Project Research from DATACOM Internship Program

Company: DATACOM

Objectif: A risk-free way to experience work on the job with us at Datacom. Practice your skills with example tasks and build your confidence to ace your applications.

What you'll learn: How Datacom's cybersecurity consultants help evaluate impacts from sophisticated cyberattacks

What you'll do: Investigate a cyber attack and produce a comprehensive report documenting your findings and outline key recommendations for improving a client's cybersecurity posture

TASK 1: APT Breach, analyzing the impact on information security

Here is the background information on your task

Welcome to the fascinating world of cybersecurity! In this task, you will be stepping into the role of a cybersecurity consultant here at Datacom. One of our leading tech corporation clients has fallen prey to a sophisticated cyberattack by a notorious Advanced Persistent Threat (APT) group known as APT34. The attack, believed to be sponsored by a foreign government, has left the organisation's network compromised, and valuable customer data and intellectual property has been stolen.

Your mission is to conduct initial research on this APT group, APT34, and assess the extent of the breach's impact on the organisation's information security. But fear not, for you will be provided with all the necessary tools required to understand cybersecurity concepts and principles, including cyberthreats, attack methods, and the importance of confidentiality, integrity and availability of information. In addition, you will also be familiarised with APT34's tactics, techniques and procedures (TTPs) and the common vulnerabilities they exploit to gain access to networks.

The objective of this task is to help our client conduct an initial investigation into APT34 and evaluate the potential impact of the attack on the organization. As a result, you will need to produce a comprehensive report documenting your findings and outlining key recommendations for improving the organisation's cybersecurity posture.

As you delve deeper into the world of cybersecurity, you will come to appreciate the critical role it plays in protecting organisations against cyberthreats. With the ever-increasing reliance on technology and the internet, cybersecurity has become a

vital aspect of any organisation's operations. It is no longer a question of whether an organisation will be targeted but rather a question of when. This task provides you with an excellent opportunity to learn and gain practical experience in the cybersecurity field while making a positive impact on our client's security posture.

Here is your task

As a cybersecurity professional, you will be expected to utilise various Open-Source Intelligence (OSINT) tools and techniques to gather information on APT34. You can find some OSINT tools in the resources section; however, feel free to conduct your own individual research.

You will also need to apply the MITRE ATT&CK Framework, a standardised tool used to identify and categorise cyberthreats, to develop a comprehensive defence strategy to protect the client's networks and systems against future attacks. You should answer the following questions in your research:

1. What is their history?

2. Which nation/state are they associated with?

3. Do they target specific industries?

4. What are their motives?

5. What are the TTPs they use to conduct their attacks?

6. What security measures could the client implement to defend against cyberattacks conducted by this APT?

Your ultimate goal is to communicate your findings and recommendations effectively to the client's leadership team, providing actionable insights that can improve the corporation's security posture. Submit your findings in the text submission box below.

Are you ready to take on this challenge and become a cybersecurity hero?

Let's get started!

Here are some resources to help you

OSINT tools to gather information on APT34:

Mandiant Security Blog: https://www.mandiant.com/resources/blog

CrowdStrike: https://www.crowdstrike.com/

Recorded Future: https://www.recordedfuture.com/

CyberScoop: https://www.cyberscoop.com/

Dark Reading: https://www.darkreading.com/

The CyberWire: https://thecyberwire.com/

SecureWorks - https://www.secureworks.com/

ThreatConnect - https://www.threatconnect.com

Kaspersky Lab: https://www.kaspersky.com/

Symantec Threat Intelligence: https://www.symantec.com/threat-intelligence

MITRE ATT&CK Framework (https://attack.mitre.org/): This is a widely used tool to categorise and identify cyberthreats. Students should familiarise themselves with the framework and understand how to apply it to develop a comprehensive defence strategy.

News and Other Resources: Students should stay up-to-date with the latest cybersecurity news and resources to gain a better understanding of the evolving cybersecurity landscape and new threats.

Cybersecurity and Infrastructure Security Agency (CISA): https://www.cisa.gov/

US-CERT: https://www.us-cert.gov/

Report: Upload your research to a dedicated repo with a READme file explaining what you are doing.