Justin Goncalves

8/18/24

Datacom Cybersecurity Virtual Experience Program

Table of Contents

Program Overview:

Welcome to the Datacom cybersecurity program!

We are thrilled to have you here. As a company, we are dedicated to delivering top-notch services to our clients in different industries, from private to public sectors.

This program offers you the chance to experience what it's like to be part of our cybersecurity team and undertake tasks that mirror their everyday work. Throughout the program, you will learn critical skills such as risk assessment, research, analysis, and providing recommendations. These skills are in high demand in the industry, and we believe this program will be a valuable resource for you to upskill and strengthen your resume as you explore career options and the possibility of a career at Datacom.

Skills you will learn and practice: Security, Research, Analytical Skills, OSINT, Communication, Risk Assessment, Risk Management, Security Analysis

Task One: APT breach: analyzing the impact on information security
Produce a comprehensive investigation report of a cyberattack on a client
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 Two: Cybersecurity risk assessment

Conduct a comprehensive risk assessment

What you'll learn

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

What you'll do

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

Task 1

Review the scenario below. Then complete the program and activites.

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 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. 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 organization's cybersecurity posture.

As you delve deeper into the world of cybersecurity, you will come to appreciate the critical role it plays in protecting organizations against cyberthreats. With the ever-increasing reliance on technology and the internet, cybersecurity has become a vital aspect of any organization's operations. It is no longer a question of whether an organization 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.

As a cybersecurity professional, you will be expected to utilize 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 standardized tool used to identify and categorise cyberthreats, to develop a comprehensive defence strategy to protect the client's networks and systems against future attacks.

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.

Resources

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/

Justin Goncalves
Datacom Cybersecurity Consultant
8/17/2024

Facing APT34: An Investigative Report to Improve Security Posture and Defense

APT34, also known as Helix Kitten, OilRig, or Greenbug, is a sophisticated and persistent group of cyber vigilantes that has been active for nearly a decade. The group is widely believed to be based in Iran, conducting cyberattacks across a wide range of sectors, primarily targeting organizations in the Middle East, but also expanding and impacting Europe and North America as well. The group's activities have been extensively researched and documented by various cybersecurity organizations, including Mandiant, CrowdStrike, Cyware, MITRE, and more. Open Source Intelligence (OSINT) highlights APT34's focus on long-term espionage and data exfiltration. Their attacks have not only compromised personal and sensitive information, but have also posed significant challenges to the affected organizations' cybersecurity defenses. APT34 has demonstrated a high level of persistence and adaptability, making them a significant threat to organizations worldwide.

APT34 has been particularly active in targeting critical infrastructure and financial services within the Middle East, impacting both government entities and private organizations. APT34 targets industries that are essential to national security and economic stability because they hold vast amounts of sensitive data, and compromising them can yield significant intelligence. The energy sector, for instance, is a prime target due to its vital role in global economics and its direct relevance to Iran's oil-driven economy. By infiltrating companies within this sector, APT34 has aimed to gather intelligence on oil production, pricing strategies, and distribution networks, potentially giving Iran an economic edge. Similarly, the finance sector is targeted to exfiltrate financial data, which could be used to undermine economic stability in adversarial nations or to support Iran's own economic activities. Cyware and CrowdStrike reports highlight that APT34 also frequently targets telecommunications networks to access sensitive communications data and government institutions to gather state secrets. The motives behind these attacks are multifaceted, combining economic espionage, disruption of adversaries, and the acquisition of strategic intelligence that could boost Iran's geopolitical position.

The Tactics, Techniques, and Procedures (TTPs) employed by APT34 are both sophisticated and adaptive, making them a dangerous and advanced threat actor in the cybersecurity landscape. According to the MITRE ATT&CK framework, APT34 typically initiates their attacks through spear-phishing emails that are carefully crafted to target specific individuals within an organization. These emails often mimic legitimate communication and are designed to trick recipients into divulging sensitive information or downloading malicious software. Once APT34 gains access to a network, they employ a wide range of techniques to maintain their presence and escalate their privileges within the system. This includes the use of custom-developed malware and PowerShell implants, as well as the exploitation of Common Vulnerabilities and Exposures (CVEs) in widely used software. APT34 is also adept at lateral movement within compromised networks, using legitimate administrative tools to avoid detection and to exfiltrate sensitive data for extended periods of time, making them extremely dangerous. Their ability to blend in with normal network activity and their use of legitimate tools for malicious purposes makes detecting and responding to their attacks highly difficult for cybersecurity teams.

To effectively defend against cyberattacks conducted by APT34, organizations need to adopt a robust and multi-layered security strategy that is informed by the MITRE ATT&CK framework and the latest OSINT reports. Enhancing email security and Information Security Awareness is a critical first step, as spear-phishing remains one of APT34's primary attack vectors. This can be achieved through the implementation of advanced email filtering systems, as well as regular training programs that educate employees on how to recognize and respond to phishing attempts. Additionally, organizations must prioritize the regular updating and patching of software to close vulnerabilities that APT34 could exploit. Utilizing advanced threat detection and response systems that leverage behavioral analysis and machine learning can help with identifying, analyzing, and mitigating suspicious activities while they occur. Furthermore, conducting regular security audits and penetration testing can help identify potential weaknesses in the network before they can be exploited by attackers. Lastly, a comprehensive incident response plan and playbook are mandatory, ensuring that the organization is prepared to respond immediately and effectively to any potential breaches. By implementing all of these measures, organizations can significantly enhance their cybersecurity posture and reduce the risk of falling victim to advanced threat actors such as APT34.

Task 2

Congratulations on successfully completing the first task!

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 unauthorised 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 prioritising 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 summarising 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 minimise 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.

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 summarises the risk assessment findings, the risk mitigation strategy and any recommended measures for implementation.

Risk Assessment Evaluation and Report

Justin Goncalves
Datacom Cybersecurity Consultant
8/17/2024

Risk Assessment Evaluation and Report

This Risk Assessment Evaluation will consider both existing physical security measures, such as the perimeter fence and padlock, and digital security measures, like firewalls and intrusion detection systems, to evaluate the organization's current security posture. By identifying gaps and areas for improvement, this report will provide actionable insights to strengthen the organization's defenses against potential threats, ultimately supporting the company's long-term resilience and operational continuity.

The client's critical assets include:

- **Sensitive Information:** This covers intellectual property, proprietary business data, and trade secrets that are vital to the client's competitive advantage.
- **Customer Data:** Personal information, financial data, and transaction histories of customers that need to be protected to maintain trust and comply with legal requirements.
- **Financial Information:** This includes accounting records, financial statements, and other transactional data crucial for the client's operations.
- **Operational Systems:** IT infrastructure, including servers, databases, and network systems that support the client's day-to-day activities.
- **Reputation:** The public image and trustworthiness of the client, which could be severely impacted by a security breach

This comprehensive approach will help prioritize risks, allocate resources effectively, and provide the leadership team with the information needed to make informed decisions about the company's security strategies.

1. **Risk Impact and Probability Assessment Matrix**: In this step, I established the risk matrix, which serves as a tool to evaluate and prioritize the identified risks. I defined the likelihood and consequence scales, assigning values to represent the probability of each risk occurring and the severity of its potential impact. By multiplying the likelihood and consequence, I calculated the overall risk ratings, which helped categorize each risk as very low, low, medium, high, very high, or extreme, providing a structured way to assess and compare the potential risks our client's organization could face. (Figure 1)

2. **Comprehensive Risk Assessment and Control Evaluation Table:**
   a. Risk Scenarios and Inherent Risk Ratings: I identified the key risk scenarios that could potentially impact the client's organization, including data breaches, ransomware attacks, insider threats, power outages, and software vulnerability exploitation. I then analyzed the sources or causes of each risk, described the potential consequences if these events were to take place, and calculated the inherent risk ratings by evaluating the likelihood and severity of each scenario in the absence of any mitigating controls. This helped to establish a baseline understanding of the risks our client faces. (Figure 2)

   b. Current Security Controls and Risk Ratings: Next, I reviewed and listed the current control measures our client has in place to mitigate each identified risk scenario. I then evaluated the effectiveness of these controls, categorizing them as excellent, good, moderate, or weak, based on their ability to reduce the likelihood and impact of the risks. After this evaluation, I calculated the current risk ratings, taking into account the protection provided by these existing controls to assess how well they are currently mitigating each risk. (Figure 3)

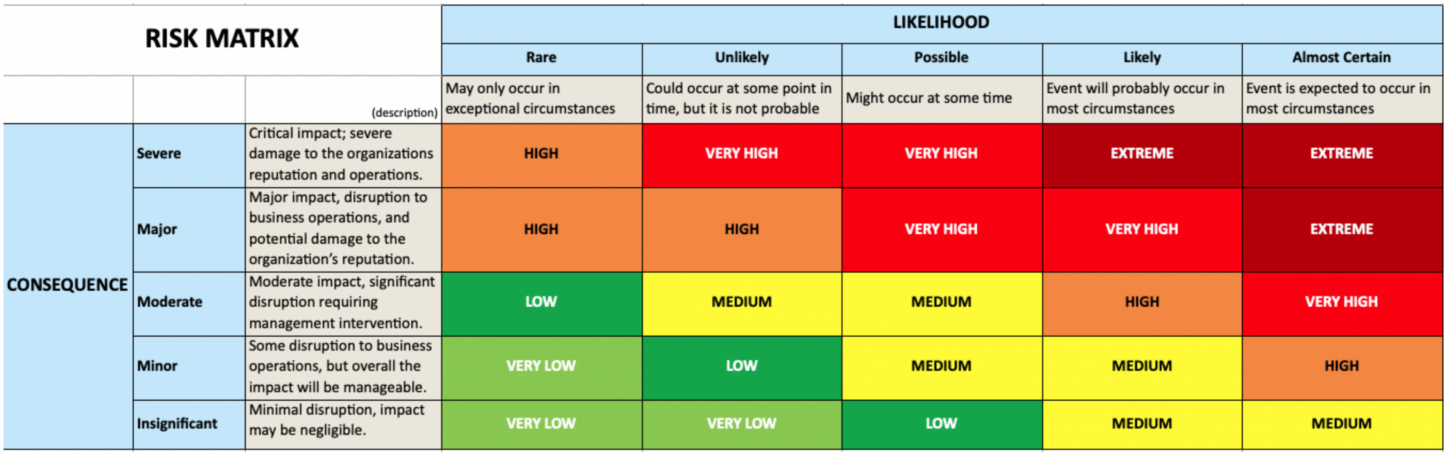
c. Recommended Security Controls and Target Risk Ratings: To conclude the risk assessment evaluation, I identified additional control measures that could further reduce the risks associated with each scenario. After proposing these new measures, I evaluated their potential effectiveness, and similar to the current security controls, categorized them as excellent, good, moderate, or weak. Finally, I calculated the target risk ratings with these additional controls in place, providing a clear picture of how these recommendations would improve our organization's overall security posture. (Figure 4)

By examining the existing physical and digital security measures, we identified key risk scenarios that could potentially impact the client's operations, assets, and reputation. Through the establishment of the Risk Impact and Probability Assessment Matrix, we prioritized these risks and assessed the effectiveness of current controls, offering a clear view of the inherent and current risk levels. The evaluation of existing controls demonstrated the effectiveness of measures already in place, but also revealed opportunities to further mitigate risks through additional recommended controls. By implementing these enhancements, the client can significantly reduce the likelihood and impact of potential threats, achieving lower target risk ratings and bolstering the organization's overall security resilience.

In conclusion, this comprehensive approach to risk assessment ensures that the client is well-equipped to protect its critical assets, maintain operational continuity, and uphold its reputation in the face of evolving security challenges. The actionable insights provided in this report will support the leadership team in making informed decisions that prioritize security, ultimately contributing to the long-term success and stability of the organization.

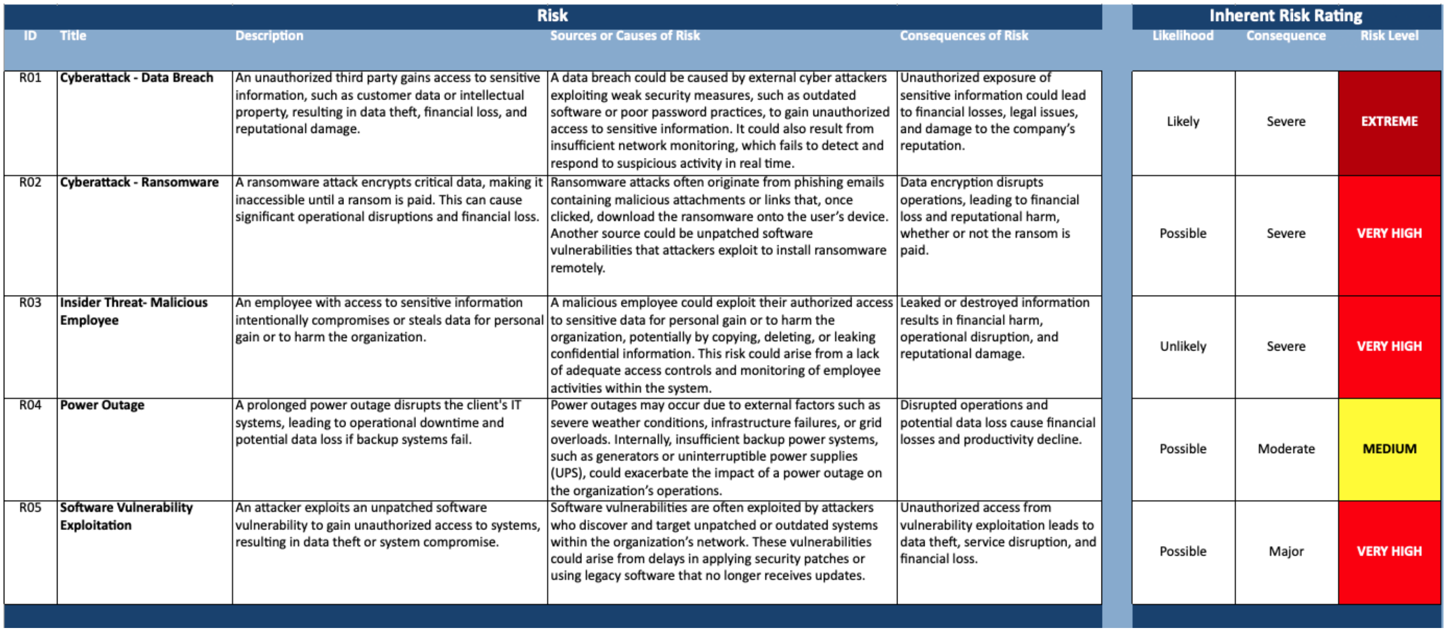
See Figures and Supporting Visuals Below

Figure 1: Risk Impact and Probability Assessment Matrix



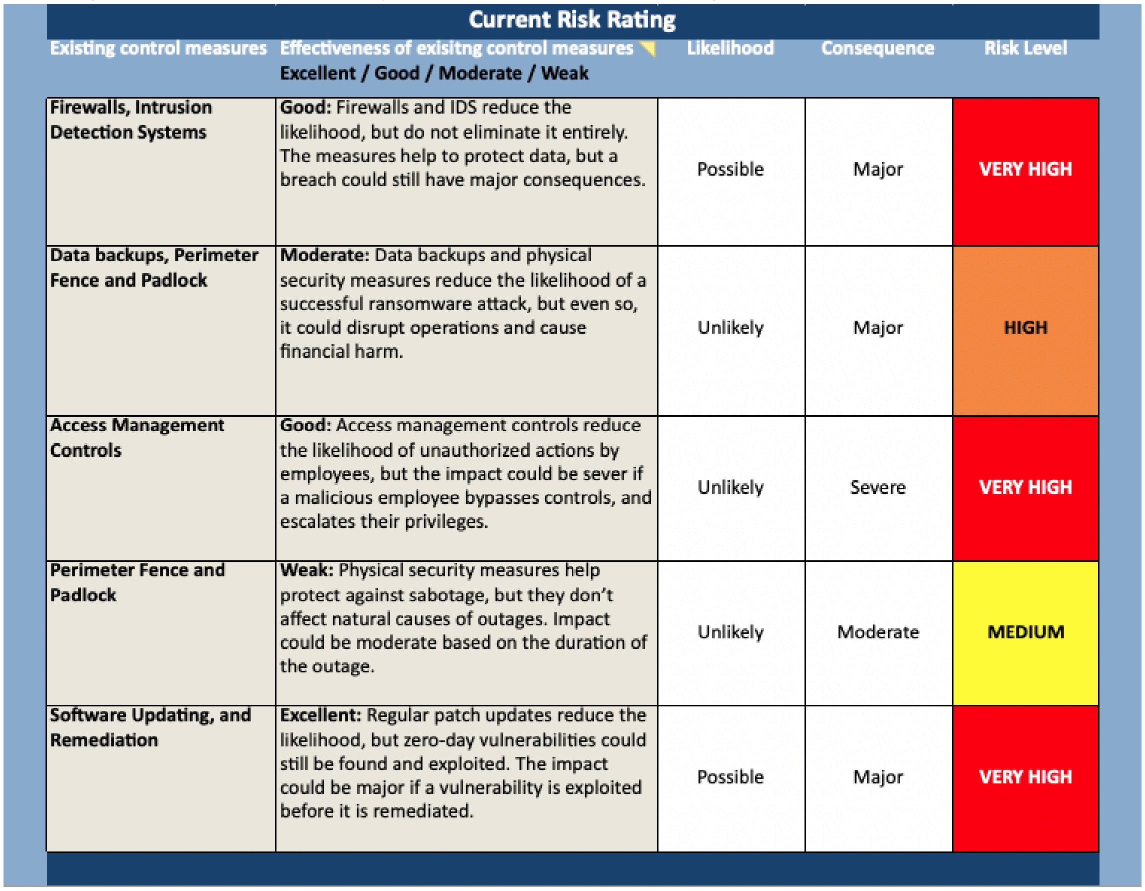
RISK MATRIX			LIKELIHOOD				
			Rare	Unlikely	Possible	Likely	Almost Certain
		(description)	May only occur in exceptional circumstances	Could occur at some point in time, but it is not probable	Might occur at some time	Event will probably occur in most circumstances	Event is expected to occur in most circumstances
CONSEQUENCE	Severe	Critical impact; severe damage to the organizations reputation and operations.	HIGH	VERY HIGH	VERY HIGH	EXTREME	EXTREME
	Major	Major impact, disruption to business operations, and potential damage to the organization's reputation.	HIGH	HIGH	VERY HIGH	VERY HIGH	EXTREME
	Moderate	Moderate impact, significant disruption requiring management intervention.	LOW	MEDIUM	MEDIUM	HIGH	VERY HIGH
	Minor	Some disruption to business operations, but overall the impact will be manageable.	VERY LOW	LOW	MEDIUM	MEDIUM	HIGH
	Insignificant	Minimal disruption, impact may be negligible.	VERY LOW	VERY LOW	LOW	MEDIUM	MEDIUM

Figure 2: Risk Scenarios and Inherent Risk Ratings



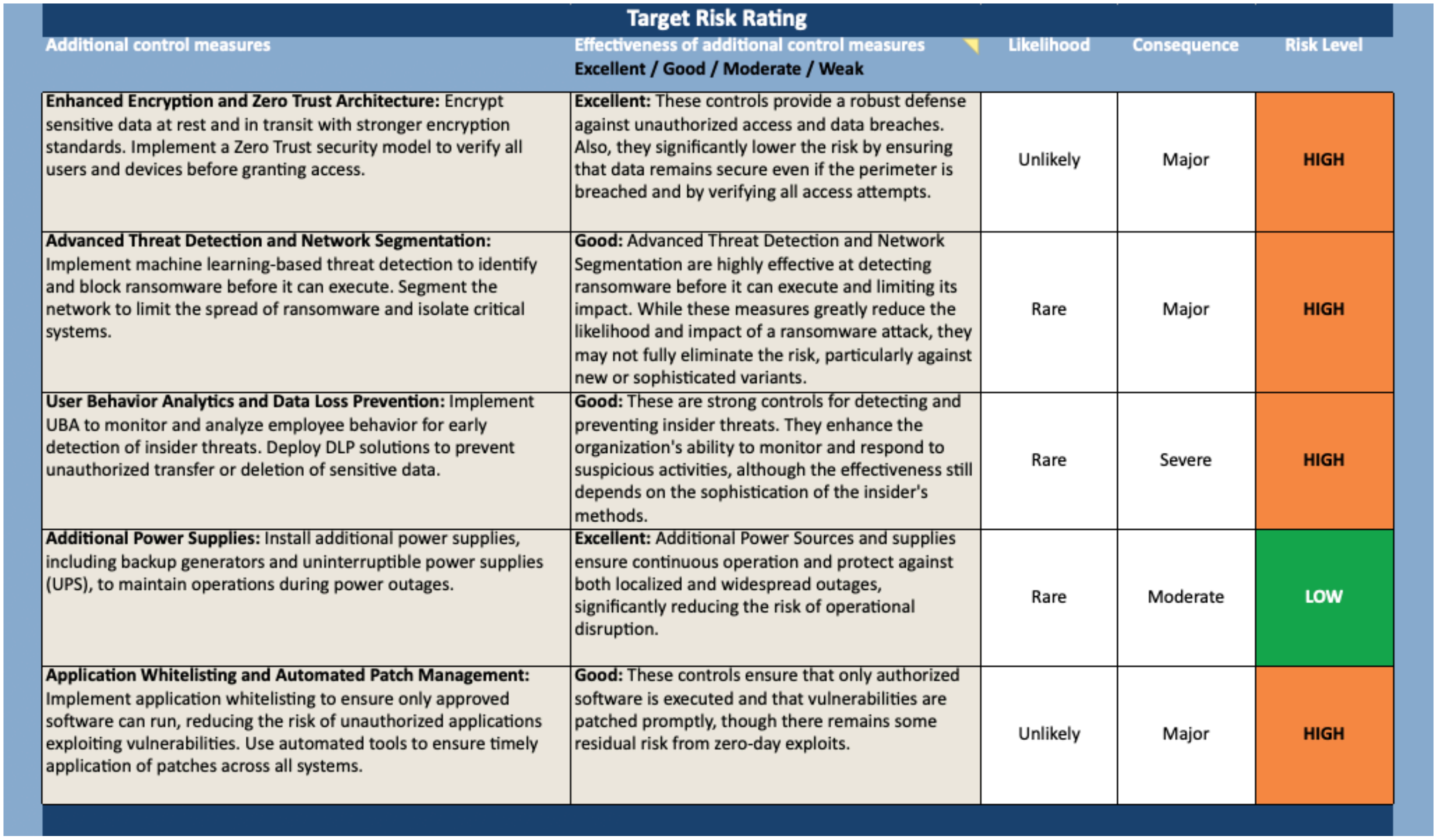
Risk					Inherent Risk Rating		
ID	Title	Description	Sources or Causes of Risk	Consequences of Risk	Likelihood	Consequence	Risk Level
R01	**Cyberattack - Data Breach**	An unauthorized third party gains access to sensitive information, such as customer data or intellectual property, resulting in data theft, financial loss, and reputational damage.	A data breach could be caused by external cyber attackers exploiting weak security measures, such as outdated software or poor password practices, to gain unauthorized access to sensitive information. It could also result from insufficient network monitoring, which fails to detect and respond to suspicious activity in real time.	Unauthorized exposure of sensitive information could lead to financial losses, legal issues, and damage to the company's reputation.	Likely	Severe	EXTREME
R02	**Cyberattack - Ransomware**	A ransomware attack encrypts critical data, making it inaccessible until a ransom is paid. This can cause significant operational disruptions and financial loss.	Ransomware attacks often originate from phishing emails containing malicious attachments or links that, once clicked, download the ransomware onto the user's device. Another source could be unpatched software vulnerabilities that attackers exploit to install ransomware remotely.	Data encryption disrupts operations, leading to financial loss and reputational harm, whether or not the ransom is paid.	Possible	Severe	VERY HIGH
R03	**Insider Threat- Malicious Employee**	An employee with access to sensitive information intentionally compromises or steals data for personal gain or to harm the organization.	A malicious employee could exploit their authorized access to sensitive data for personal gain or to harm the organization, potentially by copying, deleting, or leaking confidential information. This risk could arise from a lack of adequate access controls and monitoring of employee activities within the system.	Leaked or destroyed information results in financial harm, operational disruption, and reputational damage.	Unlikely	Severe	VERY HIGH
R04	**Power Outage**	A prolonged power outage disrupts the client's IT systems, leading to operational downtime and potential data loss if backup systems fail.	Power outages may occur due to external factors such as severe weather conditions, infrastructure failures, or grid overloads. Internally, insufficient backup power systems, such as generators or uninterruptible power supplies (UPS), could exacerbate the impact of a power outage on the organization's operations.	Disrupted operations and potential data loss cause financial losses and productivity decline.	Possible	Moderate	MEDIUM
R05	**Software Vulnerability Exploitation**	An attacker exploits an unpatched software vulnerability to gain unauthorized access to systems, resulting in data theft or system compromise.	Software vulnerabilities are often exploited by attackers who discover and target unpatched or outdated systems within the organization's network. These vulnerabilities could arise from delays in applying security patches or using legacy software that no longer receives updates.	Unauthorized access from vulnerability exploitation leads to data theft, service disruption, and financial loss.	Possible	Major	VERY HIGH

Figure 3: Current Security Controls and Risk Ratings



Current Risk Rating				
Existing control measures	Effectiveness of exisitng control measures Excellent / Good / Moderate / Weak	Likelihood	Consequence	Risk Level
Firewalls, Intrusion Detection Systems	**Good:** Firewalls and IDS reduce the likelihood, but do not eliminate it entirely. The measures help to protect data, but a breach could still have major consequences.	Possible	Major	**VERY HIGH**
Data backups, Perimeter Fence and Padlock	**Moderate:** Data backups and physical security measures reduce the likelihood of a successful ransomware attack, but even so, it could disrupt operations and cause financial harm.	Unlikely	Major	**HIGH**
Access Management Controls	**Good:** Access management controls reduce the likelihood of unauthorized actions by employees, but the impact could be sever if a malicious employee bypasses controls, and escalates their privileges.	Unlikely	Severe	**VERY HIGH**
Perimeter Fence and Padlock	**Weak:** Physical security measures help protect against sabotage, but they don't affect natural causes of outages. Impact could be moderate based on the duration of the outage.	Unlikely	Moderate	**MEDIUM**
Software Updating, and Remediation	**Excellent:** Regular patch updates reduce the likelihood, but zero-day vulnerabilities could still be found and exploited. The impact could be major if a vulnerability is exploited before it is remediated.	Possible	Major	**VERY HIGH**

Figure 4: Recommended Security Controls and Target Risk Ratings



Target Risk Rating				
Additional control measures	Effectiveness of additional control measures Excellent / Good / Moderate / Weak	Likelihood	Consequence	Risk Level
Enhanced Encryption and Zero Trust Architecture: Encrypt sensitive data at rest and in transit with stronger encryption standards. Implement a Zero Trust security model to verify all users and devices before granting access.	**Excellent:** These controls provide a robust defense against unauthorized access and data breaches. Also, they significantly lower the risk by ensuring that data remains secure even if the perimeter is breached and by verifying all access attempts.	Unlikely	Major	**HIGH**
Advanced Threat Detection and Network Segmentation: Implement machine learning-based threat detection to identify and block ransomware before it can execute. Segment the network to limit the spread of ransomware and isolate critical systems.	**Good:** Advanced Threat Detection and Network Segmentation are highly effective at detecting ransomware before it can execute and limiting its impact. While these measures greatly reduce the likelihood and impact of a ransomware attack, they may not fully eliminate the risk, particularly against new or sophisticated variants.	Rare	Major	**HIGH**
User Behavior Analytics and Data Loss Prevention: Implement UBA to monitor and analyze employee behavior for early detection of insider threats. Deploy DLP solutions to prevent unauthorized transfer or deletion of sensitive data.	**Good:** These are strong controls for detecting and preventing insider threats. They enhance the organization's ability to monitor and respond to suspicious activities, although the effectiveness still depends on the sophistication of the insider's methods.	Rare	Severe	**HIGH**
Additional Power Supplies: Install additional power supplies, including backup generators and uninterruptible power supplies (UPS), to maintain operations during power outages.	**Excellent:** Additional Power Sources and supplies ensure continuous operation and protect against both localized and widespread outages, significantly reducing the risk of operational disruption.	Rare	Moderate	**LOW**
Application Whitelisting and Automated Patch Management: Implement application whitelisting to ensure only approved software can run, reducing the risk of unauthorized applications exploiting vulnerabilities. Use automated tools to ensure timely application of patches across all systems.	**Good:** These controls ensure that only authorized software is executed and that vulnerabilities are patched promptly, though there remains some residual risk from zero-day exploits.	Unlikely	Major	**HIGH**

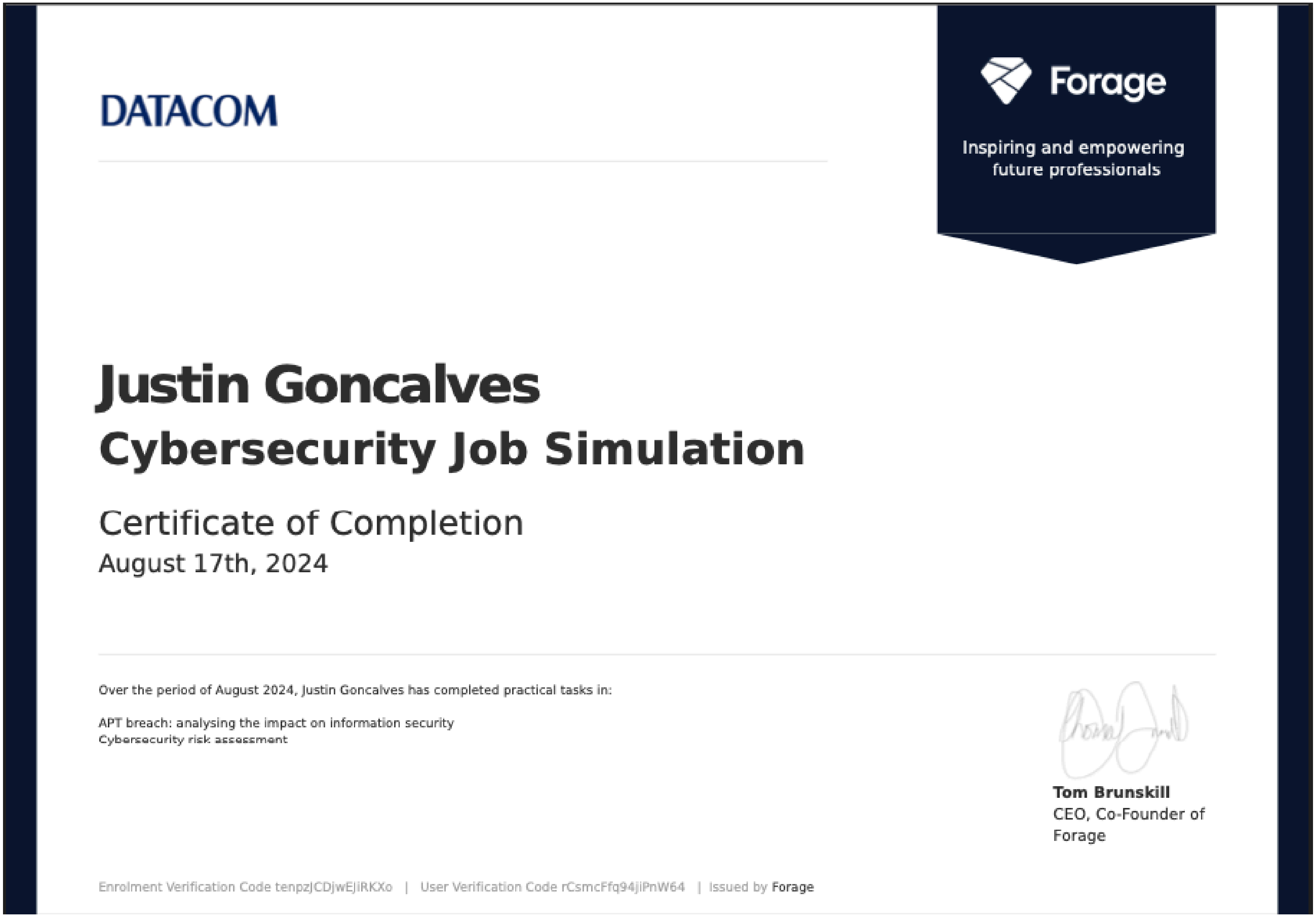
Personal Reflection

Participating in this program has been an incredibly enriching experience that has solidified my interest in pursuing a career in cybersecurity. In the first part of the program, I conducted an investigative report on APT34, which involved extensive research, communication, and security analysis. This task required me to utilize OSINT tools to gather intelligence on the threat actor and analyze their tactics, techniques, and procedures (TTPs). The experience of compiling this information into a comprehensive report not only sharpened my research and analytical skills but also enhanced my ability to communicate complex security issues clearly and effectively—skills that are crucial in any cybersecurity role.

The second part of the program involved a detailed risk assessment evaluation, where I developed a Risk Impact and Probability Assessment Matrix and a Comprehensive Risk Assessment and Control Evaluation Table. This process required me to assess various risk scenarios, evaluate the effectiveness of existing security controls, and recommend additional measures to enhance the organization's security posture. These tasks provided me with hands-on experience in risk management, a core aspect of cybersecurity consulting. I learned how to prioritize risks, develop actionable mitigation strategies, and communicate these findings in a structured and impactful report.

Overall, this program has provided me with practical skills that are directly applicable to real-world cybersecurity work. Whether it's conducting threat analysis, implementing risk management strategies, or communicating security findings to stakeholders, I now feel well-prepared to tackle these challenges in a professional setting. The combination of investigative research and risk assessment has not only deepened my technical expertise but also strengthened my resolve to build a career in cybersecurity. The insights and experience gained through this program will be invaluable as I move forward, helping me to confidently navigate the complexities of cybersecurity consulting and analysis in the future.

Certificate of Completion



DATACOM

Forage

Inspiring and empowering
future professionals

Justin Goncalves

Cybersecurity Job Simulation

Certificate of Completion

August 17th, 2024

Over the period of August 2024, Justin Goncalves has completed practical tasks in:

APT breach: analysing the impact on information security
Cybersecurity risk assessment

Tom Brunskill
CEO, Co-Founder of
Forage

Enrolment Verification Code tenpzJCDjwEJiRKXo | User Verification Code rCsmcFfq94jiPnW64 | Issued by Forage