Systems as Attack Vectors Write-up
Learn how attackers exploit vulnerable and misconfigured systems, and how you can protect them.

Task 1 Introduction

Continue exploring the SOC role in protecting the digital world, now focusing on systems as attack vectors. In this room, you will learn what the systems are, why and how threat groups target them, and what you can do as a SOC analyst to keep your company secure.

Learning Objectives

- Learn the role of a system in a modern digital world
- Explore a variety of real-world attacks targeting systems
- Practice the acquired knowledge in two realistic scenarios

Prerequisites

- Complete the Junior Security Analyst room: https://tryhackme.com/room/jrsecanalystintrouxo
- Complete the Humans as Attack Vectors room: https://tryhackme.com/room/humansattackvectors

Task 2 Definition of System

Imagine a castle again, but now with a trained gatekeeper who knows how to identify phishing and how to combat deepfakes. However, if the lock on the main gate is fragile and cheap, guardian skills do not matter, as the enemy can just sneak into the castle while no one is watching. In cyber terms, threat actors can attack insecure systems directly, without the users' knowledge.

Definition of System

Where do the banks store your cards, or where are your emails stored? The answer - on a system: a physical server, a virtual machine, or a cloud platform like Microsoft 365. Protecting such systems is crucial: if the attackers breach one user's mailbox via phishing, they compromise a single mailbox, but if they breach a mail server, they now control all thousands of mailboxes. Each system type can have a different value for threat actors, for example:

Breached System	Attack Value
A personal laptop of a school student	Steal Steam profile and add the PC to a botnet
A laptop of the bank's senior IT administrator	Get access to the internal banking systems
A mail server of a criminal law company	Dump all mailboxes and blackmail the victim
A server at the heart of an industrial	Encrypt the whole network with

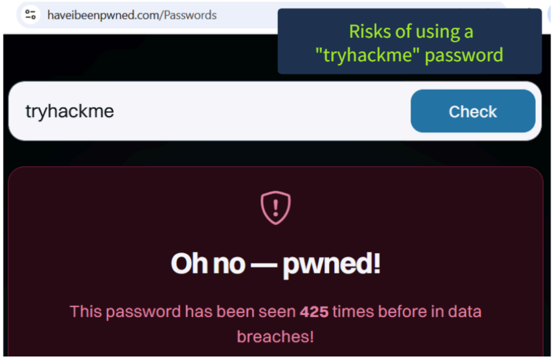
network	ransomware
A government website management panel	Damage the website content (defacement / activism)

Task 3 Attacks on Systems

In most serious attacks, the first goal is to gain access to the target system. What happens next depends on the attacker's motivation: stealing data, deploying ransomware, or even destroying information without a way to recover. However, nearly all attacks begin the same way. Let's look at three examples of how systems are attacked.

Human-Led Attacks

It's no surprise that system users are often those who start the attack: By inserting a malicious USB found on a street, downloading malware from pirated resources, or simply reusing a weak password everywhere. 81% (https://deepstrike.io/blog/password-statistics-2025) of breaches involve stolen or breached passwords - check out your passwords too! (https://haveibeenpwned.com/Passwords)


Risks of using a "tryhackme" password

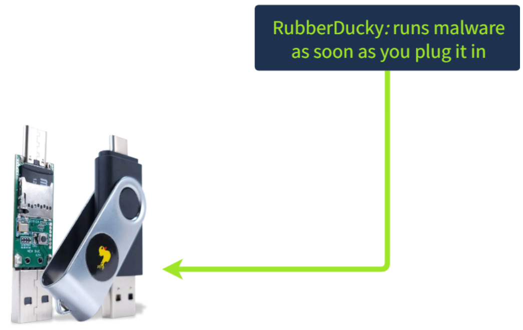
haveibeenpwned.com/Passwords

tryhackme

Check

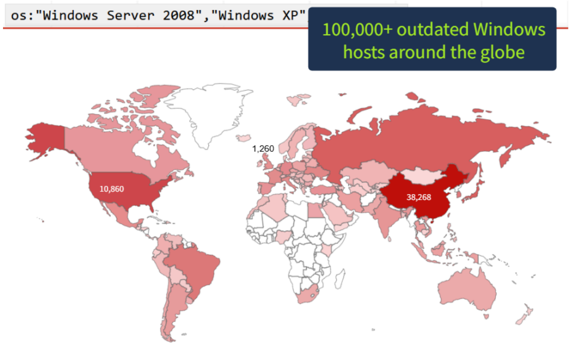
Oh no — pwned!

This password has been seen **425** times before in data breaches!

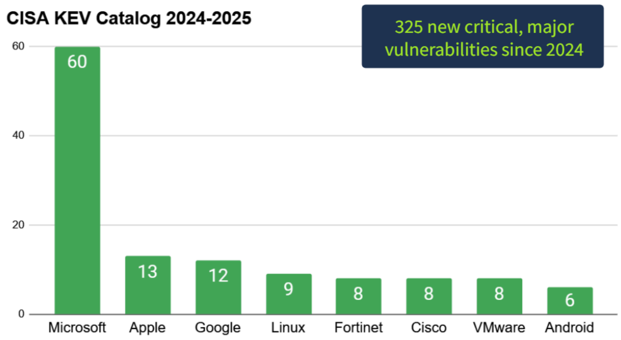

RubberDucky: runs malware as soon as you plug it in

Vulnerabilities

Every piece of software can have security flaws. In 2024, over 40,000: https://cyberpress.org/over-40000-cves-published-in-2024/ software vulnerabilities were published and more than 300: https://www.cisa.gov/known-exploited-vulnerabilities-catalog were actively exploited in major attacks. Moreover, IT administrators often increase the risks by setting weak passwords and allowing unrestricted access to their systems.


os:"Windows Server 2008","Windows XP"

100,000+ outdated Windows hosts around the globe


CISA KEV Catalog 2024-2025

325 new critical, major vulnerabilities since 2024

Supply Chain

Your PC is home to hundreds of apps, including web browsers, messengers, development, and entertainment software. Every app depends on thousands of libraries. If threat actors manage to breach one of the apps or libraries and push an update to all its users, all of them will be compromised. This technique is called a supply chain attack. The most famous examples are the SolarWinds:https://attack.mitre.org/campaigns/C0024/#:~:text=Victims%20of%20this%20campaign%20included%20government and 3CX: https://attack.mitre.org/campaigns/C0024/#:~:text=Victims%20of%20this%20campaign%20included%20government breaches which affected thousands of companies.

Emerging Threat of Supply Chain

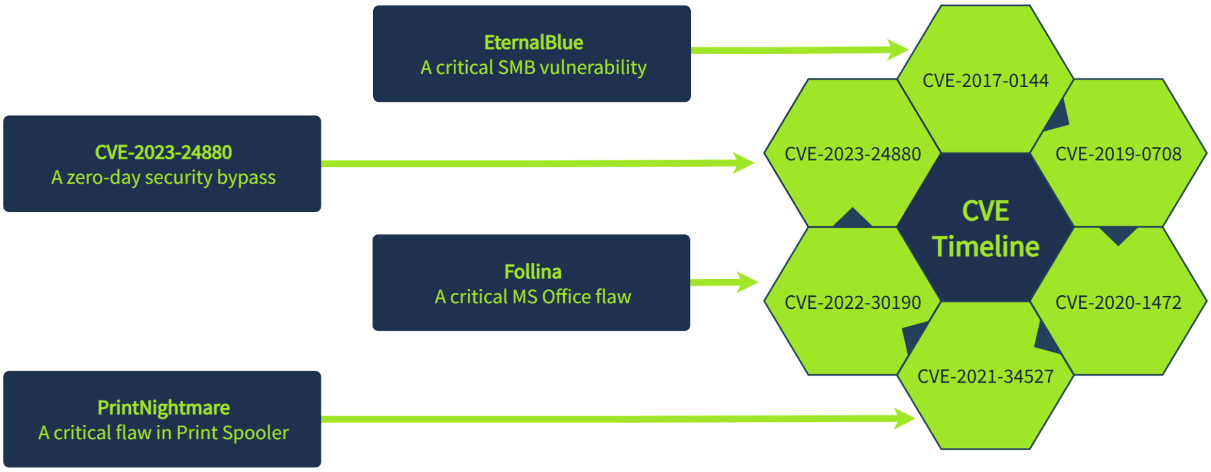
It is hard to protect from supply chain attacks since you can't always control all the software present on your laptops, servers, and web apps. Even TryHackMe once fell victim:https://tryhackme.com/room/supplychainattacks to a supply chain in Lottie Player, a library used for room animations. As a SOC analyst, you must be ready for such scenarios and know how to respond!

What is the term for a security flaw that can be exploited to breach a system?
Answer: Vulnerability

What is the name of the attack when malware comes from a trusted app or library?
Answer: Supply Chain

Task 4 Vulnerabilities
Software Vulnerabilities
Every piece of software has flaws, but some take years to be discovered. For example, Shellshock: https://www.invicti.com/blog/web-security/cve-2014-6271-shellshock-bash-vulnerability-scan, a major Linux vulnerability, existed since 1992 but wasn't found until 2014. In the worst-case scenario, attackers discover the vulnerability before anyone else. This is known as a zero-day:https://en.wikipedia.org/wiki/Zero-day_vulnerability , and only your SOC skills can determine whether it gets detected in time.

Once a vulnerability is made public, it is assigned a Common Vulnerabilities and Exposures (CVE) number. From that moment, it's a race: attackers develop exploits while defenders rush to update their systems. Here is the timeline of how Windows vulnerabilities evolve every year:



Responding to Vulnerabilities
An answer to a CVE is always a **patch** - an update supplied by the software vendor. Even for zero-days, you'll have to wait for a patch, vigilantly monitor for exploitation traces, and try to survive the stressful period before the patch is released. For example, by:

Restricting access to the system to only trusted IPs
Applying temporary measures provided by the vendor
Blocking known attack patterns on IPS or WAF

What is the CVE for the critical SharePoint vulnerability dubbed "ToolShell"?
Answer: CVE-2025-53770

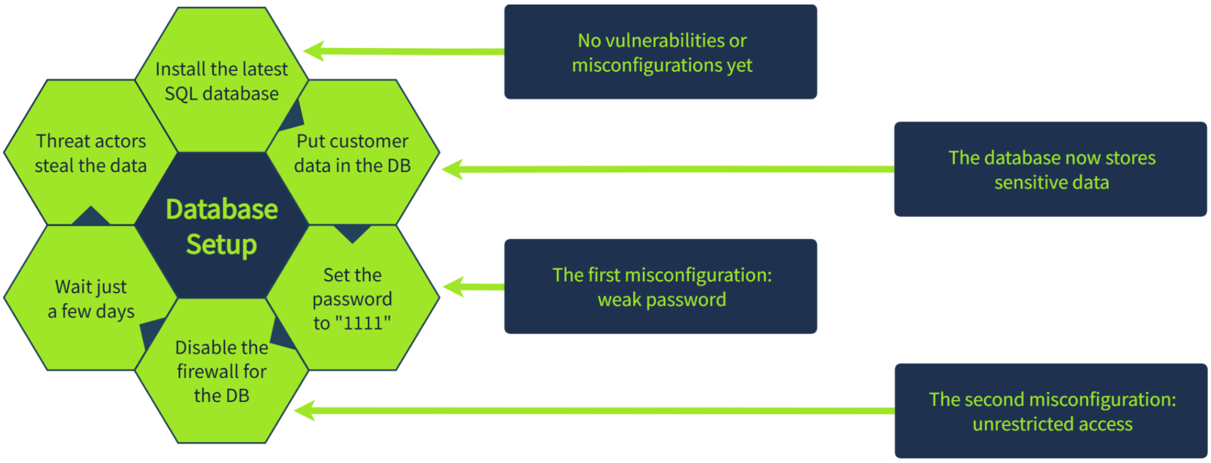
How would you respond to a detected vulnerability on your system?
Answer: Patch

Task 5 Misconfigurations
Misconfigurations
On the other hand, a misconfiguration isn't a bug in the software but a mistake in how the system was set up, often by the IT team. These errors happen frequently, usually to make things simpler, like using "1111" instead of typing a long password every time. Let's take a look at some real-world examples.

- How "123456" password: https://www.bleepingcomputer.com/news/security/123456-password-exposed-chats-for-64-million-mcdonalds-job-chatbot-applications/ exposed chats for 64 million McDonald's job applications
- How a misconfigured AWS cloud: https://www.bleepingcomputer.com/news/security/capital-one-data-breach-affects-106-million-people-suspect-arrested/#:~:text=intrusion%20occurred%20through%20a%20misconfigured%20web%20application%20firewall resulted in a breach of 106 million bank customers
- How improperly configured smart fridges:https://www.sectigo.com/blog/when-refrigerators-attack-how-cyber-criminals-i

nfect-appliances-and-how-manufacturers-can-stop-them are silently used in full-scale botnet attacks

Another common scenario is when the IT department unknowingly introduces new flaws into secure systems. Below is a simple example of how a critical database can be breached because of the insecure configuration:


Database Setup
Install the latest SQL database
Put customer data in the DB
Set the password to "1111"
Disable the firewall for the DB
Wait just a few days
Threat actors steal the data
No vulnerabilities or misconfigurations yet
The database now stores sensitive data
The first misconfiguration: weak password
The second misconfiguration: unrestricted access

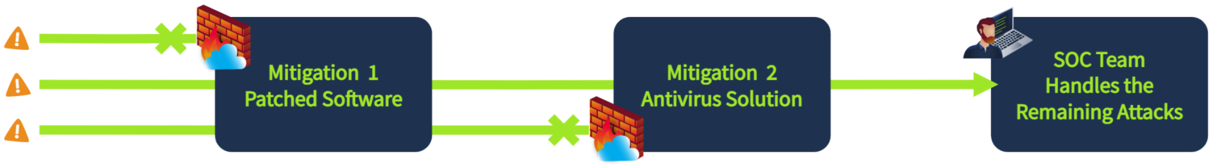
Responding to Misconfigurations
Misconfigurations do not require a software update - just a better setup. As a SOC analyst, you'll often spot them only after threat actors exploit them. However, in smaller companies, you might also be responsible for a more proactive response, for example:

- **Penetration Testing:** Hire ethical "hackers" who simulate an attack and report on discovered security flaws
- **Vulnerability Scans:** Periodically run tools that can detect default passwords or outdated software
- **Configuration Audits:** Manually review the systems to match best practices like CIS benchmarks: https://www.cisecurity.org/cis-benchmarks

Can a system patch or software update fix the misconfigurations (Yea/Nay)?
Answer: Nay

Which activity involves an authorized cyber attack to detect the misconfigurations?
Answer: Penetration Testing

Task 6 Practice
Remember our fortress analogy? Attackers are opportunists. They'll often seek the easiest path, whether through a flaw in the building itself or by manipulating someone to open a door. Attackers don't see "human hacking" and "system hacking" as separate, so you should apply equal effort into protecting both humans and systems, combining **Mitigation** and **Detection**:



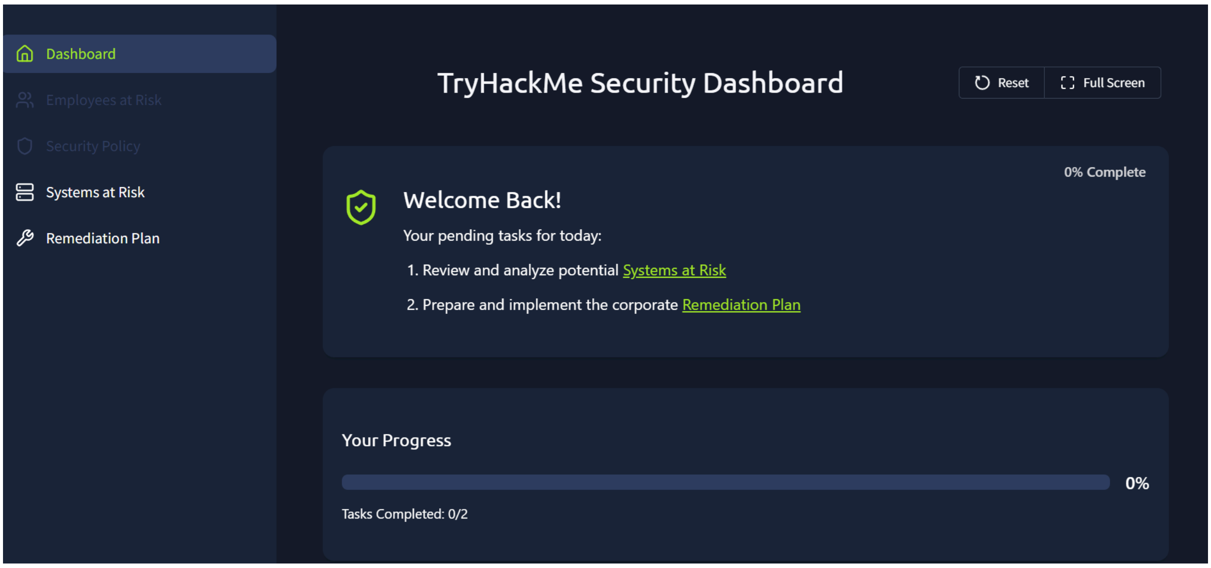
Unlike humans, you can't train the system to spot the attack. However, you can train your IT department to configure the systems and explain how to avoid simple mistakes. Below are the most common mitigation measures to protect your systems:

Mitigation	Description
Patch Management	A process of tracking and patching the vulnerable systems significantly reduces the chance of a successful attack
Training for IT	If your IT knows the risks of misconfigurations, they are less likely to leave the systems unprotected
Network Protection	The system is much harder to breach if access to it is restricted to trusted people or IP addresses
Antivirus Protection	Same as with attacks on humans, a good antivirus can stop or at least detect many different attacks

Practice

View Site: https://static-labs.tryhackme.cloud/apps/soc-systemattacks/

For this lab, continue your SOC analyst journey at TryHackMe. This time, decide what to do with the Systems at Risk and choose the best measures to protect your systems at the Remediation Plan tabs. Open the security dashboard by clicking the View Site button, complete the tasks, and claim the flags to answer the task questions!



TryHackMe Security Dashboard

0% Complete

Welcome Back!

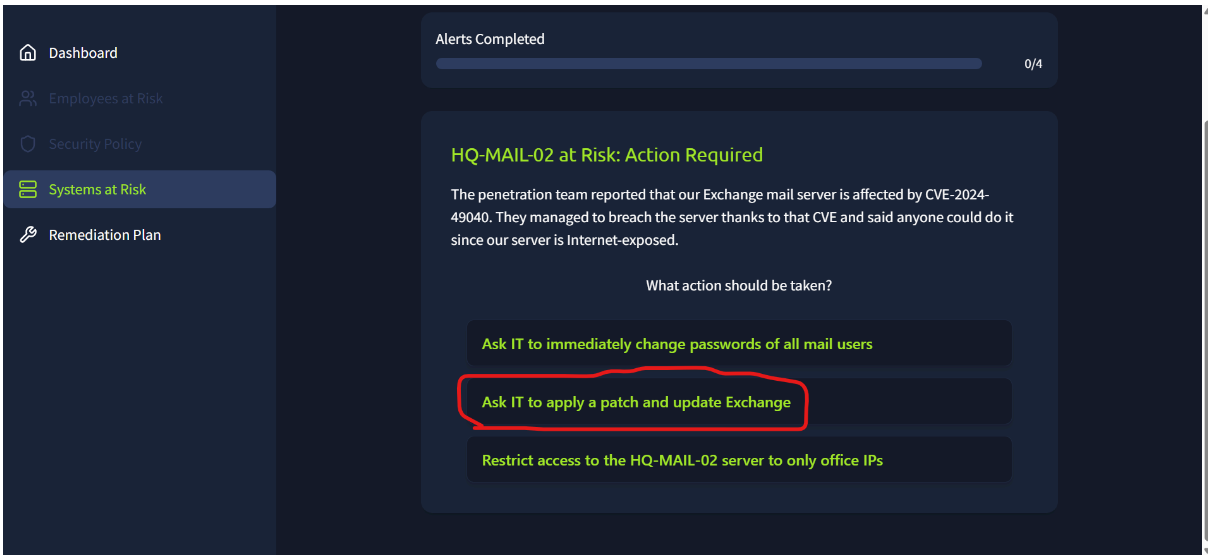
Your pending tasks for today:

1. Review and analyze potential Systems at Risk
2. Prepare and implement the corporate Remediation Plan

Your Progress

0%

Tasks Completed: 0/2



HQ-MAIL-02 at Risk: Action Required

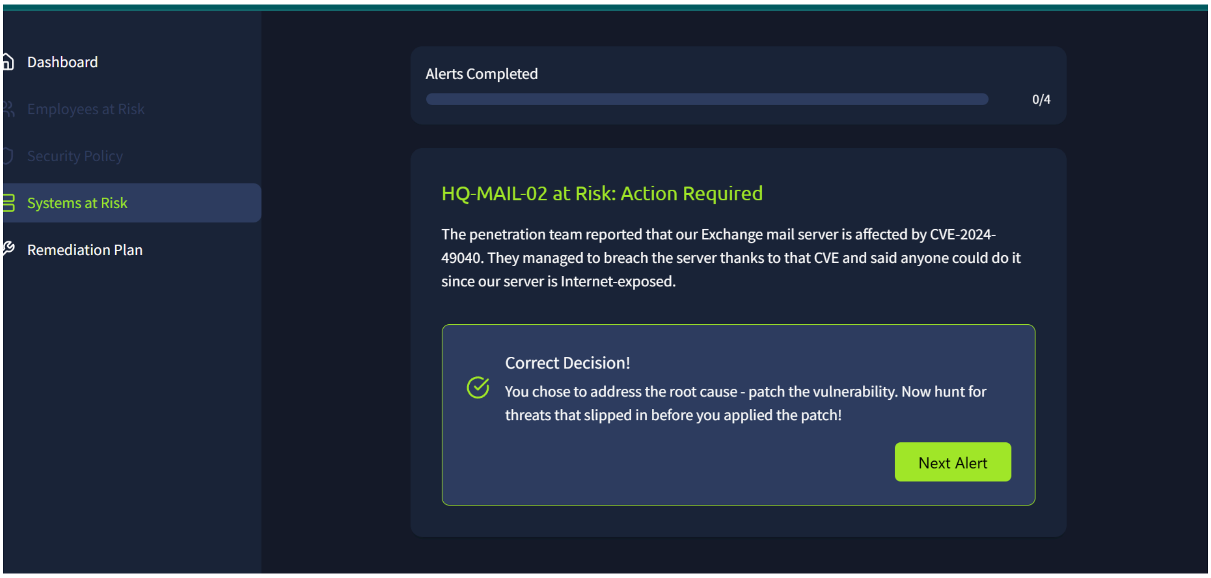
The penetration team reported that our Exchange mail server is affected by CVE-2024-49040. They managed to breach the server thanks to that CVE and said anyone could do it since our server is Internet-exposed.

What action should be taken?

Ask IT to immediately change passwords of all mail users

[✓ Ask IT to apply a patch and update Exchange]

Restrict access to the HQ-MAIL-02 server to only office IPs

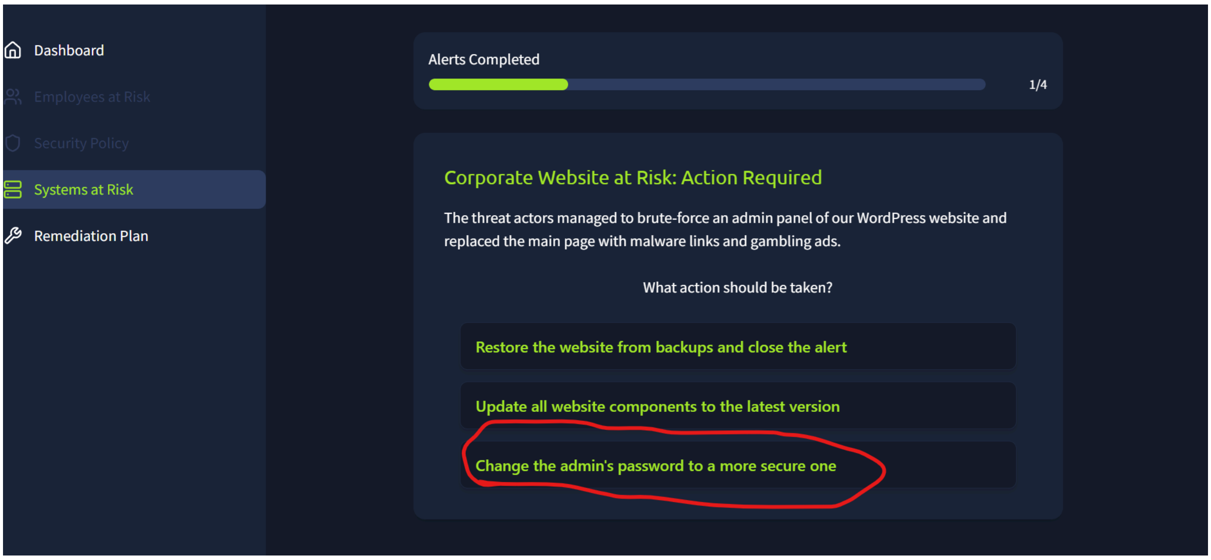


HQ-MAIL-02 at Risk: Action Required

The penetration team reported that our Exchange mail server is affected by CVE-2024-49040. They managed to breach the server thanks to that CVE and said anyone could do it since our server is Internet-exposed.

Correct Decision!

You chose to address the root cause - patch the vulnerability. Now hunt for threats that slipped in before you applied the patch!



Corporate Website at Risk: Action Required

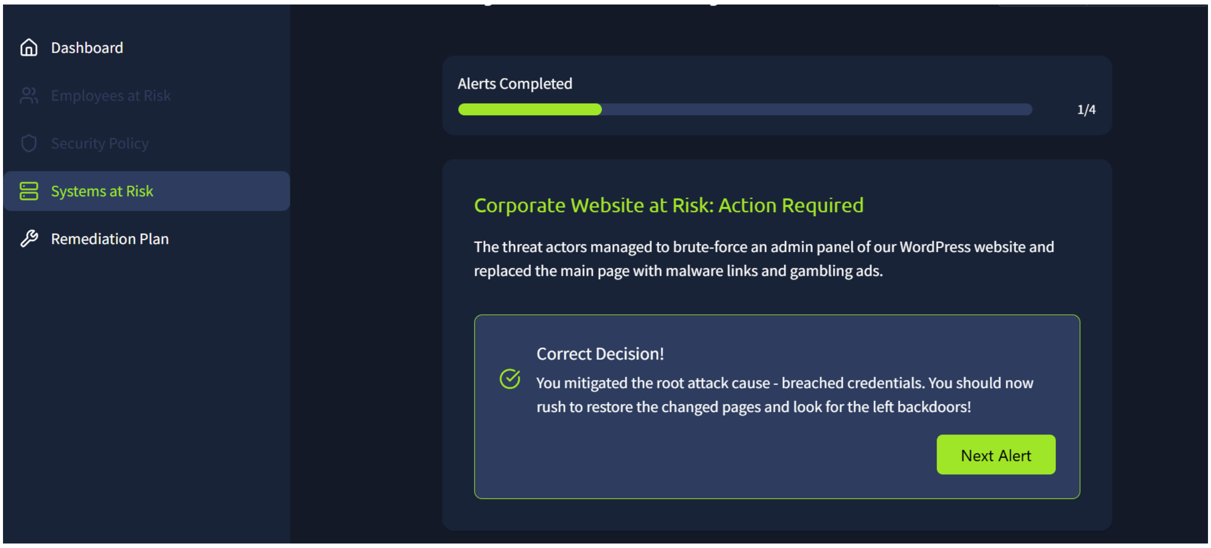
The threat actors managed to brute-force an admin panel of our WordPress website and replaced the main page with malware links and gambling ads.

What action should be taken?

Restore the website from backups and close the alert

Update all website components to the latest version

[✓ Change the admin's password to a more secure one]



Alerts Completed

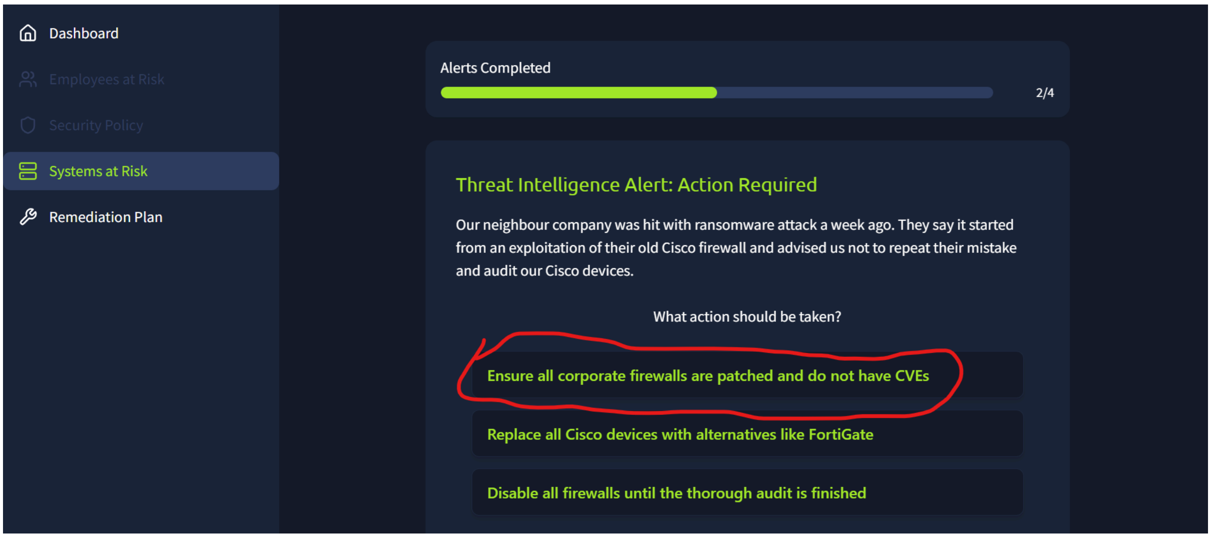
1/4

Corporate Website at Risk: Action Required

The threat actors managed to brute-force an admin panel of our WordPress website and replaced the main page with malware links and gambling ads.

✓ Correct Decision!

You mitigated the root attack cause - breached credentials. You should now rush to restore the changed pages and look for the left backdoors!



Alerts Completed

2/4

Threat Intelligence Alert: Action Required

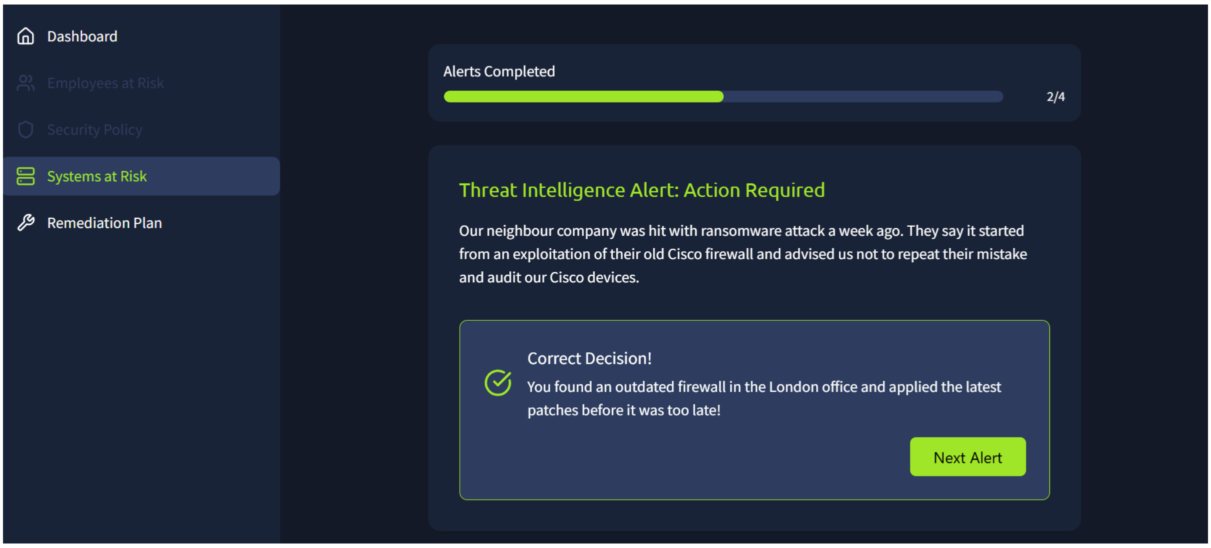
Our neighbour company was hit with ransomware attack a week ago. They say it started from an exploitation of their old Cisco firewall and advised us not to repeat their mistake and audit our Cisco devices.

What action should be taken?

[✓ Ensure all corporate firewalls are patched and do not have CVEs]

Replace all Cisco devices with alternatives like FortiGate

Disable all firewalls until the thorough audit is finished



Alerts Completed

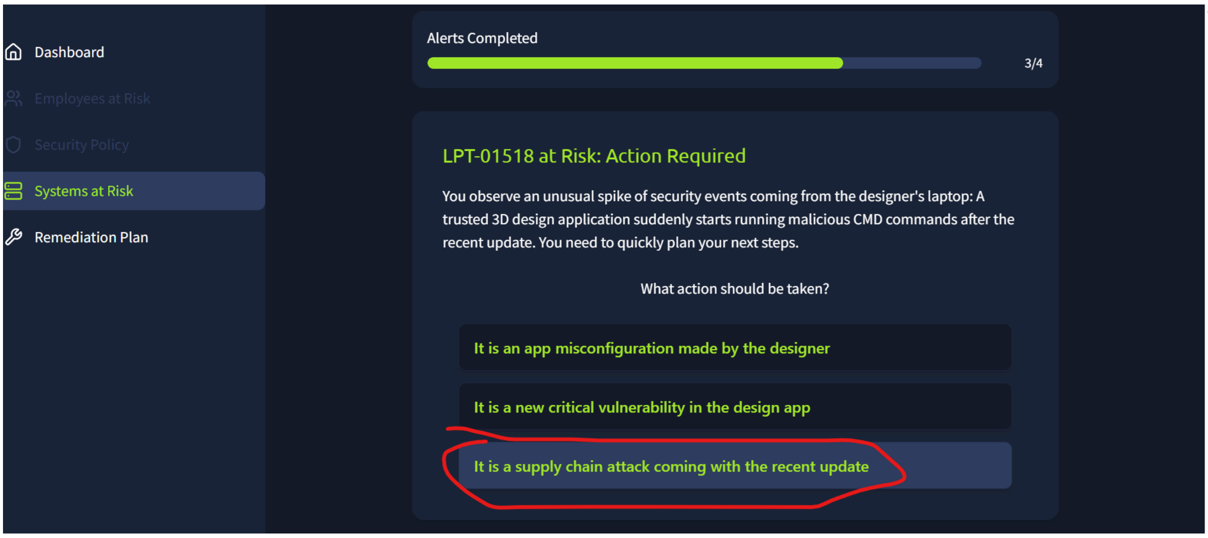
2/4

Threat Intelligence Alert: Action Required

Our neighbour company was hit with ransomware attack a week ago. They say it started from an exploitation of their old Cisco firewall and advised us not to repeat their mistake and audit our Cisco devices.

✓ Correct Decision!

You found an outdated firewall in the London office and applied the latest patches before it was too late!



Alerts Completed

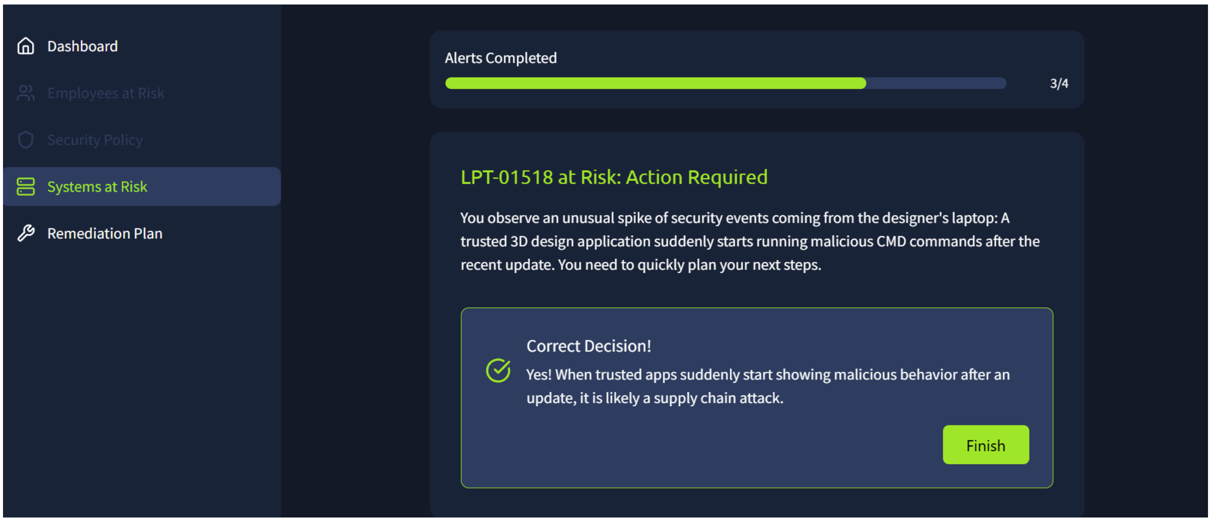
3/4

LPT-01518 at Risk: Action Required

You observe an unusual spike of security events coming from the designer's laptop: A trusted 3D design application suddenly starts running malicious CMD commands after the recent update. You need to quickly plan your next steps.

What action should be taken?

- It is an app misconfiguration made by the designer
- It is a new critical vulnerability in the design app
- [✓ It is a supply chain attack coming with the recent update]



Alerts Completed

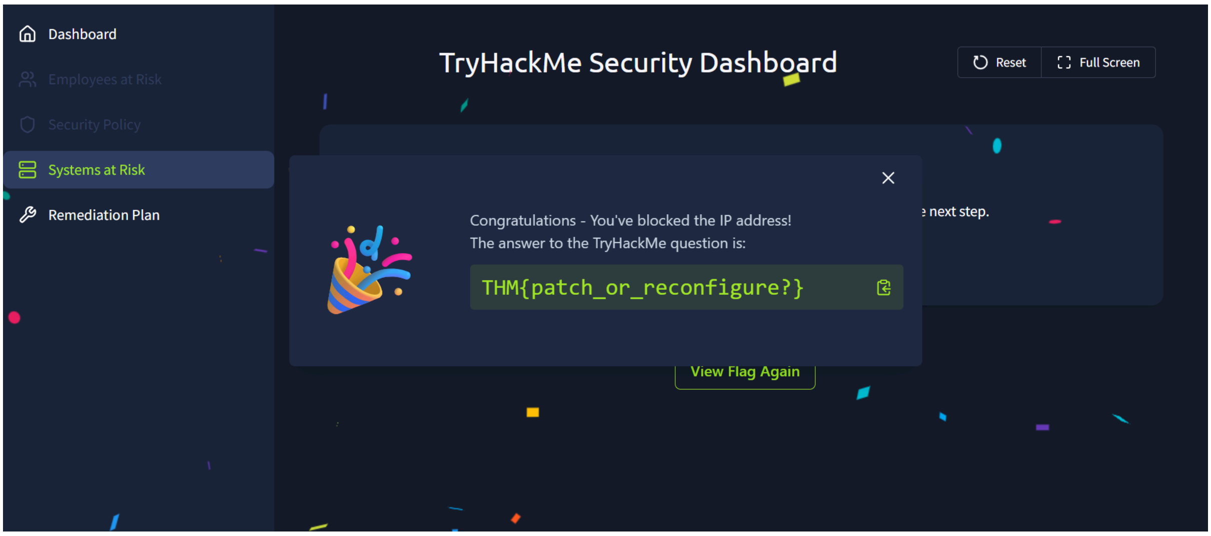
3/4

LPT-01518 at Risk: Action Required

You observe an unusual spike of security events coming from the designer's laptop: A trusted 3D design application suddenly starts running malicious CMD commands after the recent update. You need to quickly plan your next steps.

Correct Decision!

Yes! When trusted apps suddenly start showing malicious behavior after an update, it is likely a supply chain attack.

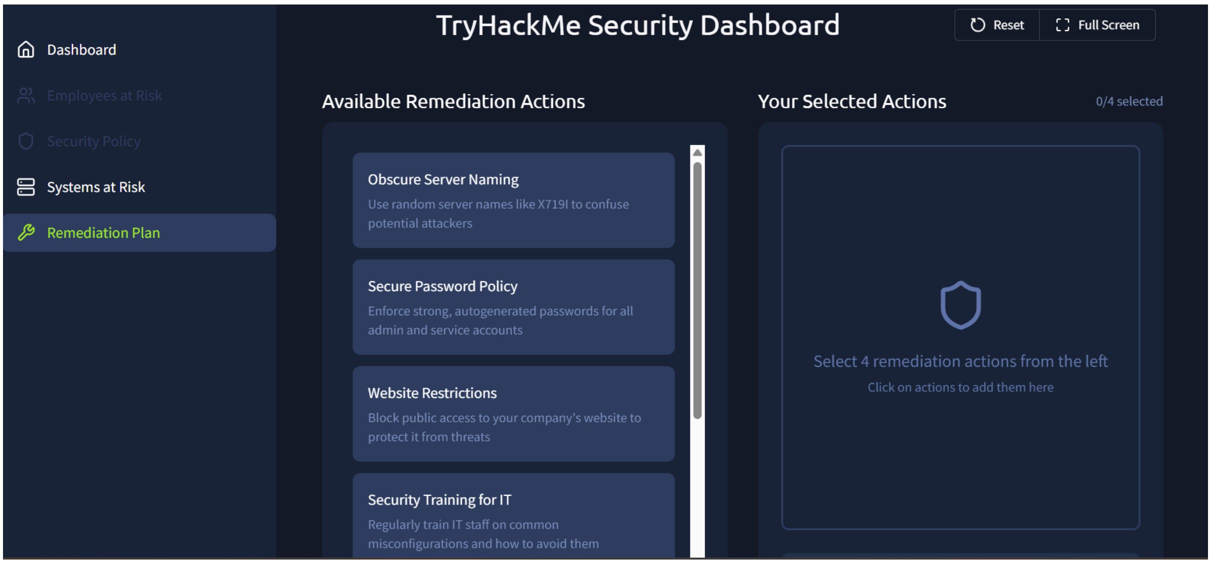


Congratulations - You've blocked the IP address!
The answer to the TryHackMe question is:

THM{patch_or_reconfigure?}

What flag did you receive after completing the "Systems at Risk" challenge?

Answer: THM{patch_or_reconfigure?}



TryHackMe Security Dashboard

Available Remediation Actions

Obscure Server Naming
Use random server names like X719I to confuse potential attackers

Secure Password Policy
Enforce strong, autogenerated passwords for all admin and service accounts

Website Restrictions
Block public access to your company's website to protect it from threats

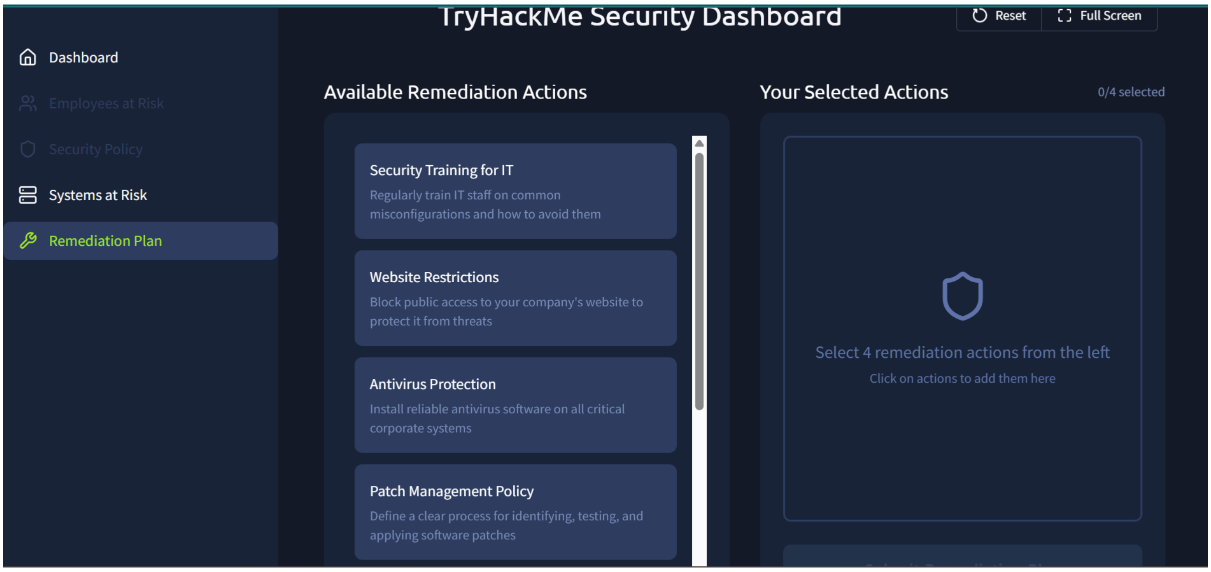
Security Training for IT
Regularly train IT staff on common misconfigurations and how to avoid them

Your Selected Actions

0/4 selected

Select 4 remediation actions from the left

Click on actions to add them here



TryHackMe Security Dashboard

Available Remediation Actions

Security Training for IT
Regularly train IT staff on common misconfigurations and how to avoid them

Website Restrictions
Block public access to your company's website to protect it from threats

Antivirus Protection
Install reliable antivirus software on all critical corporate systems

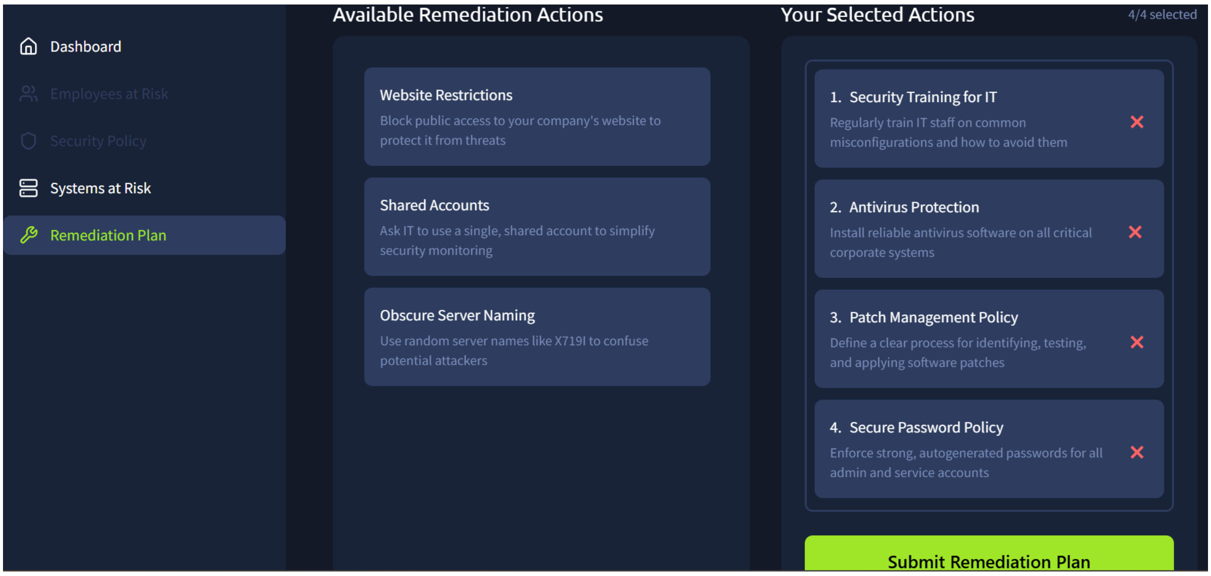
Patch Management Policy
Define a clear process for identifying, testing, and applying software patches

Your Selected Actions

0/4 selected

Select 4 remediation actions from the left

Click on actions to add them here



Available Remediation Actions

Website Restrictions
Block public access to your company's website to protect it from threats

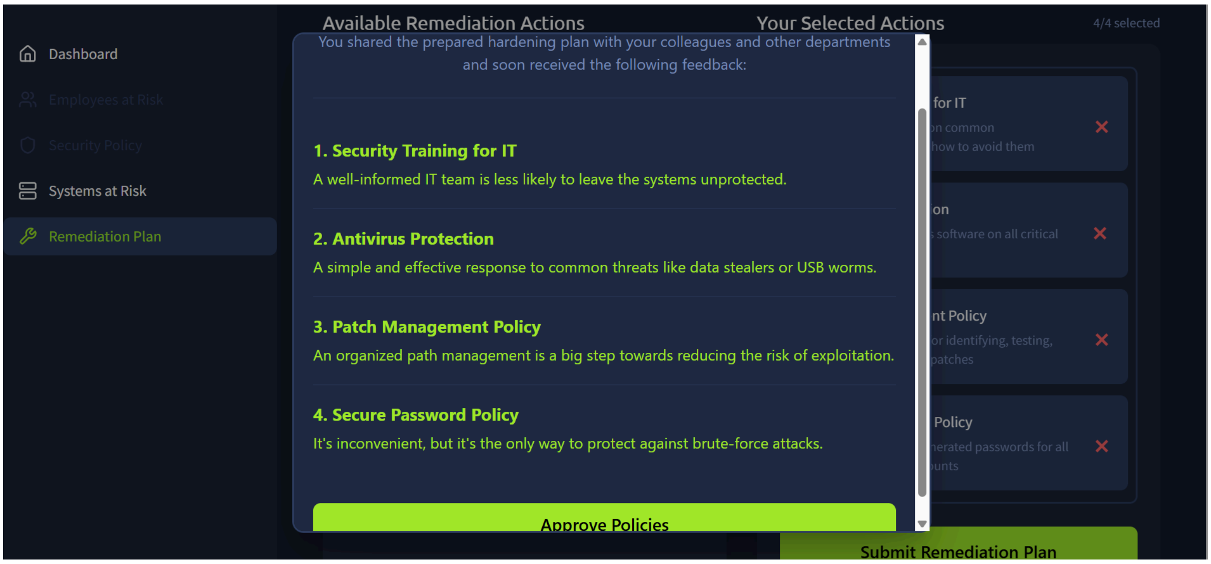
Shared Accounts
Ask IT to use a single, shared account to simplify security monitoring

Obscure Server Naming
Use random server names like X719I to confuse potential attackers

Your Selected Actions

4/4 selected

1. Security Training for IT
   Regularly train IT staff on common misconfigurations and how to avoid them ✕
2. Antivirus Protection
   Install reliable antivirus software on all critical corporate systems ✕
3. Patch Management Policy
   Define a clear process for identifying, testing, and applying software patches ✕
4. Secure Password Policy
   Enforce strong, autogenerated passwords for all admin and service accounts ✕



You shared the prepared hardening plan with your colleagues and other departments and soon received the following feedback:

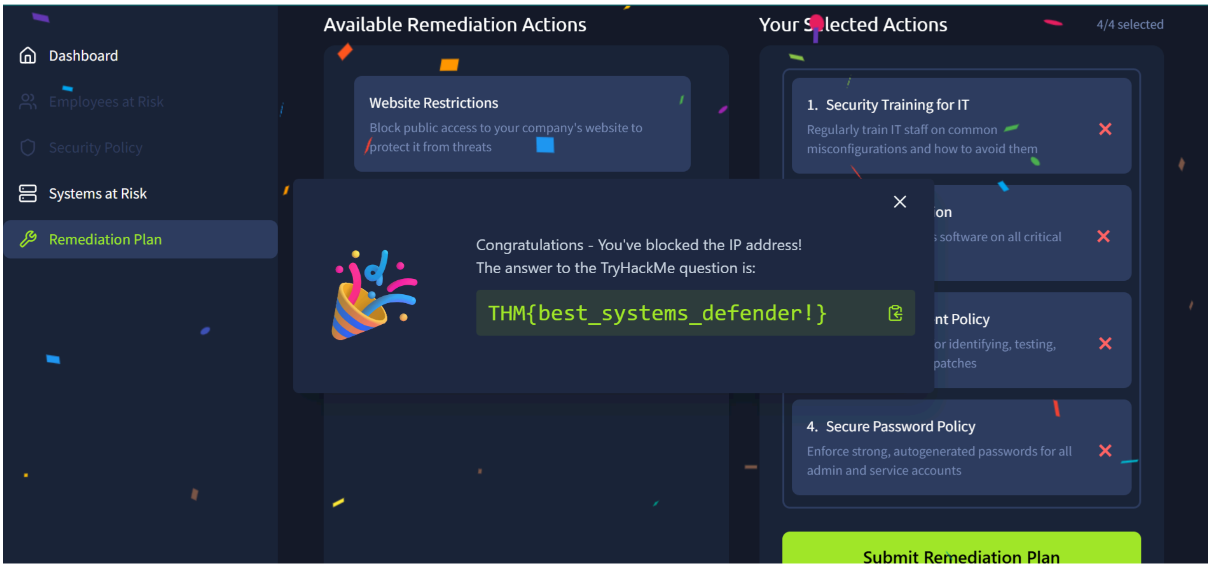
1. Security Training for IT
A well-informed IT team is less likely to leave the systems unprotected.

2. Antivirus Protection
A simple and effective response to common threats like data stealers or USB worms.

3. Patch Management Policy
An organized path management is a big step towards reducing the risk of exploitation.

4. Secure Password Policy
It's inconvenient, but it's the only way to protect against brute-force attacks.

Approve Policies



Website Restrictions
Block public access to your company's website to protect it from threats

1. Security Training for IT
Regularly train IT staff on common misconfigurations and how to avoid them

4. Secure Password Policy
Enforce strong, autogenerated passwords for all admin and service accounts

Congratulations - You've blocked the IP address!
The answer to the TryHackMe question is:

```
THM{best_systems_defender!}
```

What flag did you receive after completing the "Remediation Plan" challenge?
Answer: THM{best_systems_defender!}

Task 7 Conclusion
Even though SOC analysts don't typically manage systems directly, understanding the common attacks and defenses, and sharing them with the IT department, is a key to broadening your cyber security perspective. If you want to grow quickly and be a strong team player, stay updated on the latest threats and always share the news with others!

- The DFIR Report: How Real Intrusions Happen: https://thedfirreport.com/
- CISA: Known Exploited Vulnerabilities Catalog: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- BleepingComputer: Latest Supply Chain Attacks: https://www.bleepingcomputer.com/tag/supply-chain-attack/
- CheckPoint: Interactive Live Cyber Threat Map: https://threatmap.checkpoint.com/