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 Threat Actors implemented a supply chain attack, a method that targets third-party providers to gain indirect access to their clients' systems. in This case, the attackers compromised SolarWinds' software development pipeline, embedding the SUNBURST backdoor into legitimate Orion software updates.
Once deployed the sunburst backdoor allowed attackers to impersonate legitimate users, including those with elevated privileges preferring this over other users, to infiltrate systems without raising suspicion. These elevated privileges provided access to vast amounts of sensitive data while minimizing detection risks. The malware also included measures to avoid traditional antivirus tools and was designed to blend into legitimate network traffic, further complicating detection efforts.

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

#change-this

serial	Name	asset	vulnerability	threat/ hazard	operational reputational financial	loss of CIA?	severity	likeliho
1								
2								
3								
4								
5								
6								
7								
8								
9								
10								

1. **Key Assets**
   The key assets targeted during the SolarWinds attack included:
   - SolarWinds Orion Software platform: A critical IT management tool deployed across thousands of organizations worldwide.
   - Customer Networks and Systems: The attack affected SolarWinds' customers, including U.S. government agencies, private corporations and critical infrastructure providers.
   - Confidential Data: Sensitive information, including emails, files, files, and internal communications stored on compromised networks.
   - User credentials: Privileged accounts exploited by attackers to escalate access within targeted systems.
     Mitigation Techniques:
   - Applications Hardening: Employ secure development practices, such as code reviews and automated testing, to protect against vulnerabilities in software.
   - Access Management: use multi-factor authentication and privileged access management tools to secure user credentials.

- Encryption: Ensure sensitive data is encrypted both in transit and at rest to limit the utility of stolen data.

2. **Identified Vulnerabilities**
    - Compromised Software Development Pipeline, The attackers inserted malicious code into the Orion update by exploiting vulnerabilities in SolarWinds' development environment.
    - Insufficient Privilege Management, Post-deployment, attackers exploited privileged accounts to access sensitive data and perform lateral movement.
    - Lack of anomaly detection, The SUNBURST malware leveraged advanced evasion techniques to avoid detection, such as mimicking legitimate network activity.
    - Inadequate supply chain security, SolarWinds' lack of rigorous third-party risk management allowed the attack to propagate via trusted software updates.
    Mitigation Techniques
    - Secure development environment: Enforce strict access controls, network segmentation and real-time monitoring in software build environments.
    - Behavioural Analytics: Deploy AI-based tools to detent anomalous behaviour indicative of privilege abase or lateral movement.
    - Supply Chain Auditing: Conduct Regular security audits and assessments of third-party vendors and their software.
    - Code Integrity: Implement cryptographic signing for software releases to ensure integrity authenticity.
3. **Potential Exploits**
    - Supply Chain Exploitation, Attackers Introduced the SUNBURST malware into Orion updates, ensuring that the comprised software was widely distributed.
        - impact: Enabled attackers to bypass traditional defences by exploiting trust in SolarWinds as a vendor.
        - Mitigation: implement a zero-trust architecture, where trust is continuously verified rather than assumed. Use rigorous testing and verification processes for software updates before deployment.
    - Credential Theft And Privilege Escalation, The attackers impersonated legitimate users, including those with elevated privileges, to gain unauthorized access.
        - Impact: Provided unrestricted access to sensitive data and critical systems.
        - Mitigation: Regularly rotate and monitor privileged account credentials. Deploy PAM solutions to limit access and ensure activity is logged and audited.
    - Data Exfiltration, SUNBURST enabled attackers to extract sensitive information from victim systems over an extended period.
        - impact: Loss of intellectual property, national security data, and critical corporate information.

    - Mitigation: Employ data loss prevention solutions to detect and block unauthorized data transfer. Monitor outbound network traffic for unusual patterns.

4. **Impacts**
    - Operational Disruption, The attack disrupted the operations of several government agencies and corporations, leading to significant delays and resource allocation for incident response.
        - mitigation: develop and maintain robust incident response plans, conduct regular tabletop exercises, and ensure business continuity plans are in place.
    - Reputational Damage, The breach severely impacted SolarWinds' reputation, resulting in lost customer trust and diminished market value.
        - mitigation: foster transparency and proactive communication during incidents. Demonstrate commitment to security by adopting industry best practices and obtaining relevant certifications (e.g., IOS 27001).
    - Financial Loss, Organizations incurred substantial cost from forensic investigations, legal actions, and infrastructure recovery.
        - Mitigation: invest in cyber insurance to offset financial losses from potential breaches.
    - strategic risk, The attack undermined national security by exposing sensitive government data and operations.
        - mitigation: establish cross-agency partnerships to share threat intelligence and develop unified cybersecurity strategies.
5. **Likelihood of Exploits**
    - High Likelihood: Supply Chain Exploitation, Given the growing reliance on third-party vendors, supply chain attacks are increasingly probable.
        - mitigation: Enhance vendor vetting processes and adopt tools to monitor and validate software integrity.
    - Medium likelihood: Privilege Escalation, While less frequent than supply chain attacks, the exploitation of privileged accounts remains a significant risk.
        - Mitigation: implement role-based access controls (RBAC) and conduct regular privilege reviews.
    - Low Likelihood: Zero-Day Exploitation, The sophistication required for zero-day exploits lower their frequency but not their potential impact.
        - mitigation: patch management and rapid vulnerability remediation can minimise exposure to such exploits.
6. **Summary Of mitigation Recommendations**

    - Zero-Trust Architecture: Continuously verify user and device trust before granting access to sensitive systems.
    - Enhanced Monitoring: deploy security information and event management solutions to monitor networks for anomalies.

- Supply chain governance: Perform regular risk assessments of third-party vendors and require adherence to strict security standards.
- Cyber Hygiene: conduct regular training for employees on cybersecurity best practices, including phishing awareness and secure password management.
- incident preparedness: maintain an up-to-date incident response plan and ensure all stakeholders are familiar with their roles during a breach.
- Government Collaboration: Leverage public-private partnerships to share threat intelligence and bolster collective defences.

By addressing these vulnerabilities and implementing the suggested mitigation techniques, organizations can significantly reduce their exposure to sophisticated supply chain attacks like the SolarWinds breach. Proactive security measures, continuous monitoring and collaborative efforts are essential to defend against the evolving cyber threat landscape.

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**
   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

An attack tree is a structured representation of potential attack vectors, created from a Root Node, Branches and Branch nodes.
Attack trees showcase how adversaries might achieve their goals. Below is an attack tree

that I have created around gaining access to the SolarWinds server, addressing possible and impossible nodes, required equipment, cost and implications, and countermeasures.

Root Node

- Objective: Compromise the SolarWinds server.

Branch 1: Exploit Software Development Environment

- Node 1.1: Gain unauthorized access to developer credentials.
    - Possible: Through Phishing campaigns targeting employees.
    - Required Equipment: Email phishing Tools, spoofed domains.
    - Cost: Low/Medium, dependent on scale of Phishing campaign.
    - Countermeasures: Multi-factor authentication (MFA), phishing awareness training.
- Node 1.2: Exploit vulnerabilities in development tools.
    - Possible: Target unpatched CI/CD tools.
    - Required Equipment: Vulnerability scanners, exploit kits.
    - Cost Medium, Requires skilled operators.
    - Countermeasures: Routine vulnerability scans and patch management.
- Node 1.3: Social engineering to obtain physical access.
    - Possible but challenging: requires insider collaboration or effective impersonation.
    - Required Equipment Fake IDs, disguises.
    - Cost: High.
    - Countermeasures: Strict physical security protocols, employee ID checks.

Branch 2: Compromise Supply Chain

- Node 2.1: Inject malicious code into a software update.
    - Possible: By accessing source code repositories.
    - Required Equipment: Credentials or exploit for repository management systems.
    - cost: High, Requires extensive reconnaissance and insider knowledge.
    - Countermeasures: Code-signing practices, integrity verification.
- Node 2.2: Replace hardware components during transit.
    - Difficult might be possible: Very Difficult to pull off requires planning and insider knowledge.
    - Required Equipment: Shipping manifests, item numbers, product codes and packaging match.
    - Cost: High, Required equipment high cost and large quantity of requirements.
    - Countermeasures: Black light ink signatures, tamper proof packaging and unique internal identifiers.

Branch 3: Exploit Network Perimeter

- Node 3.1: Exploit unpatched vulnerabilities in SolarWinds' network infrastructure.

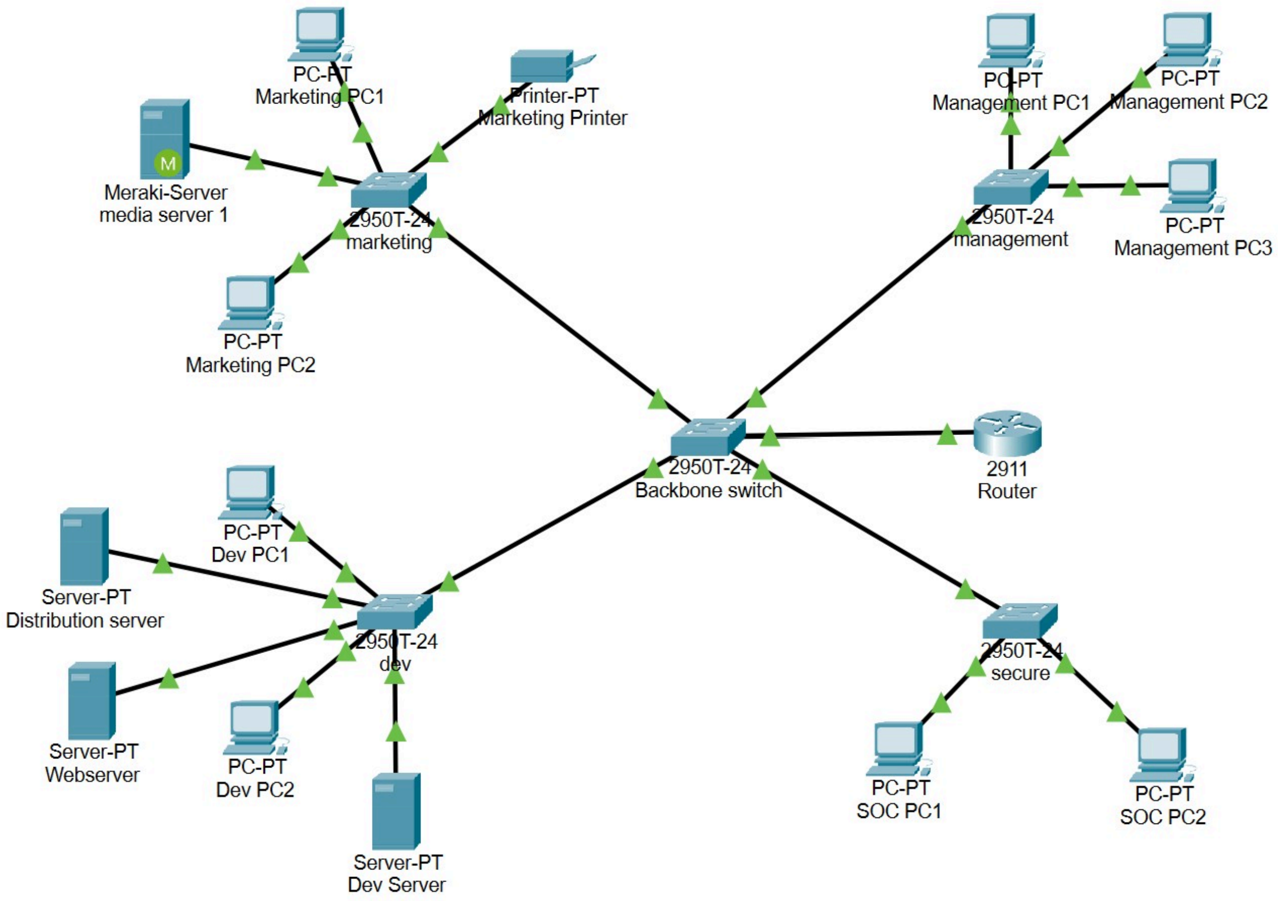
    - Possible: Use of zero-day vulnerabilities.
    - Required Equipment: Advanced exploit frameworks.
    - Cost: Very High, Zero-days are expensive to purchase from black market.
    - Countermeasures: Regular penetration testing, proactive monitoring.
- Node 3.2: Conduct Distributed Denial of Service (DDoS) to mask infiltration.
    - Possible: Requires botnet control.
    - Required Equipment: Access to a botnet.
    - Cost: Medium, Botnets can be rented on the dark web.
    - Countermeasures: Deploy DDoS mitigation solutions.

Branch 4: Exploit Insider Threats

- Node 4.1: Bribe or coerce employees.
    - Possible: Exploiting disgruntled or financially vulnerable staff.
    - Cost: Medium to High, Dependent on the employee.
    - Countermeasures: Employee vetting, reporting channels for unusual behaviour.
- Node 4.2: Recruit or plant a malicious insider.
    - Possible but rare: Requires significant resources and time.
    - Cost: High.
    - Countermeasures: Background checks, role-based access control.

Analysis
The most feasible attacks target software vulnerabilities, social engineering, or the supply chain each with varying costs and requirements. Countermeasures such as robust authentication, continuous monitoring, and regular patching to reduce risk significantly. Nodes like replacing hardware during transit are effectively impossible, and would require planning and resources outside the scope of the operation, due to robust logistical security. Emphasizing that modern threats often focus on digital vectors.

Task 5: Pre-breach Infrastructure diagram



Network diagram analysis

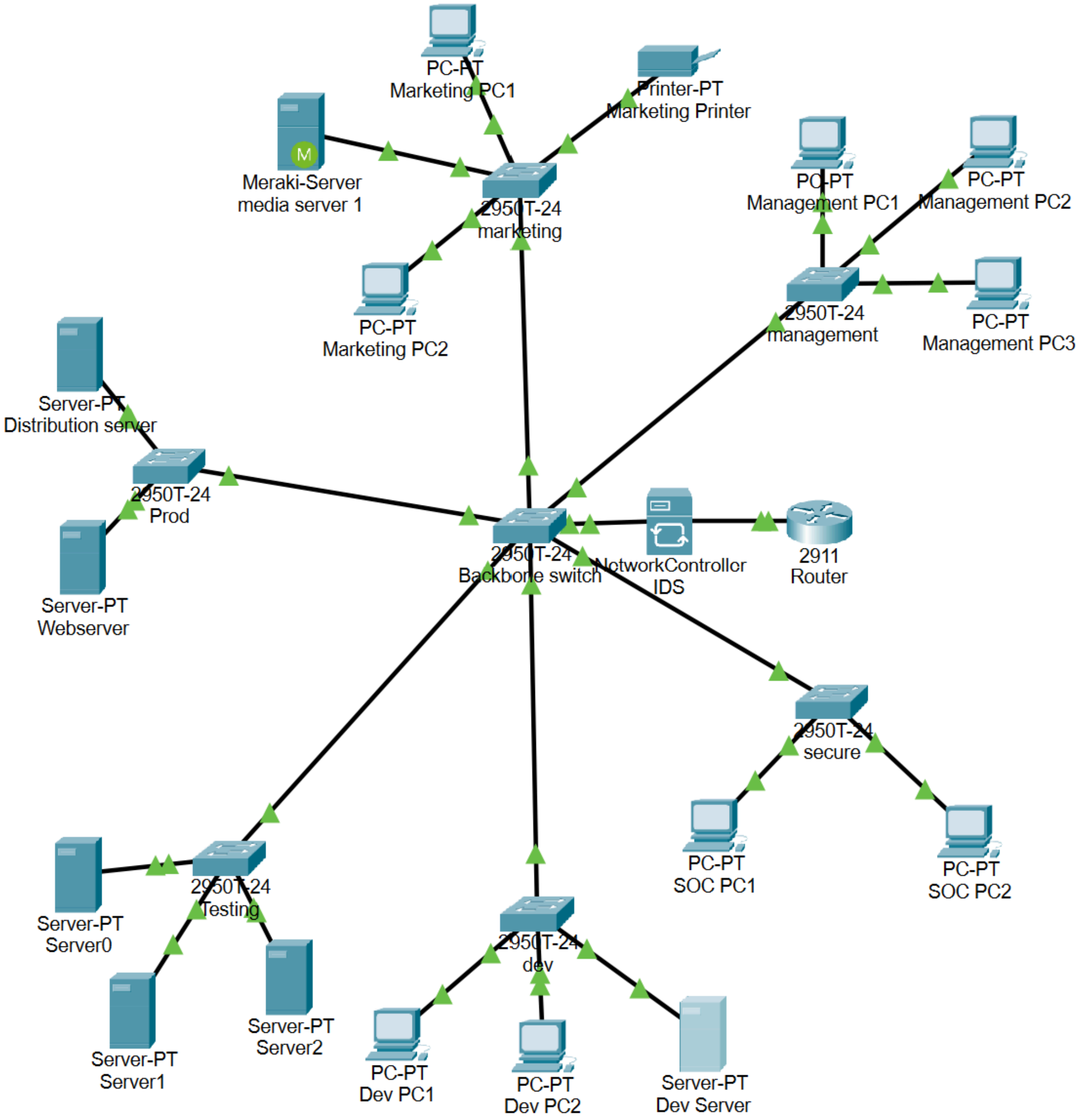
- **Routing and switching**
  - Devices: 2911 Router, 2950T-24 Switches
  - Purpose:
    - The 2911 Router facilities external communication and is responsible for routing traffic between subnets and external networks.
    - The 2950T-24 Backbone Network Switch Acts as a core switch interconnecting all 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.

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 (Server 0-2)
  - 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
  - Switch: 2950T-24 Prod
  - 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

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

Task 8: Stix SDO model