DATACOM Cybersecurity Virtual Internship

Reference: https://www.theforage.com/simulations/datacom/cybersecurity-zm6d

Tomás Villaseca C.

Tomas.villaseca.c@gmail.com

linkedin.com/in/tomasvc93/

Table of Contents

Task 1 - APT Breach: Analyzing the impact on Information Security

Task Overview:

Produce a comprehensive investigation report of a cyberattack on a client.

Will learn:

- How Datacom's cybersecurity consultants help evaluate impacts from sophisticated cyberattacks.

Will do:

- Investigate a cyber-attack and produce a comprehensive report documenting your findings and outline key recommendations for improving a client's cybersecurity posture.

Context

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 organization'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 organization's information security. 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 familiarized 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 organization's cybersecurity posture.

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.

Instructions

As a cybersecurity professional, you will be expected to utilize various Open-Source Intelligence (OSINT) tools and techniques to gather information on APT34.

You will also need to apply the MITRE ATT&CK Framework, a standardized tool used to identify and categorize cyber threats, to develop a comprehensive defense 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.

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 categorize and identify cyber threats. Students should familiarize themselves with the framework and understand how to apply it to develop a comprehensive defense 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/

Task 1.1 – Research APT34 with OSINT resources

1. What is their history?

APT34, also known as OilRig or HelixKitten, is a cyber-espionage group believed to have been active since at least 2015. This group is known for its sophisticated and persistent campaigns targeting various industries and organizations worldwide. Over the years, APT34 has been linked to multiple high-profile cyber-attacks, using advanced techniques to infiltrate networks and steal sensitive information.

2. Which nation/state are they associated with?

APT34 is widely believed to be associated with Iran. Multiple cybersecurity firms and government agencies have attributed their activities to the Iranian government, suggesting that their operations align with Iranian strategic interests.

3. Do they target specific industries?

APT34 has been known to target a wide range of industries, including:

- Financial institutions
- Energy sector (especially oil and gas)
- Telecommunications
- Government agencies
- Chemical industry
- Critical infrastructure
- Technology companies

Their choice of targets indicates a focus on gathering intelligence and potentially disrupting key sectors that are crucial for national security and economic stability.

4. What are their motives?

APT34's primary motives appear to be:

- **Espionage:** Collecting sensitive information from government entities, companies, and organizations to support national interests.

- **Surveillance:** Monitoring activities and communications of targeted individuals and organizations.
- **Disruption:** Potentially disrupting operations of critical infrastructure or key industries.
- **Economic Advantage:** Stealing intellectual property or proprietary information to benefit the national economy or state-owned enterprises.

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

Initial Access:

- **Phishing:** APT34 frequently uses spear-phishing emails with malicious attachments or links to gain initial access to target systems.

Execution:

- **PowerShell:** They utilize PowerShell scripts to execute commands and payloads on compromised systems, which are delivered through Microsoft Office documents, requiring user interaction for execution.

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

Initial Access Mitigation:

- **Email Filtering & Phishing Protection:** Implement advanced email filtering solutions to detect and block phishing emails. Utilize anti-phishing tools that analyze emails content and attachments for malicious indicators.
- **User Training and Awareness:** Conduct regular security awareness training to educate employees about recognizing phishing attempts (conduct phishing simulation campaigns).
- **Multi-Factor Authentication (MFA):** Enforce the use of MFA for email accounts and other critical systems to reduce the risk of compromised credentials from phishing attacks.
- **Safe Browsing Policies:** Implement web filtering solutions to block access to known malicious websites and enforce safe browsing policies.

Initial Access Mitigation:

- **PowerShell Constrained Language Mode:** Configure PowerShell to use Constrained Language Mode to restrict the capabilities of PowerShell scripts, preventing execution of potentially malicious commands.
- **Antivirus & EDR:** Deploy robust Antivirus and EDR solutions to monitor and detect PowerShell activity.
- **Application Whitelisting:** Only allow approved applications and scripts to execute on a system.

- **Disable Macros in Microsoft Office Documents:** Disable macros by default in Microsoft Office documents. Implement group policies to enforce macro security settings.
- **Script Block Logging:** Enable PowerShell Script Block Logging and Module Logging to capture detailed information about executed scripts.
- **Network Segmentation & Least Privilege:** Implement network segmentation to limit the spread of an attack if initial access is gained. Apply the principle of Least Privilege to restrict user access to only the resources necessary for their roles.

DATACOMP Example Answers:

What is their history?

Advanced Persistent Threat (APT) group 34, also known as OilRig or HelixKitten, is a state-sponsored cyber espionage group that has been active since at least 2014. APT34 is believed to operate out of Iran and has been associated with the Iranian government, specifically the Islamic Revolutionary Guard Corps.

Which nation/state are they associated with?

APT34 is believed to be associated with the Iranian government. Some cybersecurity experts have linked the group to Iran's Islamic Revolutionary Guard Corps (IRGC), a powerful military organization that is also involved in Iran's cyber operations.

Do they target specific industries?

APT34 is known for targeting a wide range of industries, including energy, finance, telecommunications and government agencies, mainly in the Middle East and the United States. The group's main objectives are to collect sensitive information and conduct cyber espionage activities on behalf of the Iranian government.

What are their motives?

The motives of APT34 are believed to be primarily espionage-related. They are known to target sensitive information such as intellectual property, financial data and government secrets. Some experts believe that APT34's activities are aimed at supporting Iran's strategic interests.

What are the TTPs (tactics, techniques and procedures) they use to conduct their attacks?

APT34 uses a variety of TTPs to conduct their attacks. Some of their known TTPs include spear-phishing, social engineering, malware delivery through malicious websites and password spraying. They have also been known to use custom malware, including a backdoor called POWRUNER. Once inside a target's network, APT34 uses various TTPs to maintain persistence and avoid detection. For example, the group often employs custom-built malware and command-and-control (C2) servers, and uses legitimate tools and software to evade detection.

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

To defend against cyberattacks conducted by APT34, clients could implement several security measures, including:

Employee training: providing regular cybersecurity awareness training to employees can help prevent spear-phishing attacks and other social engineering tactics used by APT34. - Multi-factor authentication (MFA): implementing MFA can prevent unauthorized access to sensitive data even if an attacker has gained access to login credentials.

Endpoint protection: deploying endpoint protection solutions such as anti-virus and anti-malware software can help detect and prevent malware infections.

Network segmentation: segmenting the network into smaller, isolated networks can help contain and prevent the spread of malware in case of a breach.

Incident response plan: having an incident response plan in place can help the client respond quickly and effectively in case of a security breach and minimize the impact of the attack.

By implementing these security measures, the client can better protect their networks and systems against APT34's attacks and other cyber threats.

Task 2 - Cybersecurity Risk Assessment

Task Overview:

Conduct a comprehensive risk assessment.

Will learn:

- How to identify, evaluate, and prioritize potential security threats and vulnerabilities to determine the level of risk and develop plans to mitigate those risks.

Will do:

- Complete a risk assessment for a client and help them define the context, assess their risk matrix, and identify potential risk scenarios.

Context

Your initial research on the APT group is a crucial step because it helps to identify the potential attackers and their methods, motives and targets. Understanding the TTPs of APT34 helps identify specific vulnerabilities and attack vectors that could be exploited.

This has laid a solid foundation for the next task, which is to conduct a comprehensive risk assessment for the client. The client has a fence around the perimeter of its property and a padlock on its entrance gate to prevent unauthorized access. However, the leadership team is concerned about potential risks and vulnerabilities that could compromise the security of its information and systems. They require a comprehensive risk assessment to identify potential security threats and vulnerabilities in their system or network.

As a cybersecurity consultant, you understand that conducting a risk assessment is an essential component of any effective cybersecurity strategy. This involves identifying, evaluating and prioritizing potential security threats and vulnerabilities to determine the level of risk and develop a plan to mitigate those risks. During the risk assessment, you will need to identify the assets that need to be protected, define the risk matrix and identify potential risk scenarios. You will assess the risk ratings for each scenario, both with and without existing measures in place. Finally, you will provide a risk assessment report to the client summarizing your findings and recommendations for mitigating risks and improving the institution's security posture.

The goal of the risk assessment is to help the client prioritize and implement appropriate security measures to mitigate and minimize risks. This will ensure the confidentiality, integrity and availability of their information and systems, as well as protect their reputation and financial resources.

Ultimately, your work will help the client comply with regulatory and legal requirements and standards and provide peace of mind knowing that their security is being handled by a knowledgeable and experienced cybersecurity expert.

Instructions

In this task, you will be documenting the client's risk position using the padlock analogy as an example. The client wants you to help them define the context, assess their risk matrix and identify potential risk scenarios.

To complete this task, you will need to:

1. Define the context – Identify the assets that need to be protected. This could include sensitive information, customer data, financial information or any other critical assets that are important to the client.

2. Define the risk matrix – Define the likelihood, consequence and risk rating for each potential risk scenario. The likelihood is the probability of the risk scenario occurring, while the consequence is the severity of the potential impact. The risk rating is a measure of the overall risk posed by the scenario, calculated by multiplying the likelihood and consequence.

3. Define three risk scenarios – Identify the specific risks that the client is trying to protect their assets from. For example, a cyberattack, natural disaster or employee negligence.

4. Assess risk rating for each risk scenario – Calculate the inherent risk rating for each scenario, assuming there are no measures in place to reduce the risk (without fence and padlock in place).

5. Assess risk rating for each risk scenario with existing measures – Calculate the current risk rating for each scenario taking existing measures in place to reduce the risk into consideration (with fence and padlock in place).

6. Assess risk levels for each risk scenario with additional measures – Identify any additional measures that could be put in place to further reduce the risk. Calculate the target risk rating for each scenario with these additional measures in place.

7. Create a risk assessment report for the client that summarizes the risk assessment findings, the risk mitigation strategy and any recommended measures for implementation.

You will need to use the provided **"Risk Assessment Template".**

Example of a Risk Scenario:

A cyberattack aimed at stealing sensitive information. The likelihood of such an attack could be rated as high, given the increasing frequency of cyberattacks. The impact of a successful cyberattack could be severe, potentially leading to loss of data, financial harm and damage to the client's reputation. The inherent risk rating for this scenario would therefore be high. However, the client may already have existing measures in place to mitigate the risk of a cyberattack, such as firewalls and antivirus software. These measures would reduce the likelihood and impact of the attack, resulting in a lower current risk rating. Finally, the client could also consider additional measures, such as regular software updates and security awareness training for employees, to further reduce the risk and achieve a lower target risk rating.

Cybersecurity Definitions

- **Risk assessment:** a process of identifying potential risks, analysing their likelihood and potential impact, and implementing measures to mitigate those risks.
- **Risk position:** The level of risk that an organisation faces.
- **Risk matrix:** A tool used to assess and evaluate risks based on the likelihood and consequence of a risk event occurring.
- **Likelihood:** The probability of a risk event occurring.
- **Consequence:** The severity of the potential impact of a risk event.
- **Risk rating:** A measure of the overall risk posed by a scenario, calculated by multiplying the likelihood and consequence.
- **Inherent risk rating:** The risk rating of a scenario without any measures in place to reduce the risk.
- **Current risk rating:** The risk rating of a scenario with existing measures in place to reduce the risk.
- **Target risk rating:** The desired risk rating of a scenario with additional measures put in place to further reduce the risk.
- **Risk assessment report:** A report that summarises the risk assessment findings, the risk mitigation strategy, and any recommended measures for implementation.
- **Avoid risk:** completely eliminate or forego risk.
- **Treat risk:** reduce the likelihood or impact of risk.
- **Transfer risk:** assign or move the risk to a third party.
- **Accept risk:** acknowledge the risk and choose not to resolve, transfer or mitigate.

Task 2.1 - Cybersecurity Risk Assessment

1. Define the context (Identify assets to protect):

- Customer database (PII) → $20 million usd
- Financial records and transactional data → $100 million usd
- Intellectual property (software and algorithms) → $800 million usd
- Operational systems → $150 million usd
- Employees records and HR data → $1 million usd.

2. Define the risk matrix:

- **Likelihood** = Probability of a risk scenario occurring.
    - **Rare:** May occur only in exceptional circumstances (once every 10+ years).
    - **Unlikely:** Could occur at some time, but not expected (once every 5-10 years).
    - **Possible:** Might occur at some time (once every 2-5 years).
    - **Likely:** Will probably occur in most circumstances (once every year).
    - **Almost Certain:** Expected to occur in most circumstances (multiple times per year).
- **Impact** = Severity of the consequences of a risk scenario occurring.
    - **Insignificant:** Negligible impact on operations, reputation, or finances (easily managed with normal procedures).
    - **Minor:** Small impact on operations, reputation, or finances (managed with minimal resources).
    - **Moderate:** Noticeable impact on operations, reputation, or finances (requires moderate resources to recover).
    - **Major:** Significant impact on operations, reputation, or finances (requires substantial resources to recover).
    - **Severe:** Catastrophic damage to operations, reputation, or finances (may lead to business failure).

$$\mathbf{Risk = Likelihood * Impact}$$

RISK MATRIX			LIKELIHOOD				
			Rare	Unlikely	Possible	Likely	Almost Certain
			May occur only in exceptional circumstances (once every 10+ years).	Could occur at some time, but not expected (once every 5-10 years).	Might occur at some time (once every 2-5 years).	Will probably occur in most circumstances (once every year).	Expected to occur in most circumstances (multiple times per year).
CONSEQUENCE	Severe	Catastrophic damage to operations, reputation, or finances (may lead to business failure).	HIGH	VERY HIGH	VERY HIGH	EXTREME	EXTREME
	Major	Significant impact on operations, reputation, or finances (requires substantial resources to recover).	HIGH	HIGH	VERY HIGH	VERY HIGH	EXTREME
	Moderate	Noticeable impact on operations, reputation, or finances (requires moderate resources to recover).	LOW	MEDIUM	MEDIUM	HIGH	VERY HIGH
	Minor	Small impact on operations, reputation, or finances (managed with minimal resources).	VERY LOW	LOW	MEDIUM	MEDIUM	HIGH
	Insignificant	Negligible impact on operations, reputation, or finances (easily managed with normal procedures).	VERY LOW	VERY LOW	LOW	MEDIUM	MEDIUM

3. Define three risk scenarios:

- **Risk Scenario 1:** Unauthorized physical access.
- **Risk Scenario 2:** Phishing attack targeting employees for sensitive information.
- **Risk Scenario 3:** Ransomware attack on critical systems.

4. Assess risk rating for each risk scenario (without existing measures):

Without fence & padlock:

- **Risk Scenario 1:** Unauthorized physical access.
  - **Likelihood:** Likely
  - **Impact:** Major
  - **Risk:** Very High

- **Risk Scenario 2:** Phishing attack targeting employees for sensitive information.
  - **Likelihood:** Almost Certain
  - **Impact:** Major
  - **Risk:** Extreme

- **Risk Scenario 3:** Ransomware attack on critical systems.
  - **Likelihood:** Possible
  - **Impact:** Severe
  - **Risk**: Very High

5. Assess risk rating for each risk scenario (with existing measures):

With fence & padlock:

- **Risk Scenario 1:** Unauthorized physical access.
  - **Likelihood:** Unlikely
  - **Impact:** Major
  - **Risk:** High

- **Risk Scenario 2:** Phishing attack targeting employees for sensitive information.
  - **Likelihood:** Almost Certain
  - **Impact:** Major
  - **Risk:** Extreme

- **Risk Scenario 3:** Ransomware attack on critical systems.
  - **Likelihood:** Possible
  - **Impact:** Severe
  - **Risk**: Very High

6. Assess risk levels for each risk scenario with additional measures:

Additional Measures → Fence & padlock, biometric access control, security guards, regular security awareness training, advanced mail filtering, robust backup systems, network segmentation, Antivirus, EDR, firewalls.

- **Risk Scenario 1:** Unauthorized physical access.
  - **Likelihood:** Rare
  - **Impact:** Moderate
  - **Risk:** Low

- **Risk Scenario 2:** Phishing attack targeting employees for sensitive information.
  - **Likelihood:** Possible
  - **Impact:** Moderate
  - **Risk:** Medium

- **Risk Scenario 3:** Ransomware attack on critical systems.
  - **Likelihood:** Unlikely
  - **Impact:** Major
  - **Risk**: High

7. Create a risk assessment report for the client that summarizes the risk assessment findings, the risk mitigation strategy and any recommended measures for implementation.

This report presents the findings of a risk assessment conducted for our client's organization, focusing on three key risk scenarios: unauthorized physical access, phishing attacks, and ransomware attacks. The assessment evaluates the current risk levels, existing control measures, and proposes additional measures to mitigate these risks.

	Risk			
ID	Title	Description	Sources or Causes of Risk	Consequences of Risk
R01	Unauthorized physical access.	Unauthorized individuals gaining physical access to sensitive areas of the organization, potentially compromising assets and data.	Inadequate physical security measures, Tailgating, and Stolen or duplicated access credentials.	Theft of physical assets, Data breach, and Damage to infrastructure.
R02	Phishing attack targeting employees for sensitive information.	Malicious actors attempting to deceive employees into revealing sensitive information or granting unauthorized access.	Social engineering tactics, Lack of employee awareness, and Sophisticated phishing techniques.	Data breaches, Financial losses, and Reputation damage.
R03	Ransomware attack on critical systems.	Malicious software encrypting critical systems and data, demanding ransom for decryption.	Phishing emails, Unpatched software vulnerabilities, and Infected external devices.	Operational disruption, Financial losses, and Data loss.

Inherent Risk Rating			Current Risk Rating				
Likelihood	Consequence	Risk Level	Existing control measures	Effectiveness of exisitng control measures	Likelihood	Consequence	Risk Level
Likely	Major	VERY HIGH	Fence & Padlock	**Excellent / Good / Moderate / Weak**	Unlikely	Major	HIGH
Almost Certain	Major	EXTREME	N/A	**Excellent / Good / Moderate / Weak**	Almost Certain	Major	EXTREME
Possible	Severe	VERY HIGH	N/A	**Excellent / Good / Moderate / Weak**	Possible	Severe	VERY HIGH

Target Risk Rating				
Additional control measures	Effectiveness of additional control measures	Likelihood	Consequence	Risk Level
Accept / Treat / Avoid / Transfer Biometric access control Security guards Visitor management system	**Excellent / Good / Moderate / Weak**	Rare	Moderate	LOW
Accept / Treat / Avoid / Transfer Regular security awareness training Advanced mail filtering	**Excellent / Good / Moderate / Weak**	Possible	Moderate	MEDIUM
Accept / Treat / Avoid / Transfer Robust backup systems Network segmentation Antivirus and EDR solutions	**Excellent / Good / Moderate / Weak**	Unlikely	Major	HIGH

By implementing these additional control measures, we can significantly reduce the likelihood and impact of the identified risk scenarios. Regular review and updates to this risk assessment will ensure our security posture remains robust in the face of evolving threats.

DATACOM Risks Assessment Report Example: (Only one risk scenario)

		Risk		
ID	Title	Description	Sources or Causes of Risk	Consequences of Risk
R01	Cyber attack	A cyberattack is a deliberate attempt by hackers to gain unauthorised access to a company's computer systems or networks, with the goal of stealing sensitive information, causing damage or disruption, or holding data ransom. The perceived sources for a cyberattack could include organised crime groups, nation-states, or individual hackers.	Organised crime groups, nation-states, or individual hackers	Data theft, system downtime, reputational damage, and financial losses.

Inherent Risk Rating		
Likelihood	Consequence	Risk Level
Likely	Major	VERY HIGH

Current Risk Rating				
Existing control	Effectiveness of exisitng control measures	Likelihood	Consequence	Risk Level
Firewalls, intrusion detection systems, antivirus software	**Firewalls** - Excellent control. Configured, maintained & tested properly. Highly effective and very fit for purpose. It substantially reduces the likelihood and/or consequence of the risk. It is cost effective. **Intrusion detection systems** - Moderate control. Configuration needs to be improved. **Antivirus** - Good control. Effective and fit for purpose. Configuration, maintenance and testing are good enough.	Possible	Major	VERY HIGH

Target Risk Rating				
Additional control measures	Effectiveness of additional control measures	Likelihood	Consequence	Risk Level
Treat - reduce the likelihood or impact of risk by following these additional control measures: - Multi-factor authentication (MFA) - Penetration testing - Regular security awareness training **Transfer** - We can also transfer this risk to a 3rd party by letting a Managed Security Service Provider made the organisation's Security Information and Event Management (SIEM) tool.	**Excellent / Good / Moderate / Weak** **Multi-factor authentication (MFA)** - Good Control. This would add an extra layer of security by requiring users to provide additional authentication factors beyond a password. **Security Information and Event Management (SIEM)** - Excellent Control. This would enable real-time monitoring of security events and alerts for any suspicious activity, and help with incident response. **Penetration testing** - Good Control. This would simulate a cyberattack to identify vulnerabilities and weaknesses in the system and help to improve the existing controls. **Regular security awareness training** - Good Control. This would help to educate employees about cyber threats and best practices to prevent them, and reduce the risk of human error or negligence.	Unlikely	Moderate	MEDIUM