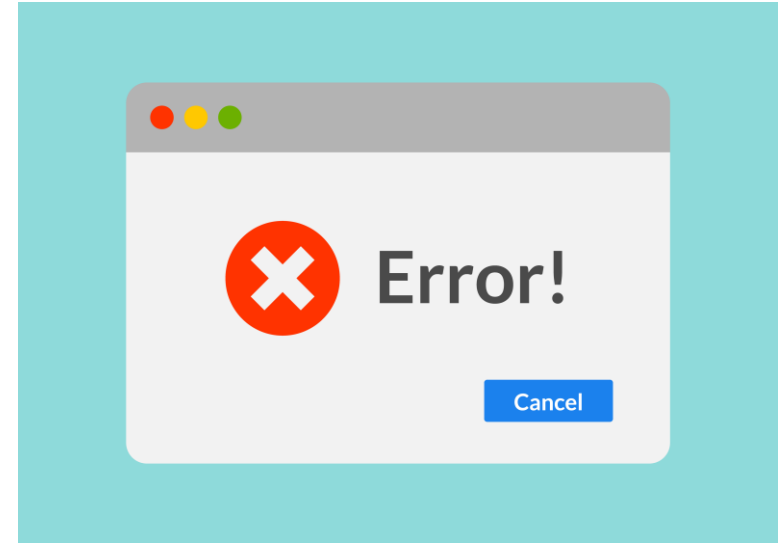
Regulatory compliance management is oftentimes a source of confusion for enterprises using public or hybrid cloud deployments. Overall accountability for data privacy and security still rests with the enterprise, and heavy reliance on third-party solutions to manage this component can lead to costly compliance issues.

WHAT ARE SOME CLOUD SECURITY CHALLENGES?

Misconfigurations

Misconfigured assets accounted for 86% of breached records in 2019, making the inadvertent insider a key issue for cloud computing environments.

Misconfigurations can include leaving default administrative passwords in place, or not creating appropriate privacy settings.



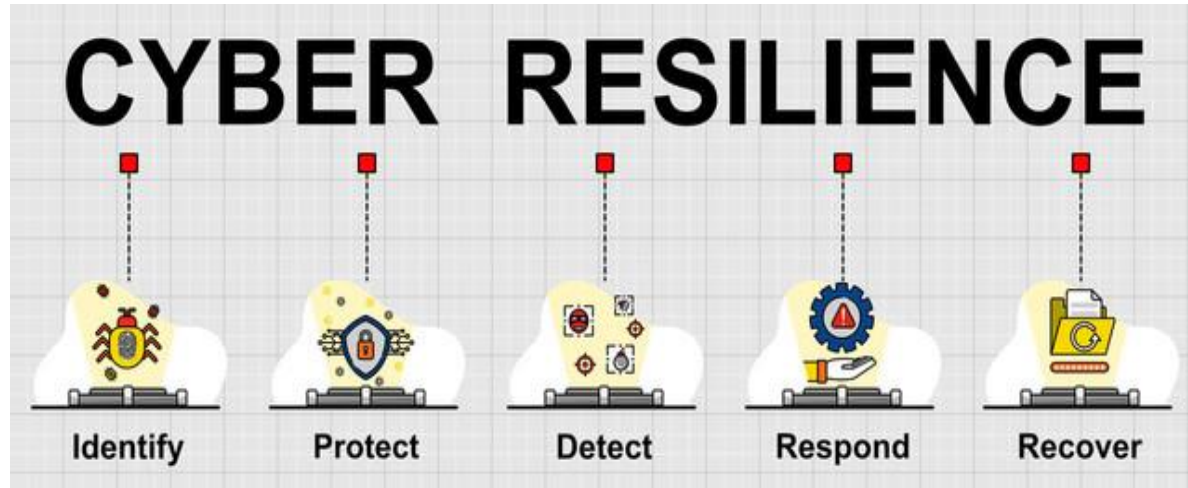
WHAT TYPES OF CLOUD SECURITY SOLUTIONS ARE AVAILABLE?

- Identity and access management (IAM)
- Data loss prevention (DLP)
- Security information and event management (SIEM)
- Business continuity and disaster recovery
- Public key infrastructure (PKI):
- Implementing two-factor authentication



HOW SHOULD YOU APPROACH CLOUD SECURITY?

- The NIST has created necessary steps for every organization to self-assess their security preparedness and apply adequate preventative and recovery security measures to their systems.
- These principles are built on the NIST's five pillars of a cybersecurity framework: **Identify, Protect, Detect, Respond, and Recover.**



IN WHAT WAYS CAN MALWARE ENTER THE CLOUD?

- There's a lot of reasons to think the cloud is more secure than on-prem servers, from better data durability to more consistent patch management — but even so, there are many threats to cloud security businesses should address. Cloud-based malware is one of them.
- Malware delivered through cloud storage apps such as Microsoft OneDrive, Google Drive, and Box accounted for 69% of cloud malware downloads

FOUR BEST PRACTICES TO PREVENT CLOUD-BASED MALWARE

1. Fix the holes in your cloud security

Fixing the holes in your cloud security should be considered one of your first lines of defence against cloud-based malware. Here are three best practices:

- Have strong identity and access management (IAM) policies:
- Properly configure your public APIs:
- Set up your cloud storage correctly:

FOUR BEST PRACTICES TO PREVENT CLOUD-BASED MALWARE

2. Protect your endpoints to detect and remediate malware before it can enter the cloud

At any time, any one of these hundreds of endpoints can become infected with malware. And if you can't detect and remediate the malware as soon as an endpoint gets infected, there's a chance it can sync to OneDrive — where it can infect more files.

Three features of endpoint detection and response that can help track and get rid of malware:

- Suspicious activity monitoring:
- Attack isolation
- Incident response



FOUR BEST PRACTICES TO PREVENT CLOUD-BASED MALWARE

3. Use a second-opinion cloud storage scanner to detect cloud-based malware

Even if you have fixed all the holes in your cloud security and use a top-notch EDR product, the reality is that malware can still make it through to the cloud — and that's why regular cloud storage scanning is so important.

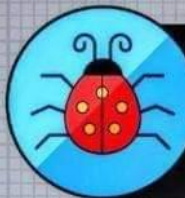


FOUR BEST PRACTICES TO PREVENT CLOUD-BASED MALWARE

4. Have a data backup strategy in place

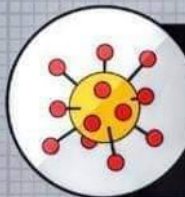
- The worst case scenario: You've properly configured your cloud, secured all your endpoints, and regularly scan your cloud storage — yet cloud-based malware still manages to slip past your defenses and encrypt all your files.
- You should have a data backup strategy in place for exactly this kind of ransomware scenario.
- When it comes to ransomware attacks in the cloud — which can cause businesses to lose critical or sensitive data — a data backup strategy is your best chance at recovering the lost files.

Types of Malware



BUGS

A type of error, flaw or failure that produces an undesirable or unexpected result. Bugs typically exist in a website's source code and can cause a wide range of damage.



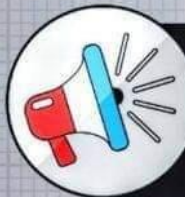
VIRUS

A piece of code that is loaded onto your website or computer without your knowledge. It can easily multiply and be transmitted as an attachment or file.



TROJAN HORSES

Much like the myth, a Trojan disguises itself as a normal file and tricks users into downloading it, consequently installing malware.



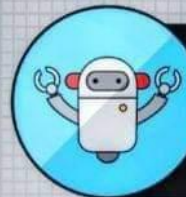
ADWARE

A type of malware that automatically displays unwanted advertisements. Clicking on one of these ads could redirect you to a malicious site.



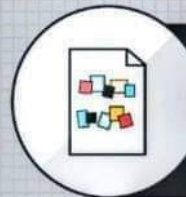
WORMS

A worm relies on security failures to replicate and spread itself to other computers. They are often hidden in attachments and will consume bandwidth and overload a web server.



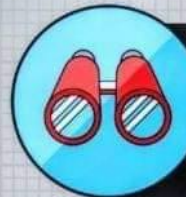
BOTS

A software program created to perform specific tasks. Bots can send spam or be used in a DDoS attack to bring down an entire website.



RANSOMWARE

Ransomware denies access to your files and demands payment, through Bitcoin in order for access to be granted again.



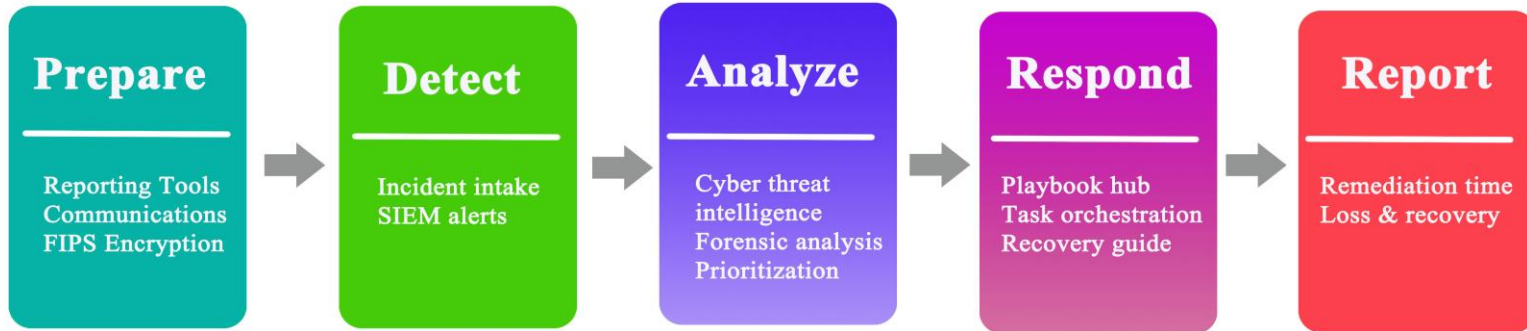
SPYWARE

A type of malware that functions by spying on a user's activity. This type of spying includes monitoring a user's activity, keystrokes and more.

THREAT INTELLIGENCE

Threat intelligence is data that is collected, processed, and analyzed to understand a threat actor's motives, targets, and attack behaviors

Protection from Cyber Threat



THREAT INTELLIGENCE

- In order to provide effective protection from cyber attacks, the techniques and methods of attack must first be understood. Cyber Threat Intelligence caters to this crucial objective: relevance of lines of defense. Cyber criminal target business operations and IT systems, so it is therefore very important to maintain a level of knowledge of such threats to adapt the detection of each of our customers.
- Cyber Threat Intelligence provides means to collect, analyze and then sort all of the data related to a cyber attack, the attacker and the procedures used. Taking action as part of a community is one of the major challenges of Cyber Threat Intelligence insofar as it lets each player broaden their knowledge of attacks and protect themselves more effectively.

SECURITY INFORMATION EVENT MANAGEMENT

How does SIEM work?

SIEM works by collecting information from logs and event data generated by an organization across its applications, security systems, and hardware. By matching events against rules and analytics engines, it's possible for SIEM systems to detect and analyze security threats in real time. Better still, everything is indexed for search to help security teams in their analyses, log management, and reporting.



EXAMPLES OF THREATS A SIEM SOLUTION CAN DETECT

- **Unauthorized access**

A handful of failed login attempts is understandable. Dial that number up to 100 and someone is probably performing a brute force attack. SIEM software can monitor user behavior and identify unusual access attempts.

- **Insider threats**

By constantly monitoring employee behavior, SIEM systems can detect insider threats both accidental and malicious. From former employees, who have yet to have their access privileges revoked, to malicious insiders, who may be trying to steal or leak sensitive information, to accidental security changes, SIEM software can detect anomalous behavior and escalate it to a security analyst for analysis.

EXAMPLES OF THREATS A SIEM SOLUTION CAN DETECT

- **Phishing**

Phishing attacks are designed to get people to voluntarily divulge personal or sensitive information by impersonating a trusted authority.

- **DoS and DDoS attacks**

Denial-of-service (DoS) attacks disrupt services by flooding networks with enough traffic to tie up system resources and trigger a crash.

- **Code injection**

Code injection involves injecting malicious code into client-side input channels, such as online forms, to gain access to an application's database or systems.

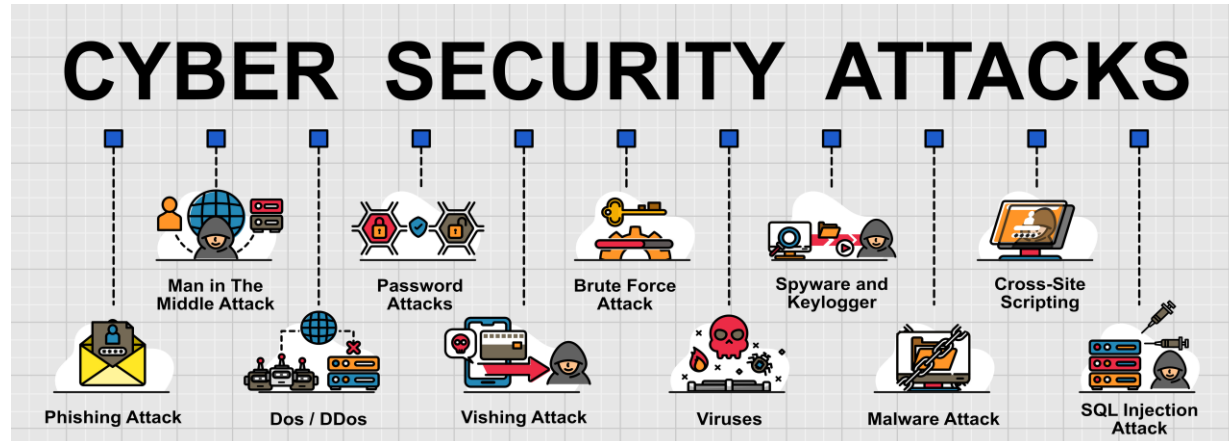
EXAMPLES OF THREATS A SIEM SOLUTION CAN DETECT

- Ransomware and other malware**

Ransomware, viruses, worms, trojans, and other types of malware are software designed to infiltrate computer systems and execute malicious programs.

- MITM attacks**

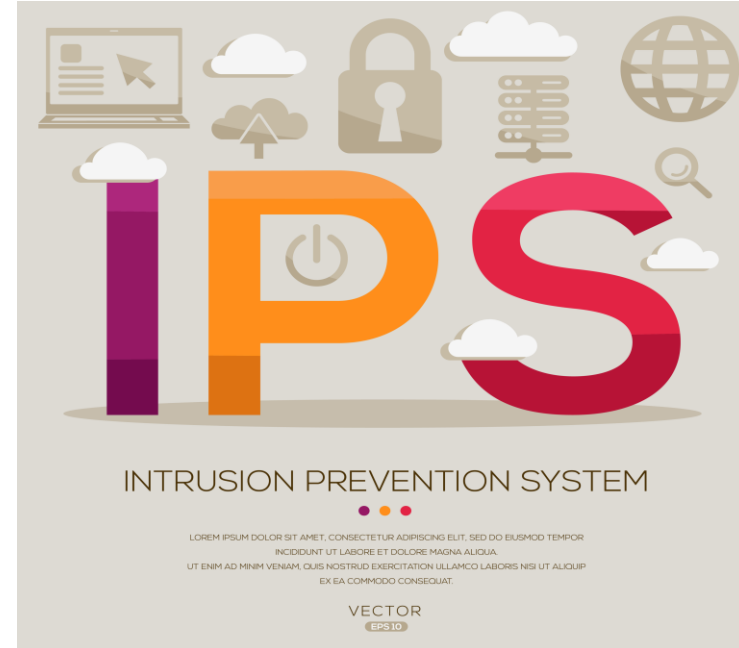
A man-in-the-middle (MITM) attack is when a malicious third party eavesdrops on communications between two hosts to steal or manipulate information.



COMMON SIEM CYBERSECURITY VENDORS








Some popular SIEM tools on the market include:

- Elastic SIEM
- SolarWinds SIEM
- Datadog
- Splunk Enterprise SIEM
- McAfee ESM
- Micro Focus ArcSight
- LogRhythm
- AT&T Cybersecurity SIEM (Formerly AlienVault USM)
- RSA NetWitness
- Netsurion EventTracker



FIREWALLS

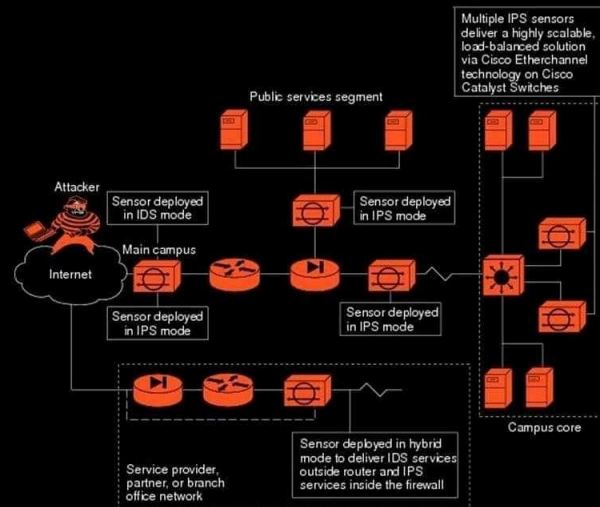
Save this post to remember
the types of firewall

	Proxy firewall	An early type of device, serves as the gateway from one network to another for a specific application
	Stateful inspection firewall	Now thought of as a "traditional", allows or blocks traffic based on state, port, and protocol
	Unified threat management (UTM) firewall	Typically combines the functions of a stateful inspection firewall with intrusion prevention and antivirus
	Next-generation firewall (NGFW)	The evolution beyond simple packet filtering and stateful inspection. This blocks advanced malware and application-layer attacks
	Threat-focused NGFW	Includes all the capabilities of a traditional NGFW and also provides advanced threat detection and remediation
	Virtual firewall	Is typically deployed as a virtual appliance in a private or public cloud to monitor and secure traffic across physical and virtual networks
	Cloud Native Firewall	With automated scaling features, enables networking operations and security operations teams to run at agile speeds

IDS Vs IPS

Most organizations have either an IDS or an IPS, and many have both as part of their security information and event management framework.

	IDS	IPS
NAME	Intrusion detection system	Intrusion prevention system
DESCRIPTION	A system that monitors network traffic for suspicious activity and alerts users when such activity is discovered.	A system that monitors network traffic and alerts for suspicious activity, like an IDS, but also takes preventative action against suspicious activity.
LOCATION	A host-based intrusion detection system is installed on the client computer. A network-based intrusion detection system resides on the network.	Located between a company's firewall and the rest of its network.
USE	Warns of suspicious activity taking place, but it doesn't prevent it.	Warns of suspicious activity taking place and prevents it.
FALSE POSITIVE	IDS false positives are usually just a minor inconvenience. Although the IDS incorrectly labels legitimate traffic as malicious, it does not prevent the traffic from entering the network.	IPS false positives can be more serious. When an IPS mistakes legitimate traffic for a threat, it stops the legitimate traffic from entering the network, which could impact any part of the organization, not just the IT team.



How to place Sensors correctly for IPS

Top 5 Password Attack Types



Brute Force Attack

A brute force attack is a type of password crack that uses a computer program to generate and try every possible combination of characters until it finds the correct password. This attack is very time-consuming and often requires large amounts of computing power, but it can be successful if the attacker has enough time and resources.

Dictionary Attack

A dictionary attack is a type of password crack that uses a list of words (usually taken from a dictionary) to generate and try possible password combinations. This attack can be successful if the password is a common word or phrase, but it is much less likely to succeed if the password is a random string of characters.



Rainbow Table Attack

A rainbow table attack is a type of password crack that uses a pre-computed table of all possible hashes of all possible passwords (or a subset thereof). This attack can be very effective if the attacker has a copy of the rainbow table, but it is much less likely to succeed if the password is a random string of characters.

Social Engineering Attack

A social engineering attack is a type of password crack that relies on tricking the user into revealing their password. This attack can be successful if the attacker is skilled at deception, but it is much less likely to succeed if the user is aware of the risks.



credential stuffing Attack

A credential stuffing attack is a type of password crack that uses a list of stolen usernames and passwords (usually obtained from an external data breach) to try and gain access to other accounts. This attack can be successful if the user re-uses passwords across multiple accounts, but it is much less likely to succeed if the user has a unique password for each account.

PRACTICAL LAB SETUP












The following slide is the final lab setup for the RMIT Develop a cyber security project:

- It covers setting up a Firewall (pfsense)
- A SIEM tool ELK on Debian 12
- A domain controller with a client joined to the domain.
- A proxy server installed in the environment (cc proxy)
- And an attacking computer to run a few simple attacks.
- The purpose of this setup is to show the students how to set up an environment with the correct tools.

PRACTICAL LAB SETUP

- The students build the lab throughout the course then are asked to rebuild it again over 5 weeks and explain what they have done.
- For the Blue teaming
- The students will set up a firewall with an IPS (SNORT) and see it work.
- The students then promote a Windows server to a domain controller and join a computer to the domain then install a proxy server (cc proxy) onto the domain.
- The students then set up the SIEM tool in Debian and send the log files from the server to the ELK stack using a tool called winlogbeat.
- Once all of this is done some attacks are run to see where the vulnerabilities may reside within the network.
- This is then discussed as a group.

PRACTICAL LAB SETUP

 pfSense2  Powered Off	
 Debian  Powered Off	
 win10 11  Powered Off	
 svr11  Powered Off	
 kali-linux-2022.3-virtualbox-amd64  Powered Off 	

Firewall

Linux SIEM computer ELK stack

Windows client

Server computer (Domain Controller)

Attacking computer