Task 1: Solar winds Attack Case study

The solar winds cyber attack was a landmark event int cybersecurity history and symbolized a turning point in the attack landscape proving that supply chain attacks were not only viable but widely successful. Spanning from September 2019 to March 26, 2020, this breach targeted SolarWinds, a significant provider of system management software, and resulted in widespread compromise of government and corporate systems worldwide.

What happened?

The attack was executed on SolarWinds' Orion software, a system management tool widely used by businesses and government agencies to monitor and manage IT infrastructures. The attack inserted a backdoor, codenamed "SunBurst", into Orion's software updates. When SolarWinds customers downloaded these updates, the malware would infiltrate their systems, granting attackers access to sensitive data and networks.

This breach leveraged a supply chain vulnerability, Where the attacker exploited a trusted software vendor to circulate malicious code to its clients. This method of distribution proved devastating due to the extensive usage of SolarWinds' products, enabling the attacker to compromise over 18,000 organizations, and gather an unprecedented amount of sensitive data.

When Did It Occur?

The known attack timeline began during September 2019, when the attackers successfully inserted their malicious code into the Orion platform. However it remained undetected for months, silently spreading to customers through routine software updates. The breach was eventually discovered on December 13th, 2020, when cybersecurity firm FireEye identified the unauthorised access to their own systems.
FireEye traced the breach back to the compromised SolarWinds updates, uncovering a expansive and lengthy espionage operation.

Who Was Behind It?

An attack of this scale is often attributed to a joint effort of many groups, In the SolarWinds attack There were two named groups who have been suspected of their involvement however to this day nobody has claimed ownership of the attack.

The main party attributed responsibility is APT29, also known as Cozy Bear, a state-sponsored hacking group associated with the Russian Foreign Intelligence Service (SVR). Cozy Bear has a long history of cyber-espionage, including involvement in attempts to manipulate U.S. presidential campaigns. Their tactics are know for their stealth and focus on high-value targets, fitting this attack perfectly.

The Other group, Nobelium, has also been linked to the attack Nobelium is a shadowy, privately-funded hacking collective believed to have ties to Russia, China, or North Koreas cyber warfare groups. This group operates with advanced capabilities and has been associated with several high-profile cyber incidents. Microsoft's internal security analysts have since named nobelium in subsequent attacks, highlighting their sustained activity and expertise.
While currently unknown where Nobelium operates out off however it is likely that they are a sub sector of one of the major Advanced Persistent threat groups likely with close ties to Cozy Bear (APT29), Fancy Bear (APT28), or Lazarus Group (APT38).

How Did The Attack Happen?

The SolarWinds attack was a sophisticated supply chain compromise targeting vulnerabilities in their software development pipeline. The attackers breached SolarWinds' environment and embedded the SUNBURST backdoor into updates for its Orion IT management software. Cryptographically signed to appear legitimate, these updates exploited the trust customers placed in SolarWinds.

Once deployed, SUNBURST operated stealthily, mimicking normal Orion functions and blending into legitimate network activity. It delayed activation, communicated with command-and-control servers, and evaded detection by antivirus tools. SolarWinds' insufficient security controls and lack of integrity checks in their build pipeline enabled this compromise, affecting thousands of government, corporate, and critical infrastructure customers.

The attackers prioritized privileged accounts to gain access to sensitive data while minimizing detection. By impersonating legitimate users and using advanced obfuscation techniques, they exfiltrated emails, files, and confidential information. This breach exposed major vulnerabilities in SolarWinds' supply chain and highlighted the risks of third-party software, emphasizing the need for stricter security practices and zero-trust architectures

Why Was It Done?

The primary motive behind the SolarWinds attack was information gathering. By compromising Orion, the attackers gained system-level access to thousands of SolarWinds customer, including:

- U.S. government agencies such as the Department of Homeland Security, Department of Defence and the Treasury.
- Major corporations, including Microsoft, Cisco, and intel.
- Critical infrastructure providers and research institutions.
  This level of access allowed attackers to harvest confidential data, monitor internal communications, and potentially disrupt critical operations. The attack's scale and targets suggest that it was not merely a financial crime but a coordinated espionage campaign, likely intended to bolster geopolitical and strategic advantages.

The Fallout

The discovery of the SolarWinds breach sent shockwaves across the cyber security community and beyond. Organisations scrambled to identify and mitigate the impact on their systems, while security experts analysed the sophisticated techniques used in the attack. The incident underscored the vulnerability of supply chains and the critical need for robust security measures in software development processes.
For SolarWinds, the attack was a reputational disaster, prompting widespread scrutiny of its practices and the boarder software supply chain ecosystems. It also led to significant policy changes, including the Biden administration's executive order on improving the nation's cybersecurity in May 2021.

Task 2: Threat Analysis and Risk Assessment of the Solar Winds Attack

Serial	Name	Assets	vulnerability	Threat	Operational, Reputational, Financial impact	Loss of CIA	Severity	Likelihood	Risk
1	Supply chain exploit	SolarWinds Orion Platform	Insecure software update pipeline	Malicious code inserted Into Orion Updates	Operational & financial: widespread compromise of customer networks, disruption of critical operations.	confidentiality	5	5	25
2	Credential Theft	User credentials	Weak access controls, absence of MFA	Attackers exploit privileged accounts	Operational: Escalated access to sensitive systems, unauthorised actions	confidentiality	4	4	16
3	Data exfiltration	Customer Data	Inadequate DLP mechanisms	Stealing sensitive files, emails, and communications data	Reputational, financial: Loss of intellectual property, exposure of sensitive information	confidentiality	5	4	20
4	Development pipeline attack	Development systems	Weak access controls in the software build environment	Compromised development environment	Operational, Reputational: propagation of malicious updates, undermining trust in software supply chain	integrity , avalibility	5	5	25
5	Privilege escalation	Privileged accounts	Insufficient privilege management	Unauthorized actions performed using privileged accounts	Reputational, operational: Unauthorized access to critical systems, prolonged network compromise	integrity	4	3	12
6	Insider threat	Employee Workstations	Lack of monitoring and detection for insider activity	Malicious or negligent actions by internal staff	Financial, Operational: Unathorised access or modification of sensitive systems	Confidentiality	4	3	12
7	Outdated security policies	Organizational processes	Failure to enforce modern security policies	Unclear or outdated guidelines for securing infrastructure	Operational: Increased likelihood of misconfiguration and exploitation	Confidentiality, Integrity	4	4	20
8	DMZ Compromised	DMZ network	Insufficient isolation	Breach of systems in DMZ and compromise of public assets	Operational, Reputational: Compromise of public assets, unauthorised access of secure networks	Confidentiality, integrity.	5	3	15
9	Lack of penetration testing	Entire IT infrastructure	Limited or no penetration test performed	Undiscovered vulnerabilities in critical infrastructure	Operational: Increased likelihood of attack due to unpatched weaknesses	Confidentiality, Integrity	4	2	12
10	Insufficient training	Employee awareness	Lack of cybersecurity training	Human errors, Phishing attacks and Misconfigurations	Operational, Financial, Reputational: Higher risk of social engineering, configuration	confidentiality	3	4	12

					issues, and insider mistakes				

In this first table we can see the risk of attack for critical assets and what they might be vulnerable to. This table takes a broad overview on vulnerabilities as to create a generalised look at the security of the asset.
Severity and likely hood are measured on a 1-5 scale from 1 being unlikely and not a threat, and 5 being mission critical threat and certain. We then measure risk based on severity x likelihood. 25 being the maximum and being a critical vulnerability that if leveraged would pose a critical threat to the company. and 0 being the opposite of that.

Serial	Name	Assets	vulnerability	Threat	controls	Severity	Likelihood	Risk
1	Supply chain exploit	SolarWinds Orion Platform	Insecure software update pipeline	Malicious code inserted Into Orion Updates	Implement secure software development practices, code signing, and zero-trust architecture for software distribution.	5	2	10
2	Credential Theft	User credentials	Weak access controls, absence of MFA	Attackers exploit privileged accounts	Enforce multi-factor authentication (MFA), privileged access management (PAM), and regular credential rotation.	4	2	8
3	Data exfiltration	Customer Data	Inadequate DLP mechanisms	Stealing sensitive files, e-mails, and communications data	Deploy data loss prevention (DLP) tools, encrypt sensitive data at rest and in transit, and monitor outbound traffic.	5	2	10
4	Development pipeline attack	Development systems	Weak access controls in the software build environment	Compromised development environment	Apply network segmentation, enforce strict build environment monitoring, and secure access controls to development tools.	5	2	10
5	Privilege escalation	Privileged accounts	Insufficient privilege management	Unauthorized actions performed using privileged accounts	Implement role-based access control (RBAC), privileged account monitoring, and behavioral analytics for unusual activity.	4	2	8
6	Insider threat	Employee Workstations	Lack of monitoring and detection for insider activity	Malicious or negligent actions by internal staff	Deploy user activity monitoring tools, insider threat detection solutions, and enforce least privilege principles.	4	2	8
7	Outdated security policies	Organizational processes	Failure to enforce modern security policies	Unclear or outdated guidelines for securing infrastructure	Regularly update security policies to align with industry standards (e.g., NIST), and conduct compliance audits.	4	3	12
8	DMZ Compromised	DMZ network	Insufficient isolation	Breach of systems in DMZ and compromise of	Strong firewalls, regular patching, network	5	2	10

				compromise of public assets	network monitoring			
9	Lack of penetration testing	Entire IT infrastructure	Limited or no penetration test performed	Undiscovered vulnerabilities in critical infrastructure	Regularly conduct penetration tests, vulnerability scans, and red team exercises to identify weaknesses.	4	3	12
10	Insufficient training	Employee awareness	Lack of cybersecurity training	Human errors, Phishing attacks and Misconfigurations	Provide regular employee training on cybersecurity best practices, phishing simulations, and secure configurations.	3	3	9

This table uses the same risk assessment scale as table 1. This post assessment table shows us the controls implemented to address security risks and lower likelihood of critical events occurring.

Task 3: Cyber kill chain analysis

The SolarWinds attack can be mapped using the Lockheed martin Cyber Kill chain framework, which outlines the phases of a cyber attack. Below is the detailed mapping of the attack:

1. **Reconnaissance**
   The attackers, identified as APT29 (Cozy Bear) and Nobelium, conducted an in-depth reconnaissance to identify SolarWinds as a high-value target due to its widespread use by critical government agencies and corporations, notably large fortune 500 companies and technology firms. The attackers focused on SolarWinds' development pipeline, This phase involved gathering technical information about SolarWinds' Orion platform, its software update mechanisms, and potential weak points in its development environment.
   - **Tactics Used:**
     - Open-Source Intelligence(OSINT): Publicly available documentation, employee social media profiles, and forums where scoured to uncover details about the company's operations and software development practices.
     - Phishing and Spear-Phishing: Employees, particularly those with access to development environments, were targeted through personalized phishing campaigns
     - probing development systems: Network scans and probing attempts were made to identify exposed or misconfigured endpoints with SolarWinds' infrastructure
2. **Weaponization**
   In this phase, the attackers developed a malicious payload, later named SUNBURST, this Payload was designed to integrate seamlessly into SolarWinds' Orion platform.

Once integrated SUNBURST would establish a backdoor and mimic legitimate traffic to evade detection.

- **Technical Details:**
  - SUNBURST was crafted to embed malicious DLL files into Orion updates, ensuring the malware appeared as part of legitimate software.
  - The malware employed techniques like domain generation algorithms (DGA) to communicate with attacker-controlled command-and-control (C2) servers, complicating detection.
  - By leveraging stolen developer credentials or exploiting build server vulnerabilities, the attackers ensured their payload was signed and distributed alongside official updates.

3. **Delivery**
   The Compromised Orion software updates containing the SUNBURST malware were delivered to SolarWinds' Trusted update process. This delivery method turned SolarWinds into an unwitting distributor of malicious software.
   - **Tactics Used:**
     - Supply chain Exploitation: By compromising SolarWinds' build process, attackers ensured that the malware would be widely distributed to approximately 18,000 organizations worldwide.
     - exploiting trust: The attackers relied on the inherent trust customers place in signed and verified software updates.
4. **Exploitation**
   SolarWinds
   When the attackers gained access to the development server, they ran the SUNBURST malware on a stolen privileged account this allowed them to gain a persistent foothold in SolarWinds development infrastructure.
   customers
   Once customers installed the compromised Orion updates, the SUNBURST malware exploited the trust relationship to execute code and establish a foothold in their systems.
   - **Technical Aspects:**
     - The malware executed under the same permissions as the Orion application, often with elevated privileges.
     - SUNBURST exploited software trust to load its malicious DLL into memory and avoid detection by using legitimate processes.
     - Privilege escalation techniques were employed to access sensitive resources within compromised environments.
5. **Installation**
   The SUNBURST malware established persistence by communicating with attacker-controlled C2 servers and installing itself in a manner that allowed it to evade security controls.
   - **Technical Details:**

- Persistence Mechanisms: The malware leveraged legitimate services and processes to avoid detection, such as embedded itself in routine tasks performed by Orion.
- C2 Communication Setup: The attackers utilized domain fronting and DNS tunnelling to establish encrypted communication with their servers, making traffic appear normal.

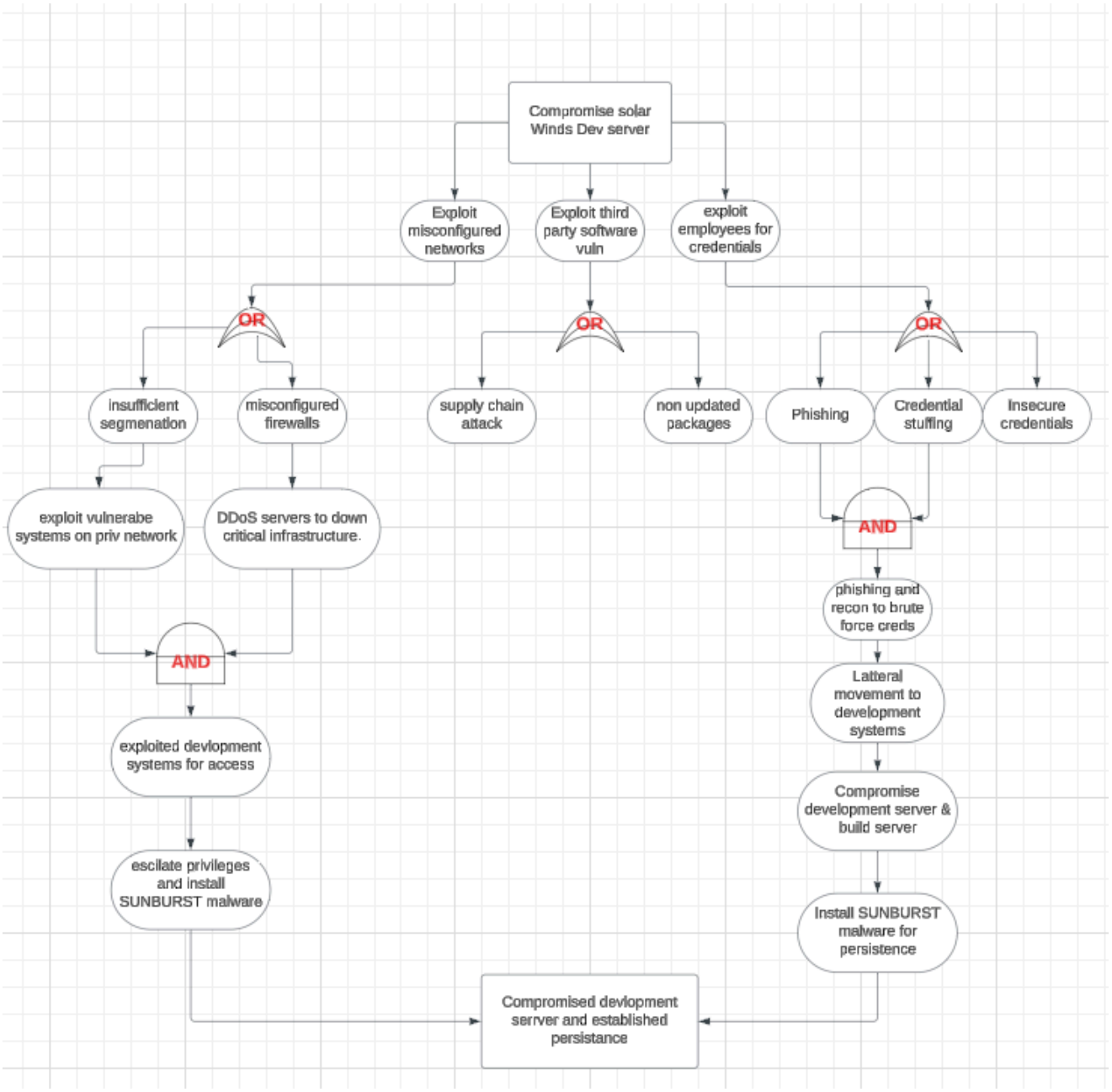
6. **Command and Control (C2)**
   The malware communicated with C2 servers to receive instructions, execute tasks, and facilitate further stages of the attack.
   - **Technical Aspects:**
     - Encrypted Communications: Traffic between SUNBURST and its C2 servers was encrypted and obfuscated to resemble legitimate network activity.
     - Modular Payloads: The attackers sent modular payloads to specific targets based on the value of their systems, enabling targeted exploitation.
     - Lateral Movement: Once established in the network, the malware enabled attackers to pivot to other systems by compromising additional credentials and exploiting trust relationships
7. **Actions On Objectives**
   The attackers used the foothold provided by SUNBURST to carry out their primary objectives, which included data exfiltration, espionage, and further compromise of high value assets and systems.
   - **Technical Aspects:**
     - Credential Harvesting: Attackers extracted credentials from memory and used tools like mimkatz to escalate privileges.
     - Lateral Movement: They exploited trust relationships between systems to move laterally within networks, targeting domain controllers and sensitive databases.
     - Data Exfiltration: Highly sensitive data, including emails and confidential documents, was extracted using encrypted channels to avoid detection.
     - Selective Targeting: Of the 18,000 affected organizations, attackers focused on approximately 100 high-value targets, demonstrating precise targeting capabilities.

Conclusion

The SolarWinds attack demonstrates the advanced tactics, techniques, and procedures (TTPs) used by nation-state actors like APT29 and Nobelium. By leveraging a supply chain vulnerability, the attackers successfully exploited the entire cyber kill chain, from reconnaissance to achieving their objectives. This breach underscores the importance of securing supply chains, implementing robust monitoring and fostering an adaptive security posture to mitigate such sophisticated threats.

This detailed analysis provides insight into the attackers' methodologies, offering a blueprint for understanding and preventing similar breaches in the future.

Task 4: Threat modelling



Attack tree explanation

Root Node

- Objective: Compromise the SolarWinds server.

Branch 1: Exploit misconfigured networks

1. insufficient Segmentation
   - **1a:** Exploit vulnerable systems on private network
2. misconfigured firewalls
   - **2a:** servers to down critical infrastructure
3. **1a + 2a:** Exploited development systems for access
4. escalate privileges and install sunburst malware

Branch 2: Exploit their party software vuln

1. supply chain attack
2. non updated packages

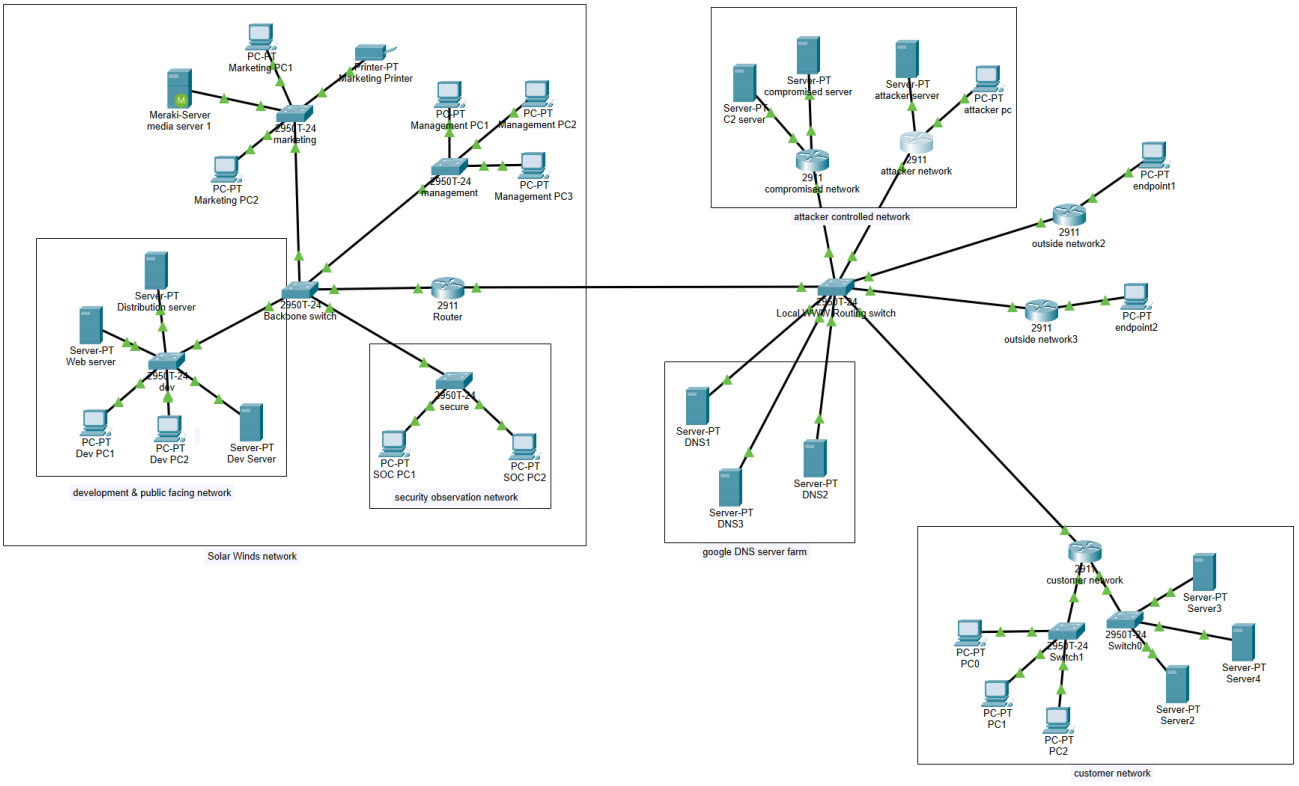
Branch 3: Exploit employees for credentials

1. phishing
2. Credential stuffing
3. Insecure credentials
4. **1 + 2:** Phishing and recon to brute force creds
5. lateral movement to development systems
6. compromise development servers & build servers
7. install sunburst malware for persistence.

In this explanation I have noted the steps taken through each attack tree branch, In my opinion branch 3 is the most likely attack method used by apt29. we can not be sure on the attack method used to gain initial access as there are not many publications on it however the generally understood method is phishing and password spam attacks, compromising a third party account and moving to gain more access from there.

I was unable to use the proper attack tree notation due to the limitations of the program I use however I still believe that it provides a valuable visual representation.

Task 5: Pre-breach Infrastructure diagram



Network diagram analysis

- **Routing and switching**
  - Devices: 2911 Router, 2950T-24 Switches
  - Purpose:
    - The 2911 Router facilities external communication and is responsible for routing traffic between subnets and external networks.
    - The 2950T-24 Backbone Network Switch Acts as a core switch interconnecting all other subnets, This High speed network switch handles inter-subnet traffic, providing routing and switching between marketing, management, development, and security subnets.
    - Each Subnet has its own 2950T-24 network switch to handle devices and local subnet traffic.
- **Marketing:**
  - Devices:
    - Marketing PCs (PC1, PC2)
    - Media server (Meraki-Server)
    - Printer (Marketing Printer)
  - Switch: 2950T-24 Marketing
  - Purpose: Enables devices to connect to the subnet and access the media server and marketing printer.
- **Management**
  - Devices:
    - Management PCs (PC1, PC2, PC3)
  - Switches 2950T-24 Management
  - Purpose: allows for centralised control and management tasks, Also allows for isolated control over connection to external and internal resources for security.
- **Development**
  - Devices:
    - Development PCs (Dev PC1, Dev PC2)
    - Servers (Distribution Server, Web Server, Dev Server)
  - Switch 2950T-24 Development
  - Purpose:
    - Provides connectivity for software development and testing.
    - Includes servers for hosting development applications and distribution purposes. (In a real world scenario these would likely be off site or hosted by a third party.)
- Security
  - Devices:
    - SOC PCs (PC1, PC2)
  - Switch: 2950T-24 Secure
  - Purpose:

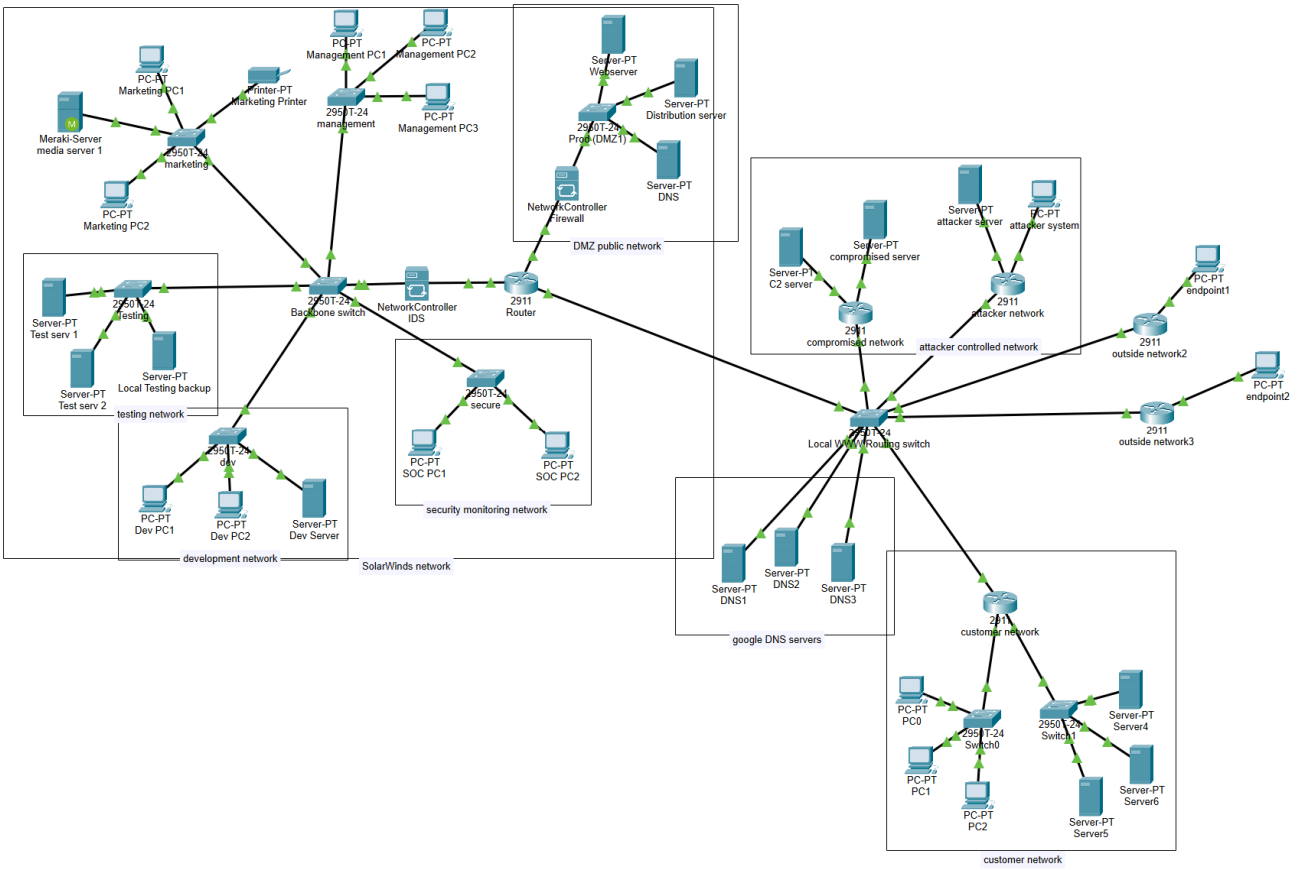
        - Dedicated to the SOC team for monitoring analysis and incident response.
        - stricter access controls and network monitoring tools.
- **VLANs**
  The configuration of the following VLANs is designed to enable traffic isolation and increase security.
  Each VLAN has access to relevant areas of the network for example, Development VLAN 30 has access to the marketing media server to enable developers to use graphical resources created by the marketing and design teams. They however do not have access to the SOC or management Devices
    - VLAN 10: Marketing
    - VLAN 20: Management
    - VLAN 30: Development
    - VLAN 40: Security/SOC

This Network Diagram has been stripped back to a simplistic interpretation of how a full network would look for SolarWinds. The development server and Distribution server would likely be hosted on prem due to the little overhead Distributing software would be, and Development server would likely contain sensitive pre-release builds of software that if released into public domain would pose a security incident for SolarWinds. Because of this Hosting on prem would allow them to maintain control over the hardware and software while managing the security of its data.

Key attack vectors for the SolarWinds hack 2020 would be the development server and the distribution server, these are both included in the network model. The development server would have access to privileged development builds of the Orion software and its development environment, attackers that gain access to this would be able to manipulate the Orion software development builds in any way they see fit. This was the approach taken in the 2020 hack of SolarWinds That allowed the attackers to implement the SUNBURST malware. From here software builds are likely tested very little and then pushed to its production version of the Orion application.

includes customer and attacker networks.

Task 6: Post-breach infrastructure diagram



Network Diagram Analysis

- **Routing and switching**
  - Devices: 2911 Router, 2950T-24 Switches
  - Purpose:
    - The 2911 Router facilities external communication and is responsible for routing traffic between subnets and external networks.
    - The 2950T-24 Backbone Network Switch Acts as a core switch interconnecting all other subnets, This High speed network switch handles inter-subnet traffic, providing routing and switching between marketing, management, development, and security subnets.
    - Each Subnet has its own 2950T-24 network switch to handle devices and local subnet traffic.
- **Marketing:**
  - Devices:
    - Marketing PCs (PC1, PC2)
    - Media server (Meraki-Server)
    - Printer (Marketing Printer)
  - Switch: 2950T-24 Marketing
  - Purpose: Enables devices to connect to the subnet and access the media server and marketing printer.
- **Management**
  - Devices:
    - Management PCs (PC1, PC2, PC3)

    - Switches 2950T-24 Management
    - Purpose: allows for centralised control and management tasks, Also allows for isolated control over connection to external and internal resources for security.
- **Development**
    - Devices:
        - Development PCs (Dev PC1, Dev PC2)
        - Servers (Distribution Server, Web Server, Dev Server)
    - Switch 2950T-24 Development
    - Purpose:
        - Provides connectivity for software development and testing.
        - Includes servers for hosting development applications and distribution purposes. (In a real world scenario these would likely be off site or hosted by a third party.)
- Security
    - Devices:
        - SOC PCs (PC1, PC2)
    - Switch: 2950T-24 Secure
    - Purpose:
        - Dedicated to the SOC team for monitoring analysis and incident response.
        - stricter access controls and network monitoring tools.
- Testing
    - Devices:
        - Testing Servers (Server1,2)
        - Testing backup server,
    - Switch: 2950T-24 Testing
    - Purpose:
        - Dedicated air gapped network for testing new hardware, software or third party tools.
        - Redundant Development environment servers and Dedicated server cluster for git and version control, this can work along side a automated code change review for security.
- Production
    - Devices:
        - Distribution servers
        - Web servers
        - DNS
    - Switch: 2950T-24 Prod (DMZ)
        - Network Locked down to a DMZ to further prevent access to internal network from external users
    - Purpose:

        - Dedicated servers for distribution and web hosting.
        - Air gapped to prevent outside interference and tampering.
        - scalable web servers to compensate for low and high traffic and help mitigate DDoS attack vulnerability (acting as a buffer).
- **VLANs**
  The configuration of the following VLANs is designed to enable traffic isolation and increase security.
  Each VLAN has access to relevant areas of the network for example, Development VLAN 30 has access to the marketing media server to enable developers to use graphical resources created by the marketing and design teams. They however do not have access to the SOC or management Devices
    - VLAN 10: Marketing
    - VLAN 20: Management
    - VLAN 30: Development
    - VLAN 40: Security/SOC
    - VLAN 50: Testing
    - VLAN 60: Production (DMZ)
- External Networking
    - External Switching (WAN)
    - DNS servers (1,2,3)
    - External LAN networks

In this network diagram I have modified the existing structure to further help mitigate the risk of attack on crucial assets as well as isolating them to prevent threat actors moving from an internal device onto the server that would then allow them to bypass security measures.

To further improve the security I would use strict access control and logging to help detect intrusion, possibly using AI to track behavioural aspects of high level accounts and alert to unusual behaviour.
I would also introduce multi factor authentication for all developers and accounts with high level permissions or wide ranging access. using both physical and online access tokens.

Task 7: Security Assurance Architecture

1. **Access Control**
   "Role based access controls are implemented for access to information systems. Processes and procedures are in place to address employees who are voluntarily or involuntarily terminated. Access controls to sensitive data in our databases, systems, and environments are set on a need-to-know / least privilege necessary basis." & *"We require that authorized users be provisioned with unique account IDs. Our password policy covers all applicable information systems, applications, and databases. Our password best practices enforce the use of complex passwords that include both alpha*

and numeric characters, which are deployed to protect against unauthorized use of passwords. Passwords are individually salted and hashed."

- It is clear that these policies were ether created after or altered due to the solar winds hack 2020, it displays clear signs of a security focused approach that would have made it much harder for attackers to exploit entry into the development systems and accounts.

2. Network Security
   "Automated tools are deployed within the network to support near-real-time analysis of events to support of detection of system-level attacks. Next generation firewalls deployed within the data centre as well as remote office sites monitor outbound communications for unusual or unauthorized activities, which may be an indicator of the presence of malware (e.g., malicious code, spyware, adware)."
   - This advanced internal testing of built automated tools, and further scrutinous scanning of both process activity and network activity Is more than likely a change made after 2020. due to the nature of the testing described here it would be reasonable to assume if this was in place before 2019 the attackers would have been discovered long before a production build was shipped to customers.
3. Incident Management
   "SolarWinds has a formalized incident response plan (Incident Response Plan) and associated procedures in case of an information security incident. The Incident Response Plan defines the responsibilities of key personnel and identifies processes and procedures for notification."
   - I have no doubt that this policy was restructured and reviewed following the solar winds attack. while they did have a good incident response time of 48hrs to isolate, remove and patch the intrusion, It is of my opinion that incident management should also be a proactive collaboration to further prevent attack rather than just a reactive approach. Therefore a review of policies and response plan should always be reviewed after an incident.
4. Physical security
   "Access to areas where systems, or system components, are installed or stored are segregated from general office and public areas. The cameras and alarms for each of these areas are centrally monitored 24x7 for suspicious activity, and the facilities are routinely patrolled by security guards. Servers have redundant internal and external power supplies. Data centers have backup power supplies, and can draw power from diesel generators and backup batteries. These data centers have completed a Service Organization Controls (SOC) 2 Type II audit and are SSAE16 accredited."
   - Physical security policies may have also been altered after this attack, it is more likely to experience a physical security breach after a digital security breach. This could be because of a reallocation of resources to recover from infrastructure loss or financial loss. Attackers also see this time where access control mechanisms may be at their weakest due to server and infrastructure downtime.

5. SolarWinds has backup standards and guidelines and associated procedures for performing backup and restoration of data in a scheduled and timely manner. Controls are established to help safeguard backed up data (onsite and off-site). We also work to ensure that customer data is securely transferred or transported to and from backup locations. Periodic tests are conducted to test whether data can be safely recovered from backup devices.
    - It is likely that data backup guidelines were updated after the breach due to the extensive time that APT29 was in the SolarWinds system. it likely compromised many backups and possibly persisted past their last backup depending on how often they delete old backups.

Solar Winds Network Security Policy

1. Introduction

The purpose of this policy is to define network security practices to protect solar wind's infrastructure, data, and network traffic from cyber threats. Informed by lessons from the SolarWinds attack, this policy emphasizes secure network structures, proactive traffic monitoring, and incident response. It applies to all employees, contractors, and third parties managing network resources.

2. Scope

This policy applies to all aspects of network traffic and architecture, including:

- Logical network design and segmentation.
- Traffic monitoring, analysis, and control tools.
- Security protocols for internal and external network communications.

3. Objectives

- Protect the confidentiality, integrity, and availability of network traffic.
- Detect and mitigate unauthorized access and anomalies in real-time.
- Align with SANS Critical Security Controls and regulatory standards.

4. Roles and Responsibilities

- **IT Administrators:** Maintain network architecture and implement traffic controls.
- **Security Team:** Monitor traffic, analyse threats, and manage incident responses.
- **Employees:** Follow security guidelines and report anomalies.
- **Third-Party Vendors:** Comply with organizational network security requirements.

5. Network Security Measures

5.1. Risk Assessment

- Conduct periodic assessments to identify vulnerabilities in network traffic and architecture.

- Categorize risks by potential impact and likelihood.
- Implement controls based on identified risks, such as access restrictions and enhanced monitoring.

5.2. Logical Network Segmentation

- Use logical zones (e.g., public, internal, restricted) to segment the network based on sensitivity.
- Implement strict access controls between zones to limit lateral movement.
- Regularly review and update segmentation to reflect evolving security requirements.

5.3. Network Traffic Monitoring and Analysis

- Deploy continuous monitoring tools, such as:
  - Intrusion Detection and Prevention Systems (IDPS).
  - Flow analysers for detecting anomalies and volumetric attacks.
- Baseline normal traffic patterns and configure alerts for deviations.
- Maintain logs of all network traffic for forensic analysis (minimum retention: six months).

5.4. Secure Communication Protocols

- Enforce encryption for sensitive traffic using protocols like TLS.
- Block insecure protocols unless explicitly required and risk-assessed.
- Use DNS filtering to block access to malicious or unapproved domains.

5.5. Zero Trust Network Architecture (ZTNA)

- Require identity verification for all devices and users accessing the network.
- Enforce strict authentication for inter-zone communication.
- Continuously monitor traffic within and between zones for anomalies.

5.6. Threat Detection and Response

- Integrate automated detection tools (e.g., SIEM) for correlating logs and identifying threats.
- Employ machine learning for advanced threat detection, including Advanced Persistent Threats (APTs).
- Maintain a playbook for common threats, such as Distributed Denial-of-Service (DDoS) attacks.

5.7. Metrics and Reporting

- Track key metrics, such as:
  - Average response time to detected anomalies.
  - Number of blocked unauthorized access attempts.

- Generate periodic reports to review the effectiveness of security measures.

5.8. Continuous Vulnerability Scanning

- Use tools to identify vulnerabilities in real-time within network traffic and endpoints.
- Apply security patches promptly and prioritize critical vulnerabilities.
- Block traffic exploiting known vulnerabilities using dynamic access controls.

6. Training and Awareness

- Provide regular training on recognizing suspicious traffic for employees.
- Train IT staff on advanced monitoring and detection tools.
- Ensure third-party vendors understand and comply with secure network access policies.

7. Incident Response

- Establish an incident response plan focused on traffic-based threats.
- Use network traffic logs to investigate incidents and implement containment measures.
- Conduct post-incident reviews to improve traffic monitoring and threat detection processes.

8. Compliance and Audit

- Align with SANS Critical Security Controls, NIST CSF, and ISO/IEC 27001 standards.
- Regularly audit traffic monitoring systems and security configurations.
- Document and address audit findings promptly.

9. Exceptions

Exceptions to this policy require approval from the Security Team and must include documented risk mitigation measures.

10. Enforcement

Violations of this policy may result in disciplinary actions, including revocation of access privileges or termination of employment. Third-party non-compliance may lead to contract termination.

11. Review and Revision

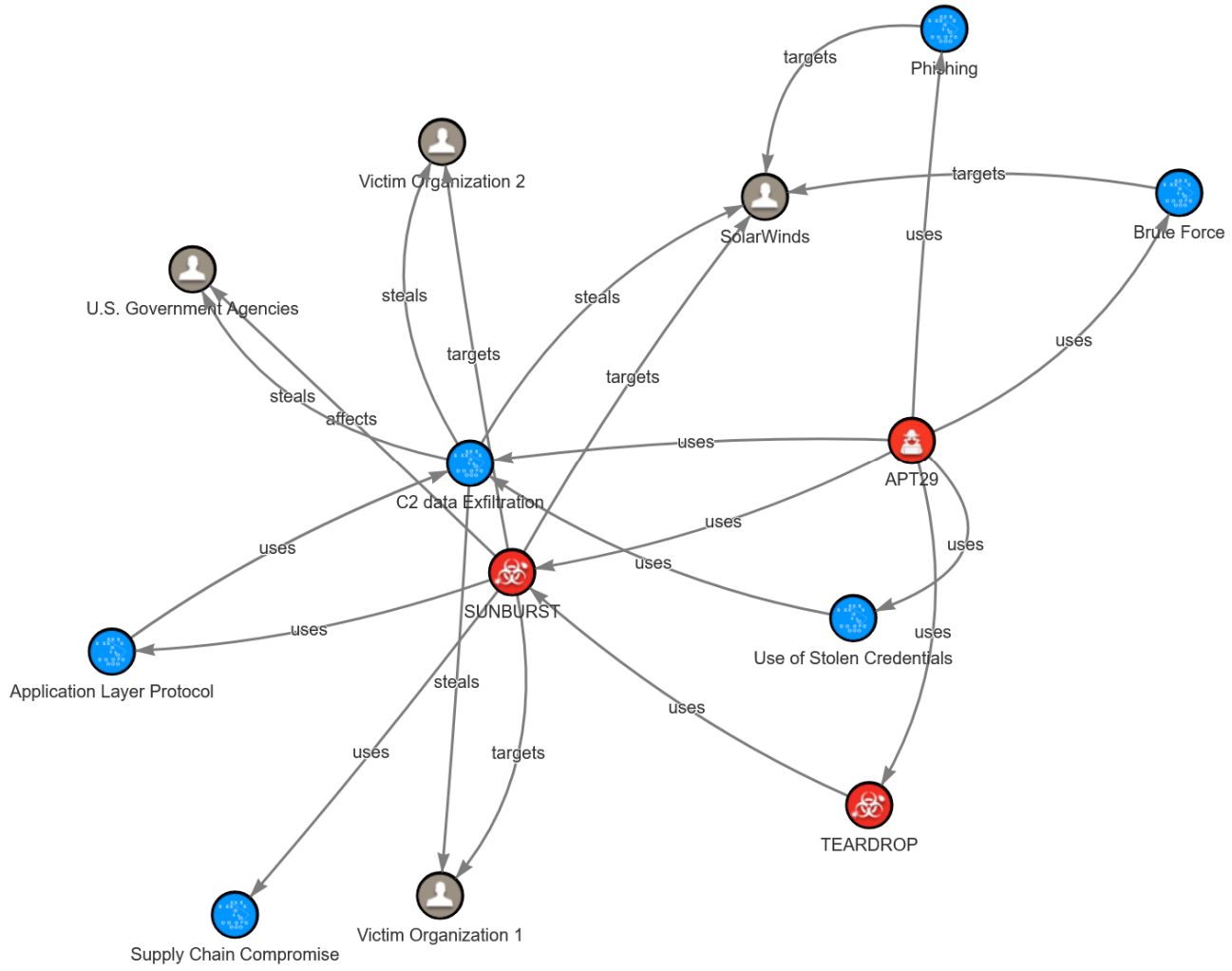
This policy will be reviewed semi-annually or when significant technological or threat landscape changes occur.

12. Document Control

- **Version:** 1.1
- **Effective Date:** 20/01/25
- **Next Review Date:** 20/01/26

- **Owner:** SolarWinds Operational Security & Compliance

Task 8: Stix SDO model



[Json Code On Github]

STIX Writeup

APT 29

- Threat actor apt29 (cozy bear)
- goals: Cyber espionage, credential theft, data theft.
- motivation: Strategic and geopolitical advantage, Exfiltration of sensitive data

Sunburst

- Malware, Trojan
- Backdoor, External access
- Description: Sunburst is a malware created to infect SolarWinds Orion build servers, and plant a backdoor in the form of a legitimate dll, communicating with a C2 server.

- cve-2020-10148

Teardrop

- malware, Loader
- Loader, persistence
- Description: Teardrop is a malware loader designed to deliver a cobalt-strike payload into memory, this would allow the attackers a form of persistence into the system.

APT 29 used a vulnerability in third party software to gain initial access into SolarWinds, While there is no official documentation stating how this occurred it has been noted that there was a possibility of password spray attacks and brute force, as well as auth token bypass and cookie theft and replication. Once APT29 gained access to SolarWinds systems they leveraged a vulnerability in the Orion build server to inject the SUNBURST and Teardrop malware into the development builds of Orion software. These development builds were distributed to major corporations that would need advanced access to these builds, this included Government organisations and other security research and development companies.

SUNBURST was designed to infect spread and communicate with a C2 server scraping sensitive data and allowing attackers to gain access to accounts remotely. Where as Teardrop was designed to create a persistent foothold into infected devices through cobalt-strike c2 beacons.

Once SolarWinds was infected it SUNBURST was executed on the development build server of the Orion software which would later infect other machines through a supply chain attack. SolarWinds was not the primary target in this attack more a means to and end goal. This end goal while still unclear, can be assumed was espionage and data theft from government organisations and other high status companies such as Microsoft.

References

- **SUNBURST Malware:** www.cisa.gov. (2021). *MAR-10318845-1.v1 - SUNBURST | CISA*. [online] Available at: https://www.cisa.gov/news-events/analysis-reports/ar21-039a.
- **TEARDROP Malware:** www.cisa.gov. (2021). *MAR-10320115-1.v1 - TEARDROP | CISA*. [online] Available at: https://www.cisa.gov/news-events/analysis-reports/ar21-039b.
- **SUNSHUTTLE Malware:** www.cisa.gov. (2021). *MAR-10327841-1.v1 – SUNSHUTTLE | CISA*. [online] Available at: https://www.cisa.gov/news-events/analysis-reports/ar21-105a.
- **SolarWinds Compromise technical report**: CISA (2021). *Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations | CISA*. [online] Cybersecurity and Infrastructure Security Agency CISA. Available at: https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-352a.

- **SolarWinds Compromise press report:** www.ncsc.gov.uk. (2021). *SolarWinds*. [online] Available at: https://www.ncsc.gov.uk/collection/ncsc-annual-review-2021/the-threat/solarwinds.
- **SolarWinds Orion CVE:** nvd.nist.gov. (2020). *NVD - CVE-2020-10148*. [online] Available at: https://nvd.nist.gov/vuln/detail/CVE-2020-10148.
- **NCSC 2021 threat review:** www.ncsc.gov.uk. (2021). *SolarWinds*. [online] Available at: https://www.ncsc.gov.uk/collection/ncsc-annual-review-2021/the-threat/solarwinds.
- **Media article on SolarWinds:** Oladimeji, S. and Kerner, S.M. (2023). *SolarWinds hack explained: Everything you need to know*. [online] Techtarget. Available at: https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know.
- **IBM Orion CVE:** www.ibm.com. (n.d.). *SolarWinds Orion (CVE-2020-10148)*. [online] Available at: https://www.ibm.com/docs/en/randori?topic=2022-solarwinds-orion-cve-2020-10148.
- **APT 29 Government article:** GOV.UK. (n.d.). *Russia: UK exposes Russian involvement in SolarWinds cyber compromise*. [online] Available at: https://www.gov.uk/government/news/russia-uk-exposes-russian-involvement-in-solarwinds-cyber-compromise.
- **Other public domain sources and articles**

apologies for the weird formatting errors, PDF did not want to play ball.