

**Swinburne University of Technology**  
**Hawthorn Campus**  
**Department of Computing Technologies**

**COS30015 IT Security**  
*Assignment 2 - Semester 2, 2024*

# Part B Incident Situational Report

**Due Date:** AEST 23:59 on 31/10/2024.

Having investigated all the artefacts provided by STARFLEET, they have requested a situation report update to understand the incident.

Compute the following template with your findings from your investigation.

STARFLEET SITREP		
Impacted STARFLEET Accounts	Student & Student ID	Marco Giacoppo (104071453)
Chris Pike (Initial account used to gain unauthorized access)  Admin account (Targeted by brute force and successfully compromised)	Class	CL1/10: Mon 10:30 – 12:30
	Tutor	Mr. Fusen Guo
Incident Timeline	Impacted STARFLEET Hosts	
1. 2024-09-09, 08:45:  • <b>Event:</b> Chris Pike received a spear-phishing email containing a malicious document, Lockheed_Martin_JobOpportunities.docx, with a link to download the file. The email was spoofed, appearing to come from a trusted source (mail.fakeemail.com).	1. <b>Impacted Host: Chris Pike’s machine</b>  <b>Severity: High</b> – Spear-phishing initiated the compromise.	

<p>2. <b>2024-09-10, 10:24:</b></p> <ul style="list-style-type: none"><li>• <b>Event:</b> An external IP, 171[.]25[.]193[.]25, used Remote Desktop Protocol (RDP) to log into the STARFLEET Remote Access machine using Chris Pike's account.</li></ul> <p>3. <b>2024-09-10, 12:01:</b></p> <ul style="list-style-type: none"><li>• <b>Event:</b> Internal IP 192.168.100.20 initiated a successful RDP connection to Chris Pike's machine using compromised credentials.</li></ul> <p>4. <b>2024-09-10, 14:35:</b></p> <ul style="list-style-type: none"><li>• <b>Event:</b> The malicious agent.exe was executed on Chris Pike's machine. This execution allowed remote access and enabled malicious activity, such as disabling security measures.</li></ul> <p>5. <b>2024-09-10, 14:45:</b></p> <ul style="list-style-type: none"><li>• <b>Event:</b> A PowerShell script was executed that disabled Windows Defender's real-time monitoring on Chris Pike's machine, allowing agent.exe and other potential malware to execute without detection.</li></ul> <p>6. <b>2024-09-10, 15:00:</b></p> <ul style="list-style-type: none"><li>• <b>Event:</b> Multiple failed login attempts were made to the Admin account on the Domain Controller using RDP from internal IP 192.168.100.20. Eventually, a successful login was achieved, granting the attacker administrative privileges.</li></ul> <p>7. <b>2024-09-10, 15:15:</b></p> <ul style="list-style-type: none"><li>• <b>Event:</b> The RunMe.PS1 PowerShell script was detected on various internal machines, originating from 192.168.100.20. This script disabled real-time protection across several hosts, making them vulnerable to attack.</li></ul> <p>8. <b>2024-09-10, 16:00:</b></p> <ul style="list-style-type: none"><li>• <b>Event:</b> Sensitive file starfleet_secrets.txt was downloaded from an internal machine and exfiltrated to an external IP address, 80[.]67[.]167[.]81.</li></ul> <p>9. <b>2024-09-10, Ongoing:</b></p>	<p>2. <b>Impacted Host: Remote Access machine</b> (Chris Pike's account was compromised).</p> <p><b>Severity: High</b> – Unauthorized access from an external source.</p> <p>3. <b>Impacted Host: Chris Pike's machine</b></p> <p><b>Severity: High</b> – This machine was fully compromised, allowing further unauthorized actions.</p> <p>4. <b>Impacted Host: Chris Pike's machine</b></p> <p><b>Severity: High</b> – This execution opened the door for deeper infiltration into the network.</p> <p>5. <b>Impacted Host: Chris Pike's machine</b></p> <p><b>Severity: High</b> – Security defences were deliberately disabled.</p> <p>6. <b>Impacted Host: Domain Controller</b></p> <p><b>Severity: Critical</b> – The Domain Controller was compromised, potentially giving the attacker control over the entire network.</p> <p>7. <b>Impacted Hosts:</b></p> <p><b>Domain Controller</b> – Severity: <b>Critical</b></p> <p><b>Internal systems across STARFLEET network</b> – Severity: <b>High</b></p> <p>8. <b>Impacted Host: Domain Controller</b> (source of the sensitive file).</p> <p><b>Severity: Critical</b> – Data exfiltration compromised sensitive information.</p>
--	---

<ul style="list-style-type: none"> <li>• <b>Event:</b> The Domain Controller and several other internal devices continued to show signs of compromise, with malicious PowerShell scripts running and unauthorized changes to security policies.</li> </ul>	<p><b>9. Impacted Hosts:</b></p> <ul style="list-style-type: none"> <li>- <b>Domain Controller</b></li> <li>- <b>Chris Pike's machine</b></li> <li>- <b>Internal systems across STARFLEET network</b></li> </ul> <ul style="list-style-type: none"> <li>• <b>Severity: Critical</b> – Systems remain compromised, enabling ongoing malicious activities.</li> </ul>
IoCs Observed	TTPs Observed
<p><b>Files:</b></p> <ul style="list-style-type: none"> <li>• Malicious file hash: SHA256 of agent.exe: d806e3e0c84b0b7208fb4ba9df5cd7b8851abce5c0bbb3ee330560aaa139f243.</li> <li>• Malicious file hash: SHA256 of Lockheed_Martin_JobOpportunities.docx: 0160375e19e606d06f672be6e43f70fa70093d2a30031affd2929a5c446d07c1.</li> <li>• <b>IP addresses involved:</b> <ul style="list-style-type: none"> <li>○ 192.168.100.20 (Internal IP used for unauthorized logins)</li> <li>○ 171[.]25[.]193[.]25 (External IP used for initial access via RDP)</li> <li>○ 80[.]67[.]167[.]81 (External IP used to exfiltrate sensitive data)</li> </ul> </li> <li>• <b>User accounts:</b> <ul style="list-style-type: none"> <li>○ Chris Pike (compromised account)</li> <li>○ Admin (targeted and successfully compromised)</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>• <b>T1486:</b> Data Encrypted for Impact – Indicating ransomware behaviour (files locked and inaccessible).</li> <li>• <b>T1021.001:</b> Remote Services – Unauthorized use of Remote Desktop Protocol (RDP).</li> <li>• <b>T1078:</b> Valid Accounts – Exploitation of legitimate credentials (Chris Pike's and Admin).</li> <li>• <b>T1204.002:</b> Spear Phishing Link – Use of a malicious document (Lockheed_Martin_JobOpportunities.docx) to deliver the initial payload.</li> <li>• <b>T1562.001:</b> Disable or Modify Tools – Disabling Windows Defender real-time protection using PowerShell commands.</li> <li>• <b>T1021:</b> Lateral Movement – Moving from Chris Pike's machine to the Domain Controller and other internal hosts.</li> </ul>
Remediation Advice	

**Immediate Actions:**

Disable the compromised accounts (Chris Pike and Admin) and reset all credentials.

Block external IP addresses involved in the attack, particularly 80.67.167.81.

Review and tighten RDP access policies, ensuring that only authorized users can access it.

**Long-term Actions:**

Implement stronger email filtering and phishing protection to prevent future phishing attacks.

Deploy multi-factor authentication (MFA) to reduce the risk of credential-based attacks.

Regularly monitor network traffic and logs for suspicious activity, particularly remote access via RDP.

Conduct employee awareness training on how to identify phishing emails.

Encrypt sensitive data and restrict access to it based on the principle of least privilege.

**More advice for securing STARFLEET'S systems:**

**Restrict RDP Access:** Limit Remote Desktop Protocol (RDP) access to only trusted devices and implement network-level authentication (NLA).

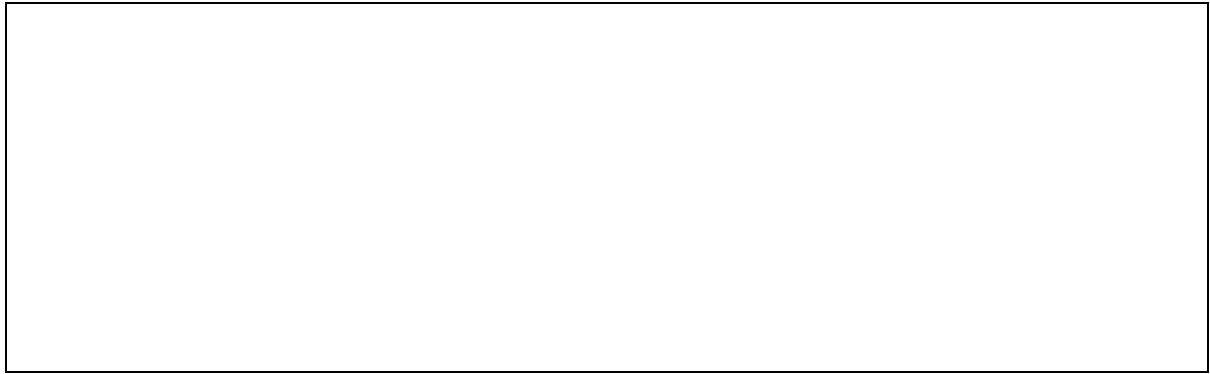
**Improve Email Security:** Deploy advanced email filtering to detect and block phishing emails containing malicious attachments or links.

**Enhance Endpoint Protection:** Re-enable and configure Windows Defender or another advanced endpoint detection and response (EDR) system with strict policies to prevent the execution of malicious scripts and binaries.

**Audit and Monitor Logs:** Regularly audit system logs, especially for critical systems like the Domain Controller, and set up alerts for suspicious activity (e.g., failed login attempts, RDP access).

**Network Segmentation:** Isolate critical infrastructure like the Domain Controller to limit lateral movement in case of a breach.

**Incident Response Plan:** Develop and test a comprehensive incident response plan, including regular simulations of ransomware attacks and data exfiltration incidents.

A large, empty rectangular box with a thin black border, occupying the upper half of the page. It is intended for the student to provide details of the incident.