National College of Ireland

Project Submission Sheet

Student Name:	Matthew Browne		
Student ID:	x21174415@student.ncirl.ie		
Programme:	MSc/PGD in Cybersecurity	**Year:**	1
Module:	Business Resilience and Incident Management		
Lecturer:	Eugene McLaughlin MSc/PGD		
Submission Due Date**:**	4th December 2025		
Word Count:	6883		

I hereby certify that the information contained in this (my submission) is information pertaining to the research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.

ALL internet material must be referenced in the references section. Students are encouraged to use the Harvard Referencing Standard supplied by the library. Using other authors written or electronic work is illegal (plagiarism) and may result in disciplinary action. Students may be required to undergo aa (ral examination) if there is suspicion about the validity of their submitted work.

Signature: Matthew Browne

Date: 3rd December 2025

1. Please attach a completed copy of this sheet to each project (including multiple copies).
2. Projects should be submitted to your Programme Coordinator.
3. **You must ensure that you retain a HARD COPY of ALL projects**, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on a computer. Please do not bind projects or place in covers unless specifically requested.
4. You must ensure that all projects are submitted to your Programme Coordinator on or before the required submission date. **Late submissions will incur penalties.**
5. All projects must be submitted and passed in order to successfully complete the year. **Any project/assignment not submitted will be marked as a failure.**

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

AI Acknowledgement Supplement

Your Name/Student Number	Course	Date
Name: Matthew Browne Student Number: x21174415	MSc/PGD in Cybersecurity	03/12/2025

AI Acknowledgment

Name Of Tool	Description	Link
Not Applicable	Not Applicable	

Description of AI Usage

Not Applicable

Evidence of AI Usage

Not Applicable

Assessment Name	Business Resilience and Incident Management CA2
Student Name	Matthew Browne
Student ID	x21174415
Email ID	x21174415@student.ncirl.ie

Contents

1.0 Introduction Statement

For my PgD Cybersecurity my report will showcase two real life events which happened one at a global scale called “Nobelium” which was one of the most prolific cyber-attacks in the world targeting the SolarWinds breach which effected in excess of “34,000” (Microsoft Security, 2021) customers and vendors , and my second one is more at a local scale called “MTU” an academic university in Ireland who experienced a ransomware attack which brought down there academic operations back in “2021” (MTU, 2023). By using both I’m looking to showcase my depth of understanding for both cyber incidents and how one is distinctively different from the other “Nobelium” (Microsoft Security, 2021) being about stealth and reconnaissance and “Mtu” being about extortion and disruption. By doing a comparative study I’m looking at how I can apply my understanding for how organisations and governments can apply incident response techniques , recovery strategies and resilient techniques to defend against these attacks both in an “APT” (thorteaches.com, n.d.) and “Ransomware” (Accenture, 2025) scenario.

1.0 Question One

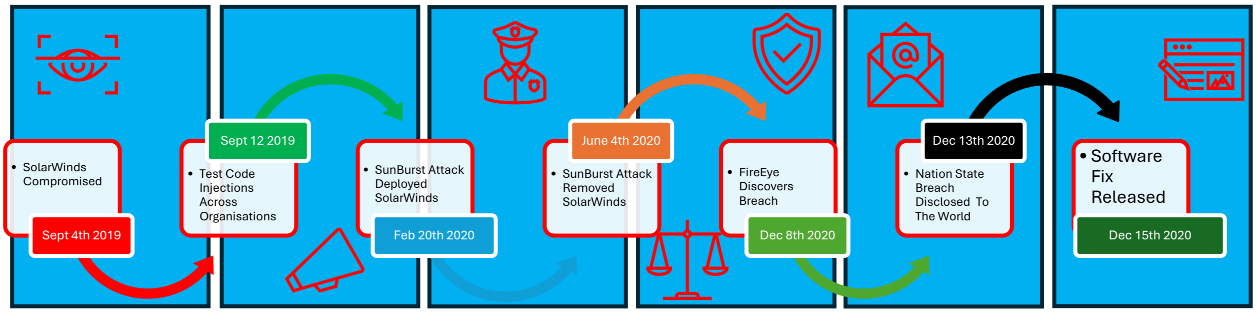
1.1 Risk Assessment and Identification of Threats

The Nobelium attack and threat actor’s showcased their abilities on the world stage by using an Advanced Persistent Threat ”APT” for short , essentially the vendor in this case which was SolarWinds was compromised due to malware which had been stored in a “DLL” file this had been part of a routine software update for the client which had been pushed out across the SolarWinds systems , this was part of a normal maintenance schedule often referred to as “Patch Tuesday” (wikipedia.org, 2023) where most organisations follow suit and update their systems against vulnerabilities and cve’s. The attack resulted in one of the most well-orchestrated reconnaissance attacks on the SolarWinds systems which yielded key takeaways of trade secrets and data theft from organisations globally , this highlighted the importance of understanding supply chain compromise with your vendors , in contrast to this Mtu experienced a cyber incident of the extortion variety (RTE, 2023) , this attack essentially looked more like a smash and grab which focused on bringing down systems in turn for a quick return on investment from the threat actors, the key difference here being was the “Nobelium” (Microsoft, n.d.)focused on long term espionage and the “Mtu” focused on financial reward both attacks resulted in disruption to services with Mtu being on the scale of locking out systems making them unavailable , encrypting systems and holding the university to ransom payment versus Nobelium’s incident which harvested data for collection purposes and then moving laterally across systems for maximum coverage. Both show us that the risk assessment profiles for the two attacks had very different motivators Nobelium being maximum impact slow gain with Mtu being fast impact and fast gain. (Microsoft Security, 2021)

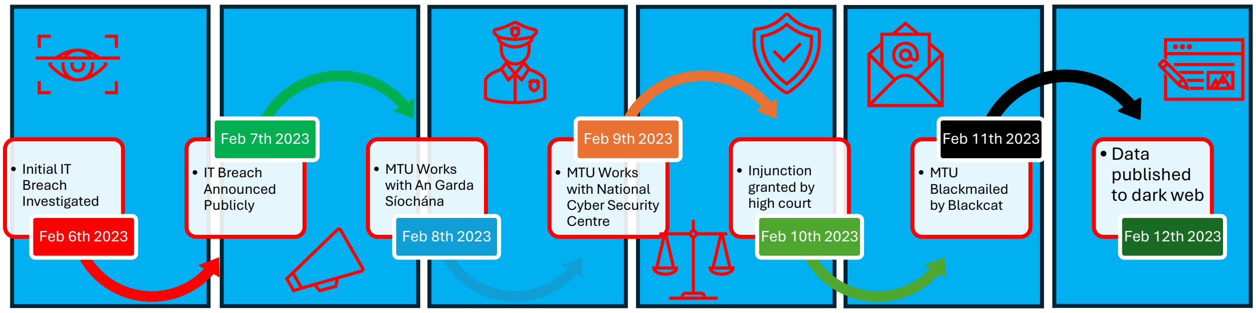
1.2 Impact on Business Operations

Looking at and reviewing the Nobelium attacks, I see that it impacted global supply chains, this resulted in a loss of confidentiality and integrity which was in line with the “CIA Triad” (ncyte.net, 2022), It also had a large exposure due to the sensitivity of the data and classification and the costs for incident response were huge as referenced by “John Lambert” from the Microsoft Threat intelligence centre (Microsoft Security, 2021) basing on the amount of teams that were involved”1000+” (Microsoft Security, 2021) . Due to the nature of the kind of attack which you can admit was stealthy this meant the data was being Ex filtered across months at a time with very little detections. In Nobelium’s case the impact on operations for months on end and visibility went unnoticed due to the recognisance but in reality, it was a large extraction of the privileged data which the attackers would later benefit from. Meanwhile when I look at Mtu they suffered from a loss of availability of systems again “CIA Triad” (ncyte.net, 2022) here as well the threat actor “BlackCat” (TheJournal, 2023) (Martin, 2023) essentially chocked their servers, workstations, firewalls and systems resulting in catastrophic business impacts to their immediate operations some of the classes got cancelled, there were delays to restoring systems and functionalities, internet access was down. All these elements across both scenarios shows us how cyber incidents can amalgamate into a litany of problems for organisations resulting in an operational crisis and a damage to reputation.

Nobelium Attack Journey (FireEye) (threatcop.com, 2022)


• SolarWinds Compromised
Sept 4th 2019
Sept 12 2019
• Test Code Injections Across Organisations
• SunBurst Attack Deployed SolarWinds
Feb 20th 2020
June 4th 2020
• SunBurst Attack Removed SolarWinds
• FireEye Discovers Breach
Dec 8th 2020
Dec 13th 2020
• Nation State Breach Disclosed To The World
• Software Fix Released
Dec 15th 2020

Ransomware Attack Journey (MTU) (Sheehy, 2023)


Initial IT Breach Investigated
Feb 6th 2023
Feb 7th 2023
IT Breach Announced Publicly
MTU Works with An Garda Síochána
Feb 8th 2023
Feb 9th 2023
MTU Works with National Cyber Security Centre
Injunction granted by high court
Feb 10th 2023
Feb 11th 2023
MTU Blackmailed by Blackcat
Data published to dark web
Feb 12th 2023

1.3 Integration into Incident Response Plan

An effective and beneficial incident response plan (Nist.gov, 2018) particularly in the boardroom, organisations often look at the how the IR Plan should be embedding controls against advanced persistent threats and ransomware part of this is the incident response life cycle model this is usually part of the "7 phases" (TitanFile, 2022). For Nobelium if there had been any form of Third-Party Assurance (Microsoft, n.d.), Code Signing as part of the Software Development Lifecycle (SDLC) or even some vendor monitoring within the Preparation Phase of the Nist framework (Anon., 2025) this would have helped. For MTU if they had implemented some form of ransomware specific playbooks (Microsoft, 2025), automated isolation procedures or even some offline backups in the containment and recovery stage they two may have recovered faster. The one discrepancy that both had were they weren't prepared for an attack, and they certainly didn't have any detection & analysis playbook ready to go for eradicating any protentional cyber threat, it's clear that both required an (IDS) and (IPS) (okta.com, 2024) or an endpoint detection and response system (EDR) (Crowd Strike, 2025) to protect their systems both internal and externally.

1.4 Recommendations for IR Plan Tailoring

Tailoring an organisations incident response plans (atlassian.com, 2010) is key to utilising insights taken from tooling such as Siem and Log sources , organisations should always go back to basics with this some preventative techniques these can include implementing "Zero Trust Architectures" (Microsoft, 2024) and limiting access to areas in our ecosystem like following the "Principle of least Privilege" (Microsoft, 2023) in both scenarios this would have prevented "lateral movement" (Microsoft, 2023) across systems for MTU and SolarWinds. Some other preventative techniques can include implementing Multi-Factor Authentication (Mfa) (Microsoft, 2024) for short and the implementation of Privileged Access Management Solutions (Pam) (Microsoft, 2025) for short an example of this might have been a "Bastion" (Microsoft, 2025) for Tier level access to critical infrastructure like the Active Directory Servers (AD) for short in MTU's case and the Active Directory Federation Servers (ADFS) (Microsoft Security, 2021) in short for SolarWinds. Another way of protecting the organisations in terms of incident response would have been to conduct tabletop exercises (Crowdstrike, 2025) (Crowdstrike, 2024) or simulations with red and blue teams, similarly, replicating an actual attack in a learning or dev environment which would have provided for some additional context and exposure for when teams experience an actual attack providing some lessons learned exercises. Lastly one other thing both organisations could have implemented was a "Risk Register" (hyperproof.io, 2021) by having this they could continually update their business impact assessments to align with their most critical assets and priorities on what was important to the business to close gaps identified to reduce their attack surface across systems also known as a "Gap Analysis" (Microsoft, 2024).

2.0 Question Two

2.1 Implications of Business Continuity Planning

The BCP should be seen as more than a lifeline for organisations without an adequate "BCP" (investopedia.com, n.d.) organisations are left with a large recovery time objective ("RTO") (druva.com, 2021) for short if the plan is inadequate or not thought out it can demonstrate a negative financial impact on the business, and possibly legal and regulatory repercussions for the organisation. When I looked the at the Mtu ransomware recovery procedures I noticed from the time it to identify the ongoing attack to the time it took to restore from it this took weeks due to Mtu not having any form of isolated backups from the rest of the systems alongside in ability for the university to be able to implement an incident response plan , the availability of "playbooks" , "runbooks" (squadcast.com, 2023)and standard operating procedures (SOP) (techtarget.com, 2021) for short these form of incidents had not been tested or scenarioized (MC Gowran , 2023) although on the flip side when I look at SolarWinds customers and the victims from the Nobelium attack they did have Bcp's available but suffered due to a weakness in the supply chain which hadn't been discovered. This shows us that the attack surface "BIA" (techtarget.com, n.d.) should extend far beyond the immediate internal networks and extend out to external and vendor connections.

2.2 Critical Appraisal of Business Resilience

The "ISO 22316" (Anon., 2020) defines an organisations resiliency (Anon., 2020)as having the ability to adapt and change based on the events and disruptions being presented at any given time , when reviewing Nobelium's case It should be noted that despite the compromise (Integrity) of the Solar Winds software and the injected malware business continuity was still at the heart of their operations despite the compromise whereas in Mut's case they looked to preserve and bring the delivery of their education and services to students outside of the universities eco system. Where both organisations would have benefited and Mtu certainly did having an alternative channel for delivery of services or even another cloud provider availability (High Availability) (wikipedia.org, 2020) configuration this would have created a redundant infrastructure allowing both organisations to at least attempt recovery or continuity of services. For both organisations if they had implemented these safeguards or guard rails they would have minimised their disruptions in comparison to not having a BCP in place.

2.3 Application of Theoretical Concepts to Scenario

Reviewing the "ISO 22301 (isms.online/, 2020)Business Continuity Management Systems Process" (isms.online, 2020) this looked at identifying and prioritising threats based on their criticality dependent on the systems and the recovery time objectives "NIST SP 800-34" (Anon., n.d.) / on the other hand this looked at contingency planning in particular "confidentiality, integrity and Availability" if we think about this realistically it all revolves around the "McCumber Cube model" (ncyte.net, 2022) which has the CIA Triad principles built into it. applying these to Mtu's scenarios both of these frameworks would prioritise maintaining key services e.g. student record databases which were internal and learning platforms which were external and then in the Nobelium scenario the purpose around business continuity planning would extend around the integrity of the suppliers systems and the mechanisms for updating them securely (SDLC) (wikipedia.org, 2019) Lifecycle showing me that continuity around the supply chain security is a key part of this process.

2.4 Quality of Justifications and Examples

For both scenarios I was able to articulate and understand that Nobelium showed me there were weaknesses in the risk management approach and identification approaches for external vendors while for Mtu it showed an inability to continue on operations due to the ransomware locking up systems effectively showing issues with standard operation procedures and translating them from paper to digital format a way in which both organisations could have done and eradicated the risk with "Azure Policy" (Microsoft, 2024) if they so wished. With Azure policy or AWS equivalent the organisations could have accessed the compliance around the assets and ensured risk mitigation techniques at a management level this showed me to be resilient both organisations required a continues validation in their approaches for recovery and not just documentation, in Mtu's case lack of documentation and procedure.

2.5 Question Three

2.6 Identification of Key IR Roles and Responsibilities

To respond appropriately to an Incident an organisation must a should have an incident response capability weather this is internal, external or through consultancy. The purposes of the Incident Response Lifecycle are to have a formal response and preparatory procedure ready should an organisation but subject to a cyber incident this allows them to protect themselves against adversaries. Many organisations follow the Nist framework (Nist.gov, n.d.) for this which has five phases of incident response, they are identify, protect, detect, respond and recover associated with these phases some of the incident response team key roles are.

Role Name	*Responsibility*
Legal Council	*Essentially this person is responsible for ensuring all individuals comply with legal responsibilities for their roles in the company, they will normally review any documentation and or compliance actions in accordance with applicable laws, tthey'll report directly into CTO, CEO, CISO.* *They will hold a Juris Doctor JD and Possibly a PhD NFQ10 alongside 10 years of legal experience.*
Incident Response Manager	*Essentially this person you could say is the PM Project Manager on the incident, there you're go to for managing the team and the contact between senior stakeholders.* *Normally they will hold a PgD NFQ9 with at least 10 years' experience alongside some vendor neutral certifications like ISC2 CISSP, CompTIA CASP+ or ISACA CISM.*
Security Analyst	*Essentially this person will be the engineer who looks after the analysis of logs within systems like Azure Aws and GCP and the alerting mechanisms, they'll attempt to priorities alerts of interest and may recommend some eradication and containment strategies,* *Normally they'll hold a BSc NFQ8 with at least 1-5 years' experience alongside some vendor neutral certifications like ISC2 SSCP, CompTIA CySA+, or Ec-Council ECSA*
Forensic Analyst	*Essentially this person will be a forensic specialist. Their job will be to preserve evidence, analyse logs, report and document the findings of examined artifacts using software like EnCase or Autopsy and support the courts in any chain of evidence requirements.* *Normally they'll hold a BSc NFQ8 with at least 1-6 years' experience alongside some vendor neutral certifications like ISC2 CCSP, CompTIA Cloud+, EC-Council CHFI*
Threat Hunter	*Essentially this person will be an Ethical Hacker or a Pen tester, they will look for threats, identify them and respond to threats appropriately as needed, they will create required rules and policies to protect the environment.* *Normally they'll hold a BSc NFQ8 or PgD NFQ9 with at least 2-7 years' experience alongside some vendor neutral certifications like ISC2 CGRC, CompTIA SecurityX, OSCP/OSCP+ or EC-Council CEH*

IT Support and or Systems Administrator	*Essentially these individuals will be supporting any IT operations changes or administrative changes on the systems both in cloud and on premise, this can include patching systems, restoring backups, implementing baselines and isolating systems.* *Normally they'll hold an Associate BSc NFQ7 with at least 1-6 years' experience alongside some vendor neutral certifications like Microsoft SC-100, CompTIA A+ N+ Security+, ISC2 CC, SSCP, Ec-Council CCT.*
Communications Officer	*Essentially this person will be required to liaise with Management, the press and speak with the Public for any internal and external communications about the incident, they would also be required to look after all Pr for the company* *Normally they'll hold a BSc NFQ8 in Communications with at least 8 years' experience.*

Certificate Vendor References

CompTIA	*SecurityX* , (CompTIA.Org, 2024) *CySA+* , (CompTIA.Org, 2023) *Cloud+,* (CompTIA.Org, 2024) *A+,* (CompTIA.Org, 2025) *Network+,* (CompTIA.Org, 2025) *Security+,* (CompTIA.Org, 2025)
ISC2	*CISSP* (ISC2.Org, 2019) *SSCP* , (ISC2.Org, 2019) *CCSP,* (ISC2.Org, 2019) *CGRC,* (ISC2.Org, 2019) *CC,* (ISC2.Org, 2025)
ISACA	*CISM,* (ISACA.org, 2020)
EC-COUNCIL	*ECSA,* (EC-Council, 2025) *CHFI,* (EC-Council , 2025) *CEH,* (EC-Council, 2025) *CCT,* (EC-Council, 2025)
OFFSec	*OSCP/OSCP+* (OffSec, 2025)
Microsoft	*SC-100,* (Microsoft, 2025)
QQI	*QQI Qualification Levels NFQ 5,6,7,8,9,10* (QQI, 2025)

All these roles (wiz.io, n.d.) would have been part of the strategic strategy which both FireEye and Microsoft would have in place alongside as part of their incident response plans and Mtu's efforts would have contained similar with the local coordination they had between IT, Management, An Garda Siochana. (RTE, 2023)

2.7 Prioritization of Roles Based on Incident Impact

Reviewing the Nobelium attack style it was distinctively different to the attack on Mtu, Forensic analysts and Threat hunting would have been a prioritised as the nature of the attacks were APT's (Microsoft Security, 2021) for Mtu's attack which was ransomware the university would have prioritised Incident Response Managers and IT Support staff and Administrators to bring systems back online for the containment and recovery from the ransomware attack both very different scenarios as one required extensive investigations and the other required fast incident response this really does depend on the incident type and the impact the incident has on the organisation e.g. espionage versus disruption this really also depends on the resource availability and budgets as well for organisations.

2.8 Communication Strategies within the IR Team

Strategies and sequencing around communication within an organisational context for incident response should highlight the type of Sop's around communicating an incident across teams this is where having an "incident response communication plan (EC-Council, 2024)" built into your disaster recovery plan is key , this allows an organisation or an analyst to escalate as deemed necessary within this it should be stipulated the communication methods for when a system is compromised this could stipulate communications methods over email , phone , text messaging services , forms , boards and so on built into this should be a method of communication for where systems may be compromised by a bad actor so "out of band channels" or methods of communications through none standard channels should be established prior to an incident , a key communication component for in incident is called a "SitRep Reports" (Goo, 2024) this allows for incident response teams to cover the key questions new individuals and analysts may have who are supporting the incident recovery or mitigation plans without the need to interrupt the meting while everyone gets acquainted with the situation.

2.9 Practical Application and Relevance of Strategy

Ways in which organisations can but their process and procedures into a practical test mechanism would be through tabletop exercises simulating scenarios just like Nobelium and Mtu can help organisations and incident response teams to strengthen and coordinate their techniques for possible lessons learned exercising. With incident response (Goo, 2024)you have two options you could implement it based on the Nist incident response lifecycle or "OODA Loop" in contrast to Nist OODA stands for "Act, Observe, Decide, Orient" (nist.gov, 2010)this was developed by the "John Boyd" which was used by the Us Air Force for dealing with live incident response in real environments , both options Nist and OODA Loop serve specific purposes with Nist being more geared towards the private sector.

3.0 Question Four

3.1 Understanding of Threat Intelligence Value

When reviewing threat intelligence and forms organisations should be thinking of the types of indicators of compromise and how they can streamline criticality of the risk remediation e.g. understanding identification of them via cve's , the length of time they have to address the vulnerabilities adding them to risk registers and databases for tracking purposes often the vulnerabilities need to be patched or mitigated these essentially go back to thinking about how an organisation or university can defend their systems against threat actors through intelligence sharing and what type of actionable insights they get from these. When I looked at the Nobelium approach by Microsoft and FireEye, I was able to see that sharing the indicators of compromise from Microsoft and FireEye allowed both organisation to be able to identify the threats faster this brought a threat intelligence clarity value piece as they were sharing with each other to known values which allowed them to map the attack paths , when I look at Mtu they didn't have the same availability in terms of database and direct support with Microsoft rather everything was through The National Cyber Security Centre (NCSC) (Ncsc, n.d.) , if Mtu had known the type of Ransomware in existence this could have helped with strengthening their defences in the long term other tools like the "Inform Assessment Tool" (Mitre.org, n.d.) from Mitre could have also helped with assessing their threat maturity.

3.2 Development of a Threat Hunting Strategy

Organisations like FireEye and SolarWinds should look at using tools like the "Inform Assessment" to be able to leverage Mitre Attack mappings Mtu would have benefited also from this being able to map back specific threats, organisations and universities should also look to Siem tooling like those provided by Microsoft such as Defender , Sentinel , Defender Xdr/Cloud or perhaps some third party tools like IBM , Qradar , Splunk all tools mentioned provide teams and organisations with abilities to be able to detect breaches before they and correlate the data being presented in the tools by ingesting and categorising it based on threat type , criticality and known bad actors. A good example of this would be having conditional access rules for Matthew saying Matthew cannot log into office 365 email from China or other impossible locations like Africa or Australia, but suddenly Sentinel is seeing logins from China and other banned countries having a proper detection Siem such as Sentinel and Response such as Defender Xdr or Cloud help with mitigating the threat. When I looked at the Mtu the same could have been said here but with a clearer focus on indicator of compromises for ransomware and privilege escalation in which a product like Sentinel and Defender could have helped prevent the privilege escalation and blocking it at the source two distinctive scenarios where both Siem and Soc tooling would have helped FireEye and Mtu with preventing and defending against attacks.

3.3 Application to Security Operations within IR Framework

When thinking about threat hunting immediately, I think what stage of the Nist framework and how Siem tooling like "Microsoft Sentinel" and "Splunk (splunk, 2025) and Qradar (qradar, 2025)" can enhance the ability of detecting and responding to the threats, as we know threat hunting should align alongside detection / analysis stage of the Nist framework what this allows organisations like FireEye and Mtu to navigate the landscape and have a real time visibility to support the containment and eradication of the threats in the environment. In the Nobelium's case this real time visibility helped FireEye and Microsoft identify threats, correlate them into an attack chain and helped reduce the overall time to detect for immediate and future requirements , Mtu could have benefited from this capability had they implemented a proper Siem tooling and was ingesting the telemetry into one or at least recording the logs would have helped to identify the attacks at an earlier stage in the kill chain.

3.4 Depth of Analysis and Justification of Strategy

What I learned from the incident with both FireEye and Mtu was that if organisations shared there intelligence updates this would have helped to accelerate the level and speed at which FireEye and Mtu spent and learning about the incidents , this threat intelligence sharing becomes a pinnacle piece of identifying the entry into the systems and the exfiltration of data and assets out of the systems. It's also evident that because Mtu didn't have any formal practice for monitoring threats this showed a gap in their ability to monitor incidents. The key common denominator that both scenarios have is that if they had a layered and hybrid defence strategy implementing Siem tooling, Intrusion prevention systems, zero trust frameworks and intelligence sharing networks these all would have allowed for an earlier detection and response to both threat types resulting in quicker erudition and recovery.

4.0 Question Five

4.1 Evaluation of Incident Response Posture

As an organisation knowing your Incident Response posture and your risk appetite are key in understanding your readiness toward potential incidents having a proper detection capability like a Siem tooling such as Microsoft Sentinel, or Splunk aids in your ability to identify real time events that occur, your ability to be able to respond and recover from said incident will depend your defensive measure like having an Av or Endpoint product available within your environment alongside any additional security measures like governance policies , firewall rules , impossible travel alerts and so on, Fire Eyes scenarios showed that there were weaknesses in the identity and access management piece as an individual outside of the organisation was able to add another device without any form of enrolment or device management this showed that having visibility across the infrastructure including on premise , cloud and mobile are key defensive techniques that should be implemented by all organisations. Whereas when we compare this with Mtu we see that their issues were around the recovery of their systems due to no proper testing in their backup systems this resulted in pressure in how they handled the communication between staff students and the public. (The Irish Times , 2023)

4.2 Identification and Analysis of Improvement Areas

As part of the Nist Framework were taught to conduct a "Post Incident Response" activity this helps with understanding the types of lessons which can be learned from the gaps identified at the end of resolving and coming out of an incident from this were able to identify some of the metrics that matter the most or should be prioritised for the next time there is a potential breach it's not something that should ever be ignored as it provides a value add for closing out an incident properly key metrics which we could have collected from both the Mtu and FireEye incident were Mean time to detect and Mean time to respond "(MTTD) and (MTTR)" in short this allows an organisation to calculate their containment rate for an incident and helps build out future capabilities and requirements to improve upon this rate. Possibly adding additional auditing capabilities like additional reviews of incidents in Soc and Siem tooling may help to align closer with Iso/Iec 27035 standards. Implementing proper "tabletop exercises" (Crowdstrike, 2025) with red, blue and purple team (EC-Council, 2024) simulations is key to identifying gaps and fortifying security products and architectures as it helps teams to learn from each other and implement additional components to enhance the overall security posture as new vulnerabilities come to light.

4.3 Recommendations for Enhancing IR Capabilities

After reviewing all the videos from Microsoft Security (Microsoft Security, 2021)and reading through the Microsoft report (Microsoft, n.d.) it highlighted a multitude of gaps in Fire Eyes supply chain vulnerability management systems , it highlighted a need for more oversight and governance around there external vendors and contract management integration points , it also highlighted a need to audit logins and record token management for their ADFS Servers possibly implementing Pam systems as an intermediate security measure to prevent standard user account logins from elevating their permissions previously like we use to do with active directory security groups bringing this capability into azure and utilising roles with just in time access is critical requirement for Fire Eye. Other possibilities include tiering the access to these systems, which highlighted the need for long term telemetry which needs to be ingested into Siem tooling like Microsoft Sentinel. The lessons learned from this breach showed me that telemetry across systems and correlation between systems is a must have for any organisation in putting together the attack story and chains , Whereas with Mtu there discrepancies highlighted more basic and foundational components of the zero trust principle which were not implemented like backup verification's "RTO and RPO" (druva.com, 2021) network segmentations like VNets and VLan's and proper incident response communications for teams and stakeholders. All of this informs me that monitoring tasks across azure and on premise, recovery procedures for backup solutions and governance across platforms have not been implemented correctly.

To enhance and remediate the gaps found as part of the lessons learned both Fire Eye and Mtu should implement a series of measures which include identity-based intrusion and detection systems like Sentinel , Splunk and Azure auditing , higher penalties for none compliance with organisational policies around supply chain assurance (pwc.com, 2023) should be implemented for external vendors a case can be made for recorded backup testing and validation walk throughs involved as an exercise for testing backup restorations the results should be audited and recorded with write ups accompanying these for ransomware protection Mtu specifically should look at resource locks in azure and the implementation of immutable backup options should be set to on both organisations should look at completing a maturity assessment in line with the "Nist CSF 2.0 ". (Nist.gov, n.d.) Lastly both organisations should look at implementing a single pane of glass product like deploying "Security Orchestration automation and Response" capability (Soar) (Microsoft, 2025)for short this will help with the containment of ransomware or malware in their environment.

4.4 Clarity and Relevance of Conclusions

My report which looked at two very different attack techniques showcased how a weakness in the supply chain for a vendor like SolarWinds /FireEye had a knock on effect across customers at a global scale this forced FireEye to re-evaluate their maturity around incident response and the practices they put in place to detect and prevent a privilege escalation attack through malware deployment across systems which resulted in a stole Azure ad token (Microsoft Security, 2021) , this highlighted an exposure for SolarWinds in there code for their agent deployment , The lack of governance around the controls and backup regression testing for Mtu resulted in extended delays to restoration procedures in there backup systems. Both results damaging the organisations reputations resulting in a lack of trust against the organisation with the public and customers. It also highlighted understanding your security posture, maturity levels and risk appetite are key to detection, prevention and eradication of malware and ransomware, if both your incident response maturity and organisation security posture are scoring low or non-existent this will affect the overall resilience scoring across systems.

As an organisation knowing your vendors and assessing your supply chain risk is a key component this should always be included as part of your risk assessment and overall management strategy scoring vendors helps with identifying gaps in your strategy. Weakness in the vendor supply chain resulted in an unknown vulnerability leaving FireEye open to exposure, while Mtu's scenario should a lack of governance around backup controls and auditing both scenarios being catastrophic, this highlights the important of organisations translating there business requirements into their chosen cloud provider in this case Azure , visualising the policies using Azure Policy (Microsoft, 2024) and tools like draw.io would have helped both organisations to become more aware of their shortcoming. The result for both being a lack of protection around open vulnerabilities and lack of understanding around the risks.

The component of continues learning and education around cyber hygiene is another topical piece here if your organisation is not continuously learning, creating collaborations across exercises and staying informed through information sharing forms and database on the latest threats this can inadvertently lower your security posture, frameworks like "Csf" "Nist 2.0", "Iso 27305" all provide for enhancements to an organisations implemented controls and sop's these frameworks help organisations to measure there compliance with best practices (tcm-sec.com, 2024) (Nist.gov, n.d.) , it also enables them to identify shortcomings in there approaches , both Mtu and FireEye should opt into some of the information sharing communities as this will allow them to strengthen their intelligence capabilities within their systems for cloud and on premise.

The breadth and depth of both attacks while distinctively different show us as cyber professionals the comparative and narrative while both different share common issues which are their resilience is dependent on their understanding of the attack surface in their organisation, this extends beyond their immediate internal systems and perimeter's this expands out as far as their vendors.

Every data point should be considered for risk mitigation and prevention techniques. The key concept that keeps coming across here is that implementing a zero-trust strategy following "Microsoft cybersecurity reference architecture" (MCRA Framework) (Microsoft, 2024) with business continuity and resilience testing should be considered as a critical priority for any organisation doing this will allow organisations to identify detect and respond appropriately to mitigate both known and unknown risks before they result in fatal disruptions to their operations (databank.com, n.d.) by following Microsoft best practice guidelines (thorteaches.com, n.d.) (Microsoft, 2025), regulatory Frameworks , proper monitoring and soc solution implementation runbooks organisations can implement a cycle of continues learning allowing them to mitigate future threats which in turn positions them to prevent further disruptions this also allows organisations to instil confidence with their board and teams for a secure resilient infrastructure.

References

Accenture, 2025. https://www.rvc.ac.uk/lisd/office-365-account/ransomware. [Online]
Available at: https://www.rvc.ac.uk/lisd/office-365-account/ransomware?gad_source=1&gad_campaignid=23020487924&gbraid=0AAAAADitEfqQPebnUahFoVoIfh3x-kOBg&gclid=EAIaIQobChMInYnH3qzskAMVaKVQBh3F5Aj0EAAYASAAEgI2ovD_BwE
[Accessed 18 November 2025].

Anon., 2020. iso-22316-organizational-resilience/. [Online]
Available at: https://www.globalsuitesolutions.com/iso-22316-organizational-resilience/
[Accessed 12 November 2025].

Anon., 2025. NIST.SP.800-61r3.pdf. [Online]
Available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r3.pdf
[Accessed 13 November 2025].

Anon., n.d. NIST.SP.800-61r3.pdf. [Online]
Available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r3.pdf
[Accessed 12 November 2025].

atlassian.com, 2010. incident-communication. [Online]
Available at: https://www.atlassian.com/incident-management/incident-communication
[Accessed 12 November 2025].

CompTIA.Org, 2023. cybersecurity-analyst. [Online]
Available at: https://www.comptia.org/en-eu/certifications/cybersecurity-analyst/
[Accessed 13 Nov 2025].

CompTIA.Org, 2024. CLOUD. [Online]
Available at: https://www.comptia.org/en-eu/certifications/cloud/
[Accessed 16 Nov 2025].

CompTIA.Org, 2024. securityx. [Online]
Available at: https://www.comptia.org/en-eu/certifications/securityx/
[Accessed 17 Nov 2025].

CompTIA.Org, 2025. a. [Online]
Available at: https://www.comptia.org/en-eu/certifications/a/
[Accessed 13 Nov 2025].

CompTIA.Org, 2025. network. [Online]
Available at: https://www.comptia.org/en-eu/certifications/network/
[Accessed 13 Nov 2025].

CompTIA.Org, 2025. security. [Online]
Available at: https://www.comptia.org/en-eu/certifications/security/
[Accessed 17 Nov 2025].

Crowd Strike, 2025. endpoint-detection-and-response-edr. [Online]
Available at: https://www.crowdstrike.com/en-us/cybersecurity-101/endpoint-security/endpoint-detection-and-response-edr/
[Accessed 12 November 2025].

Crowdstrike, 2024. red-team-blue-team-exercise/. [Online]
Available at: https://www.crowdstrike.com/en-us/services/prepare/red-team-blue-team-exercise/
[Accessed 14 November 2025].

Crowdstrike, 2025. prepare/red-team-blue-team-exercise/. [Online]
Available at: https://www.crowdstrike.com/en-us/services/prepare/red-team-blue-team-exercise
[Accessed 17 November 2025].

databank.com, n.d. continuous-operations-the-critical-role-of-redundant-infrastructure-in-data-centers. [Online]
Available at: https://www.databank.com/resources/blogs/ensuring-continuous-operations-the-critical-role-of-redundant-infrastructure-in-data-centers/
[Accessed 17 November 2025].

druva.com, 2021. understanding-rpo-and-rto. [Online]
Available at: https://www.druva.com/blog/understanding-rpo-and-rto
[Accessed 12 November 2025].

EC-Council , 2025. computer-hacking-forensic-investigator-chfi/. [Online]
Available at: https://www.eccouncil.org/train-certify/computer-hacking-forensic-investigator-chfi/
[Accessed 17 Nov 2025].

EC-Council, 2024. ethical-hacking/red-team-careers-skills-jobs/. [Online]
Available at: https://www.eccouncil.org/cybersecurity-exchange/ethical-hacking/red-team-careers-skills-jobs/
[Accessed 12 November 2025].

EC-Council, 2024. what-is-incident-response. [Online]
Available at: https://www.eccouncil.org/cybersecurity-exchange/incident-handling/what-is-incident-response/
[Accessed 12 November 2025].

EC-Council, 2025. certified-cybersecurity-technician-certification. [Online]
Available at: https://www.eccouncil.org/train-certify/certified-cybersecurity-technician-certification/
[Accessed 15 Nov 2025].

EC-Council, 2025. certified-ethical-hacker-ceh. [Online]
Available at: https://www.eccouncil.org/train-certify/certified-ethical-hacker-ceh/
[Accessed 16 Nov 2025].

EC-Council, 2025. ecsa-grandfathering.eccouncil.org. [Online]
Available at: https://ecsa-grandfathering.eccouncil.org/
[Accessed 17 Nov 2025].

Goo, P., 2024. incident-response-sitreps. [Online]
Available at: https://blog.petegoo.com/2024/03/13/incident-response-sitreps/
[Accessed 12 November 2025].

Goo, P., 2024. incident-response-sitreps. [Online]
Available at: https://blog.petegoo.com/2024/03/13/incident-response-sitreps/
[Accessed 12 November 2025].

hyperproof.io, 2021. resource/risk-register-key-benefits. [Online]
Available at: https://hyperproof.io/resource/risk-register-key-benefits/
[Accessed 12 November 2025].

investopedia.com, n.d. business-continuity-planning.asp. [Online]
Available at: https://www.investopedia.com/terms/b/business-continuity-planning.asp
[Accessed 14 November 2025].

ISACA.org, 2020. cism. [Online]
Available at: https://www.isaca.org/credentialing/cism
[Accessed 17 Nov 2025].

ISC2.Org, 2019. CCSP. [Online]
Available at: https://www.isc2.org/certifications/ccsp
[Accessed 15 Nov 2025].

ISC2.Org, 2019. CGRC. [Online]
Available at: https://www.isc2.org/certifications/cgrc
[Accessed 16 Nov 2025].

ISC2.Org, 2019. CISSP. [Online]
Available at: https://www.isc2.org/certifications/cissp
[Accessed 16 Nov 2025].

ISC2.Org, 2019. SSCP. [Online]
Available at: https://www.isc2.org/certifications/sscp
[Accessed 17 Nov 2025].

ISC2.Org, 2025. CC. [Online]
Available at: https://www.isc2.org/certifications/cc
[Accessed 15 Nov 2025].

isms.online/, 2020. iso-22301. [Online]
Available at: https://www.isms.online/iso-22301/
[Accessed 12 November 2025].

isms.online, 2020. iso-22301/. [Online]
Available at: https://www.isms.online/iso-22301/
[Accessed 12 November 2025].

Martin, A., 2023. alphv-blackcat-posted-data-ireland-munster-technical-university. [Online]
Available at: https://therecord.media/alphv-blackcat-posted-data-ireland-munster-technical-university
[Accessed 17 Nov 2025].

MC Gowran , L., 2023. mtu-it-breach-ransomware-cyberattack-cork. [Online]
Available at: https://www.siliconrepublic.com/enterprise/mtu-it-breach-ransomware-cyberattack-cork
[Accessed 17 Nov 2025].

Microsoft Security, 2021. Decoding NOBELIUM: After-action report (Episode 4). [Online]
Available at: https://www.youtube.com/watch?v=wFtGD7p58cQ
[Accessed 14 November 2025].

Microsoft Security, 2021. Decoding NOBELIUM: Countermeasures (Episode 3). [Online]
Available at: https://www.youtube.com/watch?v=fS97PC4FLCc
[Accessed 14 November 2025].

Microsoft Security, 2021. Decoding NOBELIUM: The hunt for a global threat (Episode 2). [Online]
Available at: https://www.youtube.com/watch?v=VVbSYr1cPEE
[Accessed 14 November 2025].

Microsoft Security, 2021. Decoding NOBELIUM: When nation-states attack (Episode 1). [Online]
Available at: https://www.youtube.com/watch?v=VVKT8NehO_c
[Accessed 14 November 2025].

Microsoft, 2023. secure-least-privileged-access. [Online]
Available at: https://learn.microsoft.com/en-us/entra/identity-platform/secure-least-privileged-access
[Accessed 12 November 2025].

Microsoft, 2023. understand-lateral-movement-paths. [Online]
Available at: https://learn.microsoft.com/en-us/defender-for-identity/understand-lateral-movement-paths
[Accessed 12 November 2025].

Microsoft, 2024. governance/policy/overview. [Online]
Available at: https://learn.microsoft.com/en-us/azure/governance/policy/overview
[Accessed 12 November 2025].

Microsoft, 2024. mcra. [Online]
Available at: https://learn.microsoft.com/en-us/security/adoption/mcra
[Accessed 12 November 2025].

Microsoft, 2024. process-focused-solution-fit-to-standard-fit-gap-analysis. [Online]
Available at: https://learn.microsoft.com/en-us/dynamics365/guidance/implementation-guide/process-focused-solution-fit-to-standard-fit-gap-analysis
[Accessed 14 November 2025].

Microsoft, 2024. what-is-multifactor-authentication-e5e39437-121c-be60-d123-eda06bddf661. [Online]
Available at: https://support.microsoft.com/en-us/topic/what-is-multifactor-authentication-e5e39437-121c-be60-d123-eda06bddf661
[Accessed 14 November 2025].

Microsoft, 2024. zero-trust/zero-trust-overview. [Online]
Available at: https://learn.microsoft.com/en-us/security/zero-trust/zero-trust-overview
[Accessed 16 November 2025].

Microsoft, 2025. cybersecurity-architect-expert. [Online]
Available at: https://learn.microsoft.com/en-us/credentials/certifications/cybersecurity-architect-expert/
[Accessed 13 Nov 2025].

Microsoft, 2025. MSFT-security-cyber-resilience-R2-v1.pdf. [Online]
Available at: https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/bade/documents/products-and-services/en-us/security/MSFT-security-cyber-resilience-R2-v1.pdf
[Accessed 12 November 2025].

Microsoft, 2025. MS-IR-Playbook-Final.pdf. [Online]
Available at: https://www.microsoft.com/content/dam/microsoft/final/en-us/microsoft-brand/documents/MS-IR-Playbook-Final.pdf
[Accessed 12 November 2025].

Microsoft, 2025. planning-bastion-environment. [Online]
Available at: https://learn.microsoft.com/en-us/microsoft-identity-manager/pam/planning-bastion-environment
[Accessed 12 November 2025].

Microsoft, 2025. what-is-soar. [Online]
Available at: https://www.microsoft.com/en-ie/security/business/security-101/what-is-soar
[Accessed 15 November 2025].

*Microsoft, n.d. a-report-on-nobeliums-unprecedented-nation-state-attack. [Online]
Available at: https://www.microsoft.com/en-us/security/blog/2021/12/15/a-report-on-nobeliums-unprecedented-nation-state-attack/
[Accessed 12 November 2025].*

*Microsoft, n.d. a-report-on-nobeliums-unprecedented-nation-state-attack. [Online]
Available at: https://www.microsoft.com/en-us/security/blog/2021/12/15/a-report-on-nobeliums-unprecedented-nation-state-attack/
[Accessed 14 November 2025].*

*Microsoft, n.d. assurance-developing-your-ebcm-plan. [Online]
Available at: https://learn.microsoft.com/en-us/compliance/assurance/assurance-developing-your-ebcm-plan
[Accessed 14 November 2025].*

*Mitre.org, n.d. ctid.mitre.org/inform. [Online]
Available at: https://ctid.mitre.org/inform/
[Accessed 12 November 2025].*

*MTU, 2023. cyber-attack. [Online]
Available at: https://cybercare.mtu.ie/cyber-attack
[Accessed 12 Nov 2025].*

*Ncsc, n.d. ncsc.gov.ie. [Online]
Available at: https://www.ncsc.gov.ie/
[Accessed 12 November 2025].*

*ncyte.net, 2022. the-mccumber-cube-and-cia-triad. [Online]
Available at: https://www.ncyte.net/academia/faculty/cybersecurity-curriculum/college-curriculum/interactive-lessons/the-mccumber-cube-and-cia-triad
[Accessed 12 November 2025].*

*nist.gov, 2010. nistspecialpublication800-34r1.pdf. [Online]
Available at: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf
[Accessed 15 November 2025].*

*Nist.gov, 2018. online-learning/five-functions. [Online]
Available at: https://www.nist.gov/cyberframework/getting-started/online-learning/five-functions
[Accessed 15 November 2025].*

*Nist.gov, n.d. /NIST.SP.800-61r3.pdf. [Online]
Available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r3.pdf
[Accessed 12 November 2025].*

*Nist.gov, n.d. CSWP/NIST.CSWP.29.pdf. [Online]
Available at: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf
[Accessed 17 November 2025].*

*OffSec, 2025. 40393367449108-OSCP-Candidate-Handbook. [Online]
Available at: https://help.offsec.com/hc/en-us/articles/40393367449108-OSCP-Candidate-Handbook
[Accessed 12 Nov 2025].*

*okta.com, 2024. identity-101/ids-vs-ips/. [Online]
Available at: https://www.okta.com/identity-101/ids-vs-ips/
[Accessed 18 November 2025].*

*pwc.com, 2023. resilient-supply-chain-for-procurement.html. [Online]
Available at: https://www.strategyand.pwc.com/de/en/functions/operations/resilient-supply-chain-for-procurement.html
[Accessed 12 November 2025].*

*QQI, 2025. national-framework-of-qualifications. [Online]
Available at: https://www.qqi.ie/what-we-do/the-qualifications-system/national-framework-of-qualifications
[Accessed 16 Nov 17].*

*qradar, 2025. https://www.ibm.com/products/qradar. [Online]
Available at: https://www.ibm.com/products/qradar
[Accessed 17 Nov 2025].*

*RTE, 2023. mtu-it-breach. [Online]
Available at: https://www.rte.ie/news/courts/2023/0211/1356002-mtu-it-breach/
[Accessed 17 Nov 2025].*

*RTE, 2023. munster-technological-university/. [Online]
Available at: https://www.rte.ie/news/regional/2023/0207/1354156-munster-technological-university/
[Accessed 17 Nov 2025].*

*Sheehy, . P., 2023. mtu-it-breach. [Online]
Available at: https://www.rte.ie/news/munster/2023/0208/1355517-mtu-it-breach/
[Accessed 17 Nov 2025].*

*splunk, 2025. https://www.splunk.com/. [Online]
Available at: https://www.splunk.com/
[Accessed 18 Vov 2025].*

*squadcast.com, 2023. runbook-vs-playbook-whats-the-difference. [Online]
Available at: https://www.squadcast.com/blog/runbook-vs-playbook-whats-the-difference
[Accessed 12 November 2025].*

*tcm-sec.com, 2024. nist-guidelines-for-incident-response-best-practices/. [Online]
Available at: https://tcm-sec.com/nist-guidelines-for-incident-response-best-practices/
[Accessed 12 November 2025].*

*techtarget.com, 2021. standard-operating-procedure-SOP. [Online]
Available at: https://www.techtarget.com/searchbusinessanalytics/definition/standard-operating-procedure-SOP
[Accessed 12 November 2025].*

*techtarget.com, n.d. business-impact-analysis. [Online]
Available at: https://www.techtarget.com/searchstorage/definition/business-impact-analysis
[Accessed 14 November 2025].*

*The Irish Times , 2023. mtu-data-appears-on-dark-web-after-cyber-attack. [Online]
Available at: https://www.irishtimes.com/ireland/education/2023/02/12/mtu-data-appears-on-dark-web-after-cyber-attack/
[Accessed 17 Nov 2025].*

*TheJournal, 2023. mtu-cyber-attack-high-court-5992818-Feb2023. [Online]
Available at: https://www.thejournal.ie/mtu-cyber-attack-high-court-5992818-Feb2023/
[Accessed 17 Nov 2025].*

*thorteaches.com, n.d. advanced-persistent-threat-apt. [Online]
Available at: https://thorteaches.com/glossary/advanced-persistent-threat-apt/
[Accessed 13 November 2025].*

*thorteaches.com, n.d. coding-guidelines-and-standards. [Online]
Available at: https://thorteaches.com/glossary/coding-guidelines-and-standards/
[Accessed 17 November 2025].*

*threatcop.com, 2022. https://threatcop.com/blog/nobelium-solarwind-hackers. [Online]
Available at: https://threatcop.com/blog/nobelium-solarwind-hackers/
[Accessed 17 Nov 2025].*

*TitanFile, 2022. phases-of-incident-response. [Online]
Available at: https://www.titanfile.com/blog/phases-of-incident-response/
[Accessed 17 Nov 2025].*

*wikipedia.org, 2019. Systems_development_life_cycle. [Online]
Available at: https://en.wikipedia.org/wiki/Systems_development_life_cycle
[Accessed 12 November 2025].*

*wikipedia.org, 2020. wiki/High_availability. [Online]
Available at: https://en.wikipedia.org/wiki/High_availability
[Accessed 12 November 2025].*

*wikipedia.org, 2023. Patch_Tuesday. [Online]
Available at: https://en.wikipedia.org/wiki/Patch_Tuesday
[Accessed 12 November 2025].*

*wiz.io, n.d. [Online]
Available at: https://www.wiz.io/academy/incident-response-team
[Accessed 12 November 2025].*