SIEMENS
Ingenuity for life

Mission Briefing

Siemens need your help to catch a cyber criminal who has been interfering with their work. Can you work as a team to find them?

1. Find the security breach

Siemens suspect that a cyber criminal has been trying to log on to their system. You have been given a printed copy of the security log. This is record of security related events such as log-ins and log-outs. The security log is one of the main tools used to detect and investigate unauthorised activity (including attempts).

Your task: Look for strange patterns of user activity on the log. Start by identifying the different types of information included on the log:

+ Date
+ Time
+ User
+ Event name
+ Event info
+ User device

Suspicious activity can be identified by looking for oddities in log data, such as failed log-in attempts or out of hours access.

When did the breach happen?

What device did the cyber criminal use?

Which user was hacked to get access to the system?

2. Confirming the culprit

Siemens has used the information you found about the cyber criminal to identify the user account they used. The cyber criminal left a password protected PDF on the user's device and Siemens need your help to crack the password.

Your task: You have been given a Caesar Cipher Wheel. Siemens staff found a sticky note by the device which said 'Shift 13 CAESARPASSWORD'. Crack the password.

Did you know?

A **Caesar Cipher** is one of the earliest known and simplest codes. Each letter is 'shifted' a certain number of places down the alphabet so that words can't be read. For example, with a shift of 1, A would be replaced by B, B would become C, and so on.

A strong password:

+ Has 12 characters minimum
+ Includes numbers, symbols, capital and lower-case letters
+ Isn't a dictionary word. Avoid obvious dictionary words or any others related to you e.g. where you live

What is the cyber criminal's password?

What was on the PDF document?

3. Secure the evidence

Siemens found some emails sent out during the time of the security breach. They think one or more of them is a phishing email sent by the cyber criminal.

Your task: You have been given copies of emails that Siemens has found. Take a look through them and note down anything suspicious.

Which emails do you think are phishing emails?

Why?

Did you know?

Phishing is a type of social engineering often used to steal user data such as login credentials, personal information or credit card numbers. Typically the phishing is disguised to look more trustworthy, for example using branding from a well known company.

Phishing emails can normally be spotted by looking out for emails that contain:

+ Malicious web or email links
+ Spelling and grammar mistakes
+ Suspicious attachments, and/or a message is designed to make you panic and act quickly
+ Requests for you to confirm personal information

4. Find the criminal's location

Using the information you found, Siemens has been able to find the cyber criminal's name and identity. Now the police need to find the location of the cyber criminal.

Your task: You have been given some clues found on the cyber criminal's social media. Can you use these to find the location of the cyber criminal? Look out for street signs in photos and location tagging in posts.

What is the location of the cyber criminal?

Country:

Town:

Street:

Number:

Dana Tran, Global Industrial Cyber and Digital Security expert at Siemens, initially wanted to become a doctor. Without any formal training or background in cyber technology, Dana took the skills she developed while studying medicine and ventured into the unknown world of start-ups and technology.

"When you're a doctor, you have to find out if things are weak," she says. "It's the same in cybersecurity."

"I didn't realise there's more than one way to help people. Now I'm in a role where I'm helping a broader audience and it helps me put meaning into my job."

Today, Dana's job takes her all over the world, to collaborate and communicate with governments and major organisations—urging them to take cyber-readiness in their own environments seriously. In her experience, lots of infrastructure, factories and nuclear reactors for example,aren't equipped for a large-scale cyber attack.

But despite it being her passion, Dana is only too aware that cybersecurity isn't always an obvious choice. "My brother is in school" she explains, "and none of his computer science friends are thinking about roles in cybersecurity." In addition, women are very under-represented in the field.

Read more about Dana's story at: medium.com/futuremakers

For more resources and activities, visit **siemens.co.uk/education**