CYB102 Project 6

(🔗 Instructions Page)

🕵 Student Name: Didier Joseph DESMAANGLES
✉ Student Email: djdesmangles@gmail.com

Reflection (Required)

🤔 **Reflection Question #1:** If I had to **explain "what is a cyber breach" in 3 emojis,** they would be...
(Feel free to put other comments about your experience in this unit here, too!)

💻🔓😭
💻 **Computer**: Your important and private datas
🔓**Unlocked padlock** : Your system is not secure anymore and has been fraudulently accessed from the outside
😭 **You** : are panicking and crying in shock to see all your informations in the wild.

🧠**Reflection Question #2:** Which step of the incident response process do you think is most important?

Containment is a key part of incident handling, most often rated as the number one mitigation requirement. In this hierarchy of measures, the step of containment is conclusively the one that is applied to stop the spread of damage and data loss to possibly salvage any remaining data and functions. Fast and sound containment measures taken to address an incident work effectively because they mean that there is less work to be done during the investigation, eradication, and recovery stages before the issue ends or gets escalated.

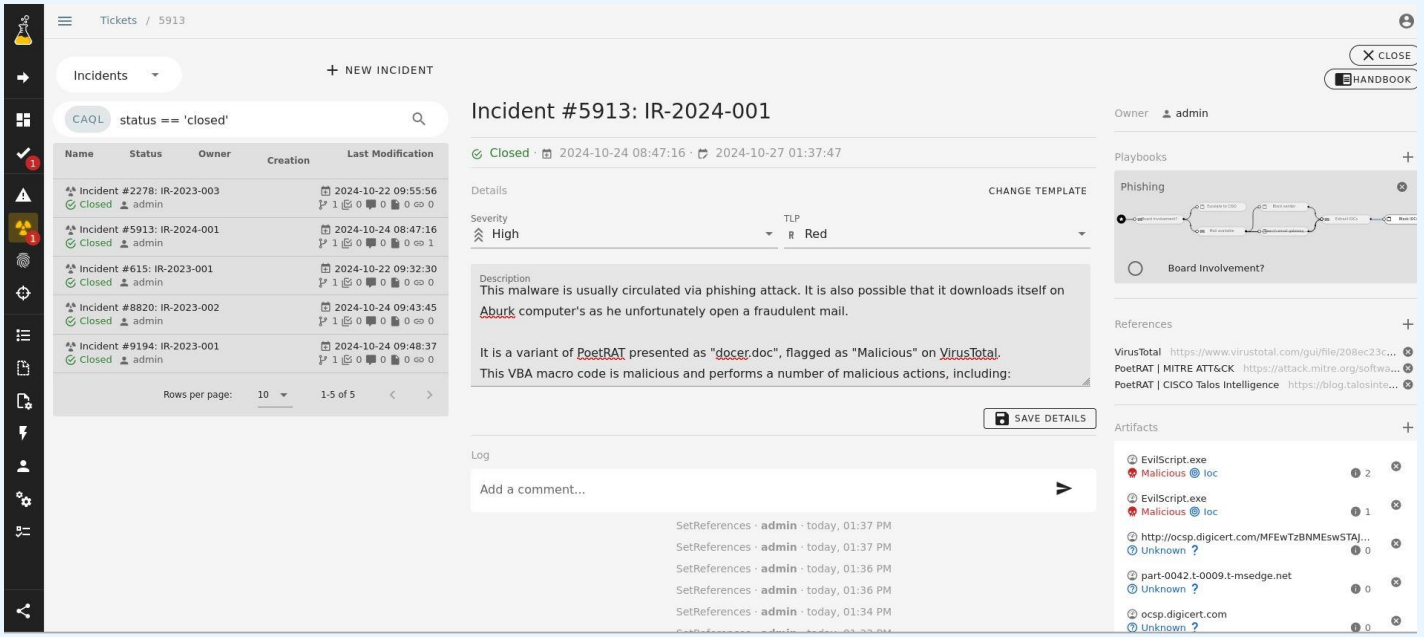
When containment is missing, even the tiniest problems can easily grow to become mammoth proportions, making it difficult to fix them at later stages.

📣 **Shoutouts:** Share appreciation for anyone who helped you out with this project or made your day a little better!

MYYYY TEEEEEEEEEEAM 17 !!!

Required Challenges (Required)

Item #1: A screenshot of your Splunk Malware case in Catalyst:



Item #2: At least one artifact and notes from an external source:

1. **EvilScript.exe | docer.doc**

- **Basic properties**

  MD5

  3aadbf7e527fc1a050e1c97fea1cba4d

- ***SHA-1***

  2cf055b3ef60582ca72e77bc4693ea306360f611

- ***SHA-256***

  208ec23c233580dbfc53aad5655845f7152ada56dd6a5c780d54e84a9d227407

- ***Vhash***

  bd46421fad0a464ff4304006b6ac9756

- ***SSDEEP***

  196608:9EjYtulHyQiaallFVAa8oPe5Nxhq1gMqnDORSG/:rtulHF7b4a8GeFhYqne/

- ***TLSH***

  T12C863324A0B59E1BD0334E348456278959BD7D9BDE3AD36B138CB72878BB3F96143348

File type

MS Word Document

document

msoffice

text

word

doc

Magic

Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, Code page: 1251, Author: Jeremy, Template: Normal.dotm, Last Saved By: Jeremy, Revision Number: 248, Name of Creating Application: Microsoft Office Word, Total Editing Time: 3d+01:26:00, Create Time/Date: Mon Nov 11 06:20:00 2019, Last Saved Time/Date: Sun Apr 12 12:08:00 2020, Number of Pages: 3, Number of Words: 839, Number of Characters: 4787, Security: 8

TrID

Microsoft Word document (39.2%) Kingsoft WPS Office document (alt.) (25.4%) Microsoft Word document (old ver.) (24.8%) Generic OLE2 / Multistream Compound (10.4%)

Magika

UNKNOWN

File size

7.95 MB (8331598 bytes)

History

Creation Time

2019-11-11 06:20:00 UTC

First Seen In The Wild

2020-05-30 22:21:30 UTC

First Submission

2020-04-13 16:38:17 UTC

Last Submission

2021-12-27 05:47:55 UTC

Last Analysis

2024-10-24 00:56:44 UTC

Names

docer.doc

mMbFY2c2mCAmTNvTkYIxyhaoS6yi5K

output.177041112.txt

539229.doc

208ec23c233580dbfc53aad5655845f7152ada56dd6a5c780d54e84a9d227407.docx

208ec23c233580dbfc53aad5655845f7152ada56dd6a5c780d54e84a9d227407.bin

Azerbaijan_special.doc

Item #3: A brief write-up of your findings and Lessons Learned:

1. **Teamwork makes the dream work**
   The first thing that comes to mind is the importance of working as a team. Communication and good listening skills are extremely important. Sometimes, another teammate mentions the little detail that unlocks the whole situation. So we have to be good listeners, be open to discussion, and learn to trust. We can only see part of the truth. We have to put everything on the table to get a better perspective.

2. **The devil is in the details**
   attention to detail is vital in a SOC. You must also develop the right reflexes and always be ready to find a way around a difficulty or challenge because no situation is perfect.

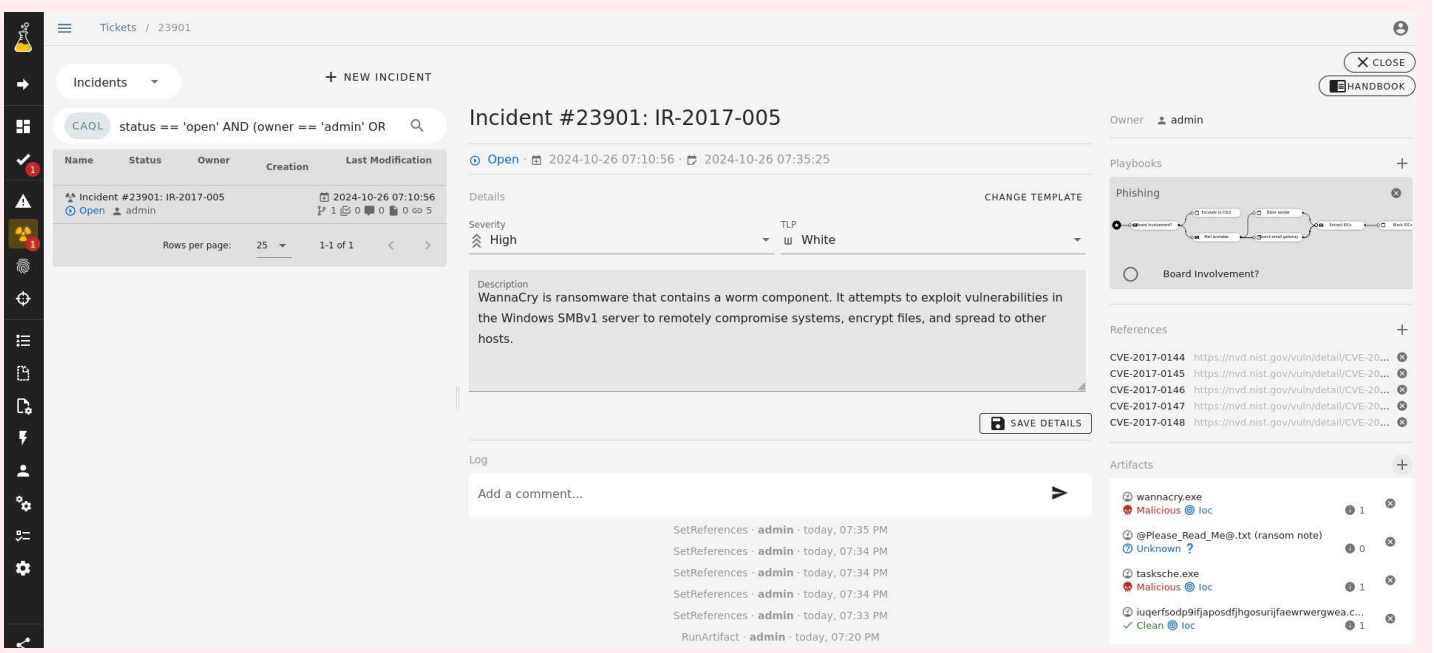
3. **Importance of tools such as VirusTotal, AbuseIPDB and others**

   Submitting the MD5 Hash “3aadbf7e527fc1a050e1c97fea1cba4d” revealed a wealth of details about the malware (EvilScript.exe) found in the previous exercise. We knows now it

is a worm “PoetRAT” that use phishing to infect target. In our investigation we will make sure to check Aburk email to confirm what happen and understand how the infection started.
VirusTotal also gives a very helpful list of articats, helping us with the mitigation.

Stretch Challenge (Optional)

Bonus Task #1: Catalyst Investigation - Use Catalyst to manage the incident and fill out the case with the Artifacts, Tasks, and TTPs that you researched:



Bonus Task #2: NIST or Sans Framework Analysis - Write a report that outlines the steps of either the NIST or SANS framework and how it could have prevented the breach:

Incident Response Report:
NIST Framework Analysis of WannaCry Breach

Context

What was the WannaCry ransomware attack?
https://www.cloudflare.com/learning/security/ransomware/wannacry-ransomware/
The WannaCry ransomware attack was a major security incident that impacted organizations all

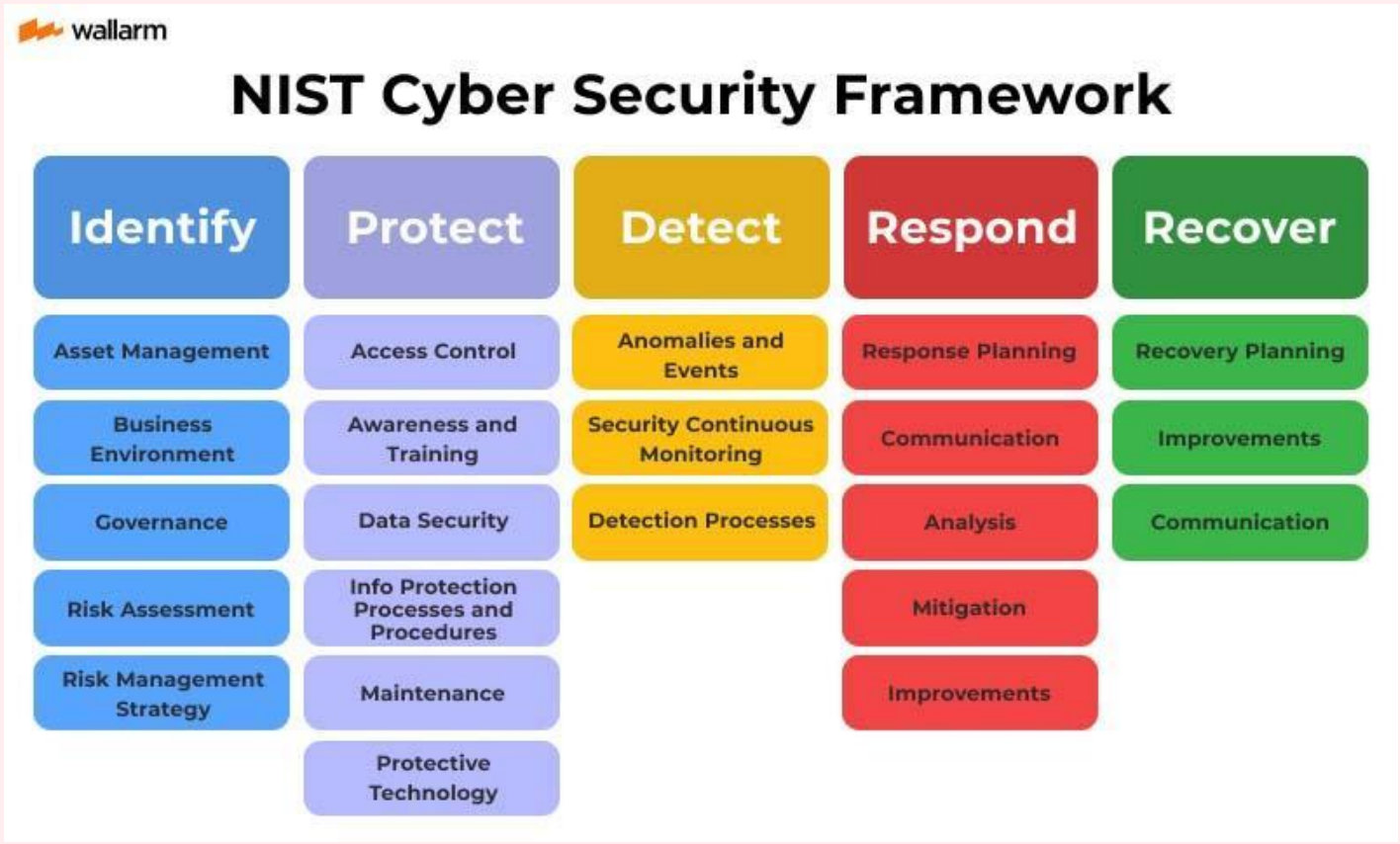
over the world. On May 12, 2017, the WannaCry ransomware worm spread to more than 200,000 computers in over 150 countries. Notable victims included FedEx, Honda, Nissan, and the UK's National Health Service (NHS), the latter of which was forced to divert some of its ambulances to alternate hospitals.

Within hours of the attack, WannaCry was temporarily neutralized. A security researcher discovered a "kill switch" that essentially turned off the malware. However, many affected computers remained encrypted and unusable until the victims paid the ransom or were able to reverse the encryption.

WannaCry spread by using a vulnerability exploit called "EternalBlue." The US National Security Agency (NSA) had developed this exploit, presumably for their own use, but it was stolen and released to the public by a group called the Shadow Brokers after the NSA was itself compromised. *EternalBlue only worked on older*, *unpatched versions of Microsoft Windows*, but there were more than enough machines running such versions to enable WannaCry's rapid spread.

What is the NIST framework?
The NIST Cybersecurity Framework is a set of guidelines, standards, and best practices developed by the National Institute of Standards and Technology (NIST) to help organizations manage and reduce cybersecurity risks. The framework is designed to be flexible and adaptable, allowing organizations of all sizes and industries to strengthen their cybersecurity posture and better protect critical infrastructure, systems, and data.

The NIST Framework, if deployed, should help protect the organization and its clients against such threats as WannaCry and weaken the threats- if they do occur.



Core Components of the NIST Cybersecurity Framework

The framework has five primary functions:

1. **Identify**: Understand and manage cybersecurity risks to systems, assets, data, and capabilities. This involves asset management, business environment assessment, governance, risk management, and understanding organizational vulnerabilities.
2. **Protect**: Implement safeguards to limit or contain the impact of potential cybersecurity events. This includes identity management, access control, data security, and awareness training.
3. **Detect**: Develop and maintain systems to identify cybersecurity events promptly. Detection activities include continuous monitoring, threat detection, and incident identification.
4. **Respond**: Define actions to take once a cybersecurity incident has been detected. This includes developing incident response plans, communication protocols, and analysis of security events.
5. **Recover**: Restore capabilities or services that were impaired by a cybersecurity incident. Recovery activities involve planning for resilience, restoring data, and improving response and recovery planning from previous incidents.

Now, let's apply the NIST Framework to the WannaCry case.

- **IDENTIFY**
    - **Asset Management**: Ensure that systems, especially critical infrastructure using SMB, are up-to-date with patches and known vulnerabilities (like MS17-010, which WannaCry exploited).
    - **Business Environment:** is about understanding the organization's mission, objectives, stakeholders, and critical functions. This understanding is crucial in prioritizing cybersecurity efforts and allocating resources effectively to protect core business functions. In the context

of the WannaCry ransomware attack, focusing on the Business Environment would mean examining the organization's operations, dependencies, and impacts to better anticipate and mitigate ransomware risks.

1. Understand Critical Business Functions and Dependencies

- **Identify Essential Systems and Applications**: Define the specific systems, applications, and data that are crucial to business operations. For instance, an organization could prioritize protecting systems supporting core processes, such as production lines, financial systems, or healthcare records.
- **Assess System Dependencies**: Recognize dependencies, such as network access (e.g., SMB protocol for file sharing), that WannaCry exploited. Mapping out these dependencies helps organizations identify which systems are interconnected and could be at risk if one system is compromised.
- **Evaluate Third-Party Risks**: Consider third-party vendors or partners who may interact with critical systems. Understanding this landscape allows for better control over potential external vulnerabilities that could introduce WannaCry or similar ransomware.

2. Analyze Business Impact and Tolerance for Downtime

- **Determine Potential Impact of Data Loss or Encryption**: Evaluate how a ransomware incident, like WannaCry, would impact different areas, from operational disruptions to potential financial and reputational harm. This insight aids in defining backup priorities, recovery time objectives (RTOs), and recovery point objectives (RPOs) for critical data.
- **Set Downtime Tolerance for Key Functions**: By assessing how long the organization can afford for certain functions to be offline (e.g., manufacturing lines or customer-facing portals), companies can tailor incident response and business continuity strategies accordingly, ensuring minimal impact if WannaCry or similar ransomware strikes.

3. Align Cybersecurity Goals with Business Objectives

- **Link Cybersecurity with Business Goals**: Position cybersecurity initiatives, such as patch management and backup systems, as essential for supporting business objectives, like protecting client data and ensuring uninterrupted service delivery. For instance, highlighting how patching would have prevented WannaCry can emphasize the value of these security initiatives.
- **Risk Tolerance and Resource Allocation**: Define the organization's tolerance for cybersecurity risks in line with business objectives, guiding investment in security measures proportionate to the impact on critical operations. This could include prioritizing budget allocations for security controls on systems highly vulnerable to ransomware exploits.

4. Engage Key Stakeholders and Define Responsibilities

- **Identify Relevant Stakeholders**: Engage stakeholders across departments, such as IT, legal, compliance, and executive management, to foster a comprehensive understanding of ransomware threats like WannaCry and their impact. Clear

communication ensures that all stakeholders appreciate the importance of security measures, such as the MS17-010 patch to safeguard against SMB vulnerabilities.
    - **Clarify Roles in Incident Response**: Define roles and responsibilities for handling ransomware incidents. For example, IT may lead technical containment and eradication, while legal handles regulatory notifications, and executive leadership coordinates public relations in the event of an incident.
  - **Governance:** ensures that an organization's cybersecurity policies, procedures, and risk management efforts align with its mission, objectives, and regulatory requirements. It provides a framework for accountability and oversight that helps protect essential business functions against cyber threats like WannaCry. Applying the Governance function in response to the WannaCry ransomware attack involves establishing policies, oversight mechanisms, and clear roles to enhance preparedness and resilience.
  - **Risk Management**: In the NIST Cybersecurity Framework 2.0, Risk Management involves identifying, assessing, and mitigating risks in alignment with the organization's objectives, ensuring that cyber defenses and resources effectively address potential threats. For an attack like WannaCry, which exploited a known vulnerability in the SMB protocol to spread ransomware across networks, implementing Risk Management practices would significantly reduce the likelihood of an incident.
  - **Risk Management Strategy**: provides guidance on identifying, assessing, and mitigating risks associated with ransomware attacks. WannaCry exploited a known vulnerability in the Windows SMB protocol, impacting unpatched systems globally. This strategy would use a structured approach to reduce the likelihood of infection, contain potential incidents, and minimize operational disruption.

- **PROTECT**
  - **Access Control**: Limit SMB access between devices on the network and restrict administrative privileges to critical systems only.
  - **Data Security**: Ensure backup solutions and data encryption are in place, with an offline copy stored safely to mitigate ransomware impact.
  - **Awareness Training**: Educate users on ransomware risks and phishing, which can be a common attack vector for malware distribution.
  - **Maintenance**: Implement a regular patching and updating process to address critical vulnerabilities, such as MS17-010, which would have prevented WannaCry from exploiting the SMB vulnerability
  - **Protective Technology**:
    1. **Secure Configurations and Hardening**
    - **Network Hardening**: Disable SMBv1 protocol where possible, as it is outdated and highly vulnerable to exploits. Implement additional security configurations, such as disabling unnecessary services and limiting system functions to reduce attack surfaces.

    2. Access Control and Authentication

    - **Multi-Factor Authentication (MFA)**: Require MFA for accessing sensitive systems and applications, particularly administrative or high-privilege accounts that ransomware could use to spread further across the network.
    - **Least Privilege Principle**: Limit user access based on the principle of least privilege,

ensuring that employees and systems only have access to resources they strictly need. Restrict administrative privileges for SMB access to minimize the chances of ransomware exploiting high-level accounts.

3. Network Segmentation and Isolation

- **Implement Network Segmentation**: Divide the network into segments with restricted communication between them, isolating critical assets from general network traffic. This makes it harder for WannaCry to move laterally if an endpoint is infected.
- **Restrict SMB Traffic**: Limit SMB traffic to only specific systems and use internal firewalls to control access to SMB services. Blocking SMB at the firewall for segments that don't require it minimizes exposure to WannaCry's primary exploit vector.

4. Endpoint Protection and Monitoring

- **Deploy Endpoint Detection and Response (EDR)**: Use EDR solutions on all endpoints to detect, alert, and potentially quarantine systems that exhibit WannaCry indicators of compromise (IOCs), such as the creation of suspicious files or unusual SMB traffic.
- **Anti-Malware Solutions**: Ensure all endpoints have up-to-date anti-malware solutions capable of identifying WannaCry and other ransomware variants. Configure regular scans and real-time detection of ransomware signatures.

5. Intrusion Detection and Prevention Systems (IDPS)

- **Network-Based IDPS**: Deploy an IDPS that monitors network traffic for signs of WannaCry propagation, such as unusual SMB traffic or connections to known malicious IP addresses associated with WannaCry. This helps detect early indicators of compromise before significant spread occurs.
- **Host-Based IDPS**: Install host-based intrusion prevention systems on critical servers to monitor for unauthorized file changes and process executions that could indicate ransomware behavior.

6. Data Protection and Backup

- **Secure Backup Systems**: Implement regular, automated backups of critical data stored offline or in a separate network segment, disconnected from daily operations. This reduces the impact of WannaCry by ensuring data can be restored without needing to pay a ransom.
- **Test Backup Restoration**: Regularly test backup restoration processes to confirm data can be reliably recovered if a ransomware attack occurs. This includes checking for WannaCry infection on backup copies to prevent reinfection during restoration.

7. Logging and Monitoring

- **Centralized Logging**: Implement a centralized logging solution, such as a Security Information and Event Management (SIEM) system, to collect and analyze logs from

endpoints, network traffic, and access control systems. This enables faster detection and response to WannaCry indicators.

- **Continuous Monitoring**: Set up continuous monitoring for abnormal network traffic patterns, file changes, or high-volume file encryption activities. Create alerts for unusual behavior on SMB protocols, which is a sign of WannaCry or similar ransomware activity.

8. Email and Web Protection

- **Email Filtering**: Deploy advanced email security to filter out phishing emails and malicious attachments that could introduce WannaCry or similar threats. Enable sandboxing to analyze suspicious attachments before delivery to end users.
- **Web Content Filtering**: Block access to known malicious websites associated with WannaCry, as well as IP addresses linked to ransomware operations, to prevent initial infection and limit command-and-control (C2) communication.

- **DETECT**
  - **Anomaly Detection**: Set up SIEM (Security Information and Event Management) systems to monitor and alert on unusual SMB traffic or access attempts. Set up an Intrusion Detection System to see abnormal network traffic.
  - **Log Analysis**: Monitor logs for WannaCry-related activity, like connections to the kill switch domain or the presence of suspicious executable files (e.g., wannacry.exe).
  - **Threat Intelligence**: Utilize threat intelligence feeds to stay updated on WannaCry-specific IOCs and signatures and proactively search for these within network data.

- **RESPOND**

Incident Response Plan: Develop an incident response playbook specifically for ransomware, detailing how to isolate infected systems and communicate with stakeholders.

The NIST Incident Response Framework is structured around four critical phases: Preparation, Detection and Analysis, Containment, Eradication and Recovery, and Post-Incident Activity. Each of these steps plays a vital role in building a robust defense against ransomware attacks.

1. Preparation

Goal: To build a strong foundation for incident response through policies, training, and resources to detect and respond effectively.

Actions in Preparation:

- **Maintenance\Patch Management**: Establish a *patch management policy* that ensures timely updates for software, operating systems, and applications. *Vulnerabilities like the SMB protocol exploit, which WannaCry used (EternalBlue), could have been mitigated if patches were applied. (*The vulnerabilities were known, and the exploit was there…)
- **User Training and Awareness**: *Conduct regular training on phishing and email security* to help users recognize malicious emails or attachments, as ransomware is often spread through social engineering tactics.

- **Data Backup Strategy**: Implement a frequent and secure backup system to prevent data loss from ransomware attacks. These backups should be tested regularly and stored offline or in a protected environment. The **3-2-1 backup strategy** is a widely recommended approach to data backup that ensures strong data redundancy and resilience against data loss. It's designed to safeguard data by maintaining multiple copies across various storage types and locations. Here's what each part of the strategy means:

3 Copies of Data:
Keep three total copies of your data. This includes the original data plus two backups. Having multiple copies provides redundancy, so if one backup fails, others are still available.

2 Different Storage Types:
Store your backups on two different media types to reduce the risk of simultaneous failure. For example, one backup could be on an external hard drive, while the other is stored on a NAS (Network Attached Storage) or another digital medium.

1 Offsite Copy:
Keep one copy of the data offsite, away from the primary location. This protects your data from local disasters like fires, floods, or theft. This offsite copy can be stored in the cloud or in a physical location distant from the primary site.

Example
If a business has critical data on its main server, it might:

- Store one backup on an onsite NAS,
- Keep another on an external hard drive stored elsewhere onsite,
- And keep a third backup offsite in a secure cloud storage provider.

This 3-2-1 strategy is simple yet robust, providing a strong line of defense against data loss from hardware failure, human error, or disasters

Impact on WannaCry Prevention:
Proper preparation, particularly through a strong patch management policy, could have closed the SMB vulnerability that WannaCry exploited. Employee training and robust data backups would have further strengthened defenses, limiting the spread and impact of ransomware even if initial infection attempts succeeded.

2. Detection and Analysis

Goal: To quickly detect and analyze indicators of compromise (IOCs) to understand and respond to potential security incidents.

Actions in Detection and Analysis:

- **Intrusion Detection and Monitoring**: Deploy Intrusion Detection Systems (IDS) and other monitoring tools to flag unusual activity, such as sudden spikes in SMB network traffic, which was characteristic of WannaCry. In terms of IOCs, we could mention:
  - **Network Traffic**: High volume of SMB (Server Message Block) protocol traffic, typically on ports 445 and 139.

- **Suspicious Files**: Executables named tasksche.exe, wannacry.exe, @Please_Read_Me@.txt (ransom note), and .wnry file extensions on encrypted files.
- **Malicious IPs and URLs**: Communication with certain IP addresses or URLs known to be associated with the WannaCry Command and Control (C2) infrastructure.
- **WannaCry Kill Switch Domain**: Attempted access to a specific "kill switch" domain (iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com) that, when registered, slowed the spread of WannaCry.

- **Threat Intelligence**: *Use threat intelligence feeds* to stay informed of recent vulnerabilities and attack vectors, like the *EternalBlue exploit, which was known prior to the WannaCry outbreak*.

- **Incident Prioritization**: Establish a process for prioritizing incidents based on potential risk to key systems and data, ensuring that critical assets are protected first.

  Impact on WannaCry Prevention: Early detection would have alerted teams to WannaCry's lateral movement within the network. Monitoring and threat intelligence could have flagged anomalous traffic patterns linked to ransomware activity, allowing response teams to initiate containment before the ransomware spread widely.

  Mitigation \ Containment Strategy: Quickly isolate infected machines from the network to prevent the lateral spread of ransomware through SMB.

  - **Isolate Infected Systems**: Identify all systems displaying WannaCry indicators of compromise (IOCs) and immediately disconnect them from the network. This prevents the ransomware from moving laterally across SMB (Server Message Block) protocol vulnerabilities.
  - **Block SMB Traffic**: Temporarily disable SMB services (ports 445 and 139) across the network until you confirm that all devices are patched and free of infection. This mitigates WannaCry's primary method of spread.
  - **Segmentation**: Use network segmentation to separate critical systems and limit potential spread to specific network segments. This minimizes impact, allowing isolated containment.
  - **Quarantine Affected Devices**: Move any devices with confirmed IOCs to a segregated VLAN or isolated containment zone. Ensure no device is returned to the main network without thorough inspection and confirmation of remediation.
  - **IOC Investigation**: Actively search for and investigate WannaCry IOCs, like unusual file names and encrypted files, across all systems.
  - **Implement Access Control and Temporary Policies**
    - **Restrict User Access**: Temporarily limit administrative and privileged user access to critical systems to prevent accidental reinfection or spread.
    - **Monitor for Lateral Movement**: Set up monitoring and alerting on suspicious activities, such as unauthorized attempts to access SMB services, unusual file changes, or connections to known WannaCry-related domains.

- **RECOVER**
  The Recovery phase of the NIST Framework in response to a WannaCry incident focuses on restoring normal operations, securing systems, and implementing lessons learned to enhance resilience. This how this phase would look like in the WannaCry incident:

1. **System Restoration**
   - **Restore from Secure Backups**: Rebuild affected systems using secure, offline backups taken before the WannaCry infection. Validate these backups to ensure they are uninfected, and follow a staged restoration approach, prioritizing critical systems.
   - **Reinstall Compromised Software**: If backups aren't available, reinstall the operating system and software on affected devices to eliminate any residual malware.
   - **Data Recovery**: If some data wasn't backed up and was encrypted by WannaCry, assess whether it's feasible to recover without paying the ransom. Use any available decryption tools (if applicable), though success may vary.
2. **Infrastructure Patching and Hardening**
   - **Apply Patches (MS17-010)**: Ensure that all devices, including restored and unaffected systems, have the critical MS17-010 patch applied to prevent exploitation of the SMB vulnerability.
   - **Update and Secure Software**: Confirm that all applications, operating systems, and firmware are up-to-date. Disable SMBv1 if not required by legacy systems, as this protocol is outdated and was a key vector for WannaCry.
3. **Improvement : Verify and Monitor System Stability**
   - **Test Restored Systems**: Thoroughly test each restored system for functionality and security, ensuring they perform normally and are free from residual infections.
   - **Activate Monitoring Systems**: Reinforce monitoring for unusual network traffic, specifically on SMB ports (445 and 139), and any WannaCry IOCs. Set alerts for any signs of reinfection or ransomware-related behavior.

Conclusion
The NIST Incident Response Framework provides a comprehensive and systematic approach that could have significantly mitigated, or even prevented, the impact of WannaCry. Through proactive preparation, timely detection, effective containment, and thorough post-incident reviews, organizations can safeguard critical assets against ransomware threats and continually evolve their security practices.

Submission Checklist

👉*Check off each of the features you have completed.* ***You will only be graded on the features you check off.***

Required Challenges

- ~~Item #1~~
- ~~Item #2~~
- ~~Item #3~~

Stretch Challenge

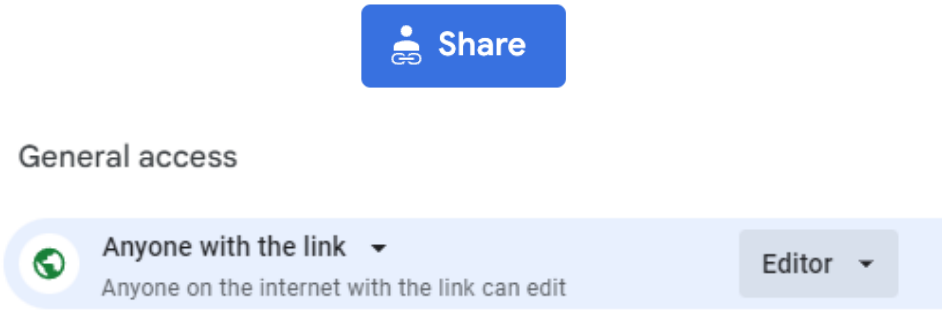
- ~~Bonus Task #1~~

- ~~Bonus Task #2~~

Tip: You can see specific grading information, including points breakdown, by going to the grading page on the course portal.

Submit your work!

Step 1: **Click** the Share button at the top of your screen double check that anyone with the link can edit.



Step 2: **Copy** the link to this document.

Step 3: **Submit** the link on the portal.