Attack Path Management Services
Sample Report

Client: ACME Ltd.

March 2022

Table of Contents

SWISS IT SECURITY PART OF SWISS IT SECURITY GROUP

Confidential

The information, data and drawings embodied in this document (collectively the "Document") are strictly confidential and are being furnished solely for informational purposes. They are not to be used for any other purpose or made available to any other person or reproduce in whole or in part without the express prior written consent of XM LTD and SITS-Group. Any form of reproduction, dissemination, copying, disclosure, modification, distribution and or publication of the Document is strictly prohibited. This Document was prepared by the SITS-Group and contains selected information pertaining to XM LTD and SITS-Group and does not purport to be all-inclusive. Neither XM LTD and SITS-Group nor any of its respective officers or employees make any representation or warranty, expressed or implied, as to the accuracy or completeness of this Document and no legal commitments or obligations shall arise by reason of this Document.

Attack Path Management - Defence by Offense

Attack Path Management (APM) Services, powered by the XM Cyber platform, provide the first fully automated APT (Advanced Persistent Threat) Simulation Platform to continuously expose all attack vectors from breach point to any critical organisational asset above and below the surface. This continuous loop of automated red teaming is completed by ongoing and prioritised actionable remediation of security gaps. APM Services operate as an automated purple team that fluidly combines red team and blue team processes to ensure that organisations are always one step ahead of hackers.
Attack Path Management Services provide organisations with a clear, up-to-date understanding of where and how hackers can (and will) infiltrate their network and compromise critical assets. The platform is meticulously designed to work safely in an organisational network, simulating malicious methods without disrupting network availability or causing harm to critical assets.

Attack Path Management Services – Features

- Automated generation of actionable and prioritised remediation reports
- Customised attack scenarios from any starting point to any target asset
- Comprehensive and up-to-date attack methods
- Fully secure simulation based on actual user actions implemented in real-time
- Detailed visual display of the attacker path(s) to critical assets
- Comprehensive reports on organisation cybersecurity status and posture

How does the Platform do it?

XM Cyber has found a way to perform simulations using a small software (sensor) that collects information safely and securely without impacting the host/network. This is possible by continuously checking conditions on machines as an attacker would. The simulation is done by checking the conditions on all devices and then performing calculations in the DB. If the calculation result is confirmed, the platform show that an attack is possible. These include user activity, misconfigurations, and vulnerabilities. The platform does not trigger alerts or test the existing security controls during simulations, just like an actual attacker would.

What's in it for the ACME Ltd.?

- Factual cyber risk management based on actual risks in the infrastructure
- Prioritise the IT tasks and optimise work effort
- Personal, civil, and criminal risk mitigation
- Prevent attacks and dramatically save costs
- Shine a light, a continuous MRI, on security blind spots in your infrastructure
- Laser focus on security issues that directly affect Business Assets

PART OF SWISS IT SECURITY GROUP

Executive Summary

Summary

SITS-Group and ACME Ltd. (the client) commenced an assessment of the platform to identify the value to the organisation. Different attack scenarios towards the critical assets have been identified in the scope below and were configured. The platform identified ways to move laterally and compromise devices and assets within the scope provided.

The remediation actions taken during the assessment and others suggested in this report are prioritised to close attack paths and increase the overall security posture of the devices in scope. The platform offers the ability to continuously assess the client's environment for any changes to IT hygiene, vulnerabilities, and user behaviours that might expose current and future devices and assets to risks those attackers can leverage.

Participants

1. Client

Project/Business Owner & Stakeholders:	John Doe
Technical Responsible:	Gwen Jones, Lori Lead
Technical Team:	Sandra Gardner, Jo Hess, Mary Hilt

2. SITS-Group

Regional Sales Director:	Roberto Southwood
Technical Director:	Laura J Foster

Scope

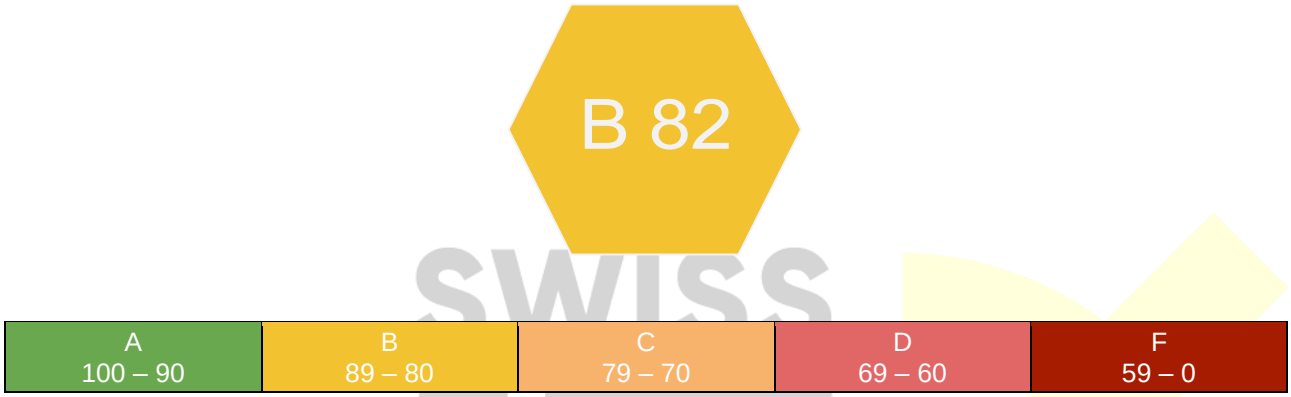
Both a timeframe as well as IT assets that are used productively have been selected as follows:

- The assessment started on the 15th of February 2022 until the 05th of March 2022
- The data gathering for this report was conducted on the 05th of March 2022
- In total only 412 different assets (~1%) from the client's environment were covered.
  - 105 of 412 was Microsoft Windows Clients (e.g., Windows 7 / 10 devices)
  - 37 of 412 was Microsoft Windows Servers (e.g., 2012-2019) with different roles
  - 178 of 412 were AWS Cloud entities
  - 92 of 412 were Azure Cloud entities

SWISS IT SECURITY PART OF SWISS IT SECURITY GROUP

Overall Security Score

The platform has developed a unique algorithm to calculate the Security Score of a company by focusing on the risk to Critical Assets and how complex it can be to compromise Critical Assets. The lower the number, the higher the risk. After the execution, the platform rated the client's environment as follows.



The Security Score represents the holistic overview of the overall Security Posture. The Security Score is the average score of all different attack scenarios together. Each scenario's score is measured by how many critical assets have an attack path towards them and their complexity.

Scenario Name	Security Score - Grade	Security Score - Number
Risk from Clients to Domain Controllers	F	25
Risk from Clients to AWS	B	85
Risk from Clients to Azure	C	78
Risk from Cloud to Cloud	A	98
Risk from Supply Chain Connections	B	89

Conclusion

It is important to outline that the assessment was conducted only over a short period with just a small subset of the client's assets. However, the platform has proven - safely and securely - that the client's critical assets are vulnerable to several attack techniques.

Only the continuous assessment of the entire client organisation will show all attack paths to critical assets. This is due to an ever-changing landscape of IT environments, dynamic network changes, Cloud environments, and new attack techniques.

In addition, all scenarios need to be aligned to the critical business questions and then be executed regularly following the process below.

Recommendation

The following recommendations have been clustered in Short Term (1-2 months), Mid Term (3- 4 months) as well as Long Term (4+ months & continued) activities:

Short Term Recommendations

- The client's IT Security & IT, Operation teams to examine remediation options for the key findings
- APM Services Deployment Planning
  - Deployment Phasing, Roles & Responsibilities, Milestones, and next Quick Wins
- Deployment Workshops
  - Further scenario definition aligned with critical business and IT KPIs, detailed design, operational process definition

Mid Term Recommendations

- APM Services Deployment
  - The rollout of the Sensor, Integration with the existing ecosystem, and 3rd Party applications at the client (e.g., Log Management / SIEM, VM Scanner, EDRs, etc.)
- Execution of the initial and holistic client Attack Simulation across the entire organisation
- Platform Admin & Operational Training for the client Teams

SECURITY
PART OF SWISS IT SECURITY GROUP

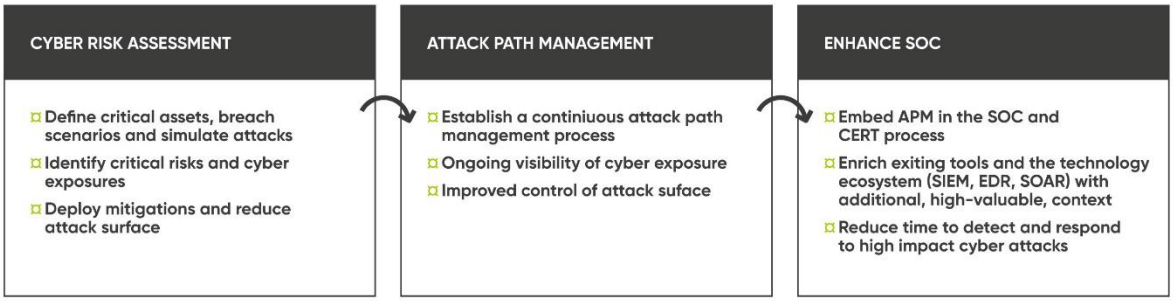
Long Term Recommendations

- Operational Continuous Attack Path Management towards critical assets
- Risk Remediation Project to furtherly increase and improve the overall Security Posture

Attack Path Management Services from SITS-Group would fully support all Short Term, Mid Term, and Long-Term Recommendations activities. Furthermore, SITS-Group can provide additional resources through its holistic Support Programme with Customer Operation Managers.

Typical Client Journey with Attack Path Management Services

Following the overall recommendations, APM Services successfully helped a vast set of clients to develop, enhance and implement a holistic Cyber Security Programme. The typical client journey can be outlined in three different phases, where SITS-Group will support each phase and its Customer Success Managers dedicated to our clients.



SWISS SECURITY PART OF SWISS IT SECURITY GROUP

Technical Summary

Scenarios – Definition and Findings

APM Services can answer whether critical assets in an organisational network are secured continuously and align the scenarios with Risk Management answering Business Demands.
With each definition and execution of a scenario, APM Services highlight:

- If the critical assets can be compromised,
- the Attack Path towards the critical assets,
- the compromise rate of the client's network as well as,
- the time it took to run the scenario and compromise the critical assets.

The following scenarios were identified:

1. The Risk from Clients to Domain Controllers

With this specific scenario, the platform outlines how an attacker can move laterally and escalate its privileges from a default client user and computer (i.e., client's employee) to compromise Domain Controllers as critical assets.

- Are the critical assets secure? No, all critical assets are compromised.
- This scenario shows a compromise rate of up to 87% of the entire network in scope.
- From the initial breach to compromising the critical assets, it took 2 hours and 5 mins.

2. The Risk from Clients to AWS

With this specific scenario, the platform outlines how an attacker can move laterally from a default client user and computer (i.e., client's employee) and compromise any AWS entities as critical assets.

- Are the critical assets secure? No, some of the critical assets are compromised.
- This scenario shows a compromise rate of up to 21% of the entire network in scope.
- From the initial breach to compromising the critical assets, it took 10 mins.

3. The Risk from Clients to Azure

With this specific scenario, the platform outlines how an attacker can move laterally from a default client user and computer (i.e., client's employee) and compromise any Azure entitles as critical assets.

- Are the critical assets secure? No, some of the critical assets are compromised.
- This scenario shows a compromise rate of up to 45% of the entire network in scope.
- From the initial breach to compromising the critical assets, it took 7 mins.

4. The Risk from Cloud to Cloud

With this specific scenario, the platform outlines how an attacker can move laterally from one Cloud environment (e.g., AWS) towards the other Cloud environment (e.g., Azure) and compromise entities respectively.

- Are the critical assets secure? Yes, all critical assets are secured.
- This scenario shows a compromise rate of up to 2% of the entire network in scope.

5. The Risk from Supply Chain Connections

With this specific scenario, the platform will outline how an attacker can take over a 3rd Party Connection and compromise any internal critical asset. This is reflecting a Supply Chain Attack.

- Are the critical assets secure? No, some of the critical assets are compromised.
- This scenario shows a compromise rate of up to 51% of the entire network in scope.
- From the initial breach to compromising the critical assets, it took 37 mins.

Scope - Sensor Rollout

As per the agreement between the client and SITS-Group, the scope was defined as follows.

Device Type	Assets	Count
Microsoft Windows[1]	Workstations	
	• Number of Microsoft Windows 7:	7
	• Number of Microsoft Windows 10:	98
	Servers	
	• Number of Microsoft Windows Server 2012:	2
	• Number of Microsoft Windows Server 2012 R2:	24
	• Number of Microsoft Windows Server 2016:	5
	• Number of Microsoft Windows Server 2019:	6
Linux/Unix	*None in scope*	2
Apple macOS	*None in scope*	–

[1] For easier readability and structure, subversions, or specific OS roles (e.g., DC) of each Operating System are summarized under each top operating system

Scope – Integrations

As per the agreement between the client and SITS-Group, the following integrations were planned.

Integration Type	Assets	Count
AWS Entities	*AWS EC2 Instances, S3 Buckets, Lambda*	*178*
Microsoft Azure Entities	Azure VMs, Blob Storage/Containers, Serverless-Code	*92*
EDR Integration	*None in scope*	–
SIEM Integration	*None in scope*	–
SOAR Integration	*None in scope*	–

SWISS IT SECURITY
PART OF SWISS IT SECURITY GROUP

Timeline

Phase Name	Details	Start and Due date
Planning	Scope agreement Sensor deployment plan Sensor exclusions	15th of February 2022
Set-Up	Sensor distribution Connecting cloud entities*	17th of February 2022
Kick-off	Define risk scenarios KPI and Success Criteria agreement	18th of February 2022
Tech-Review Follow up #1	Discuss findings, answer questions, and possible remediations activities	23rd of February 2022
Tech Review Follow up #2	Discuss findings, answer questions, and possible remediations activities	28th of February 2022
Data Gathering[2]	Date & Time for Data Gathering that has been used in this report	05th of February 2022
Presentation & Summary	Review Summary report Summary presentation	07th of February 2022

[2] This is the point in time when the data has been gathered and the report authoring has been started. Scenarios and campaigns were still executed until the Presentation & Summary Discussion, hence latest numbers and statistics may have been changed

Quick Wins

During the assessment, remediation, and quick wins to increase the Security Level were already discussed and implemented by the client's technical team.

Several attack vectors are now closed with the remediations implemented that could compromise the client's critical assets.

However, other attack techniques remain open and active as implementing the remediations would have taken longer than the timeframe. It is essential to assess and remediate those attack techniques continuously. SITS-Group guides the remediation of attack techniques with the highest impact throughout this document, including "Simulated Remediation".

SWISS IT SECURITY
PART OF SWISS IT SECURITY GROUP

Success Criteria

During the Kick-Off, the client and SITS-Group have agreed on some Success Criteria. The table below shows the result of the Success Criteria.

Success Criteria	Pass	Fail	Note
SC1	✓	–	The platform has shown through several scenarios that various critical assets (e.g., Domain Controllers) are currently at high risk and increased likelihood of being compromised.
SC2	✓	–	The platform was able to show attack vectors with attack technique details towards critical assets.
SC3.1	✓	–	The platform is unaware of any events related to the Sensor or its task to impact the rolled-out endpoints.
SC3.2	✓	–	The platform is unaware of any events related to the platform activity, scenarios, or campaigns to have had any performance impact.
SC3.3	✓	–	The platform is unaware of any events related to the platform activity, scenarios, or campaigns to have impacted the environment.
SC3.4	✓	–	The platform is not aware of any events related to the operation of platform, carried out scenarios and tests to have had *any* impact on the environment.
SC4	✓	–	The platform was able to show pivoting points or hubs (so-called Choke Points) within the network through which a majority of attack paths traverse.
SC5	✓	–	The platform was able to show attack vectors and attack techniques that are related to risky user activity, software vulnerabilities as well as misconfigurations (or bad IT hygiene)
SC6	✓	–	The platform showed shared/cached credentials to accounts used on several machines and highlighted critical assets at risk.

SWISS IT SECURITY PART OF SWISS IT SECURITY GROUP

Remediation Plan

This chapter outlines the Remediation Plan for the client to achieve the portrayed & simulated Remediation scores[3].

Each link gives technical insights into each of the Attack Techniques, its Description, the Impact, Remediation Steps, and the top results of affected machines/entities.

ID	Attack Technique	Scope	Further References[4]
1	Domain Credentials	acme.com\Administrator acme.com\IT-Support acme.com\BackupAdmin	*Platform Link*
2	File Infectors & Taint Shared Content	\\ACME-FS1.acme.com\SharedDrive\Book1.xlsx	*Platform Link*
3	DHCPv6 DNS Poisoning	ACME-FS1.acme.com ACME-DC1.acme.com ACME-SQL1.acme.com ACME-WKS2.acme.com	*Platform Link*

The exact remediation steps are described (incl. free text, screenshots, and further references to vendors like Microsoft) for each option available within the platform.

The Discovery Technique „Network Reachability" has been excluded from the list above to focus on the security-related Attack Techniques.

[3] In the defined Scope.

[4] Please note that access has been granted to the Technical Team during the timeframe. Access may not work from all networks due to security reasons

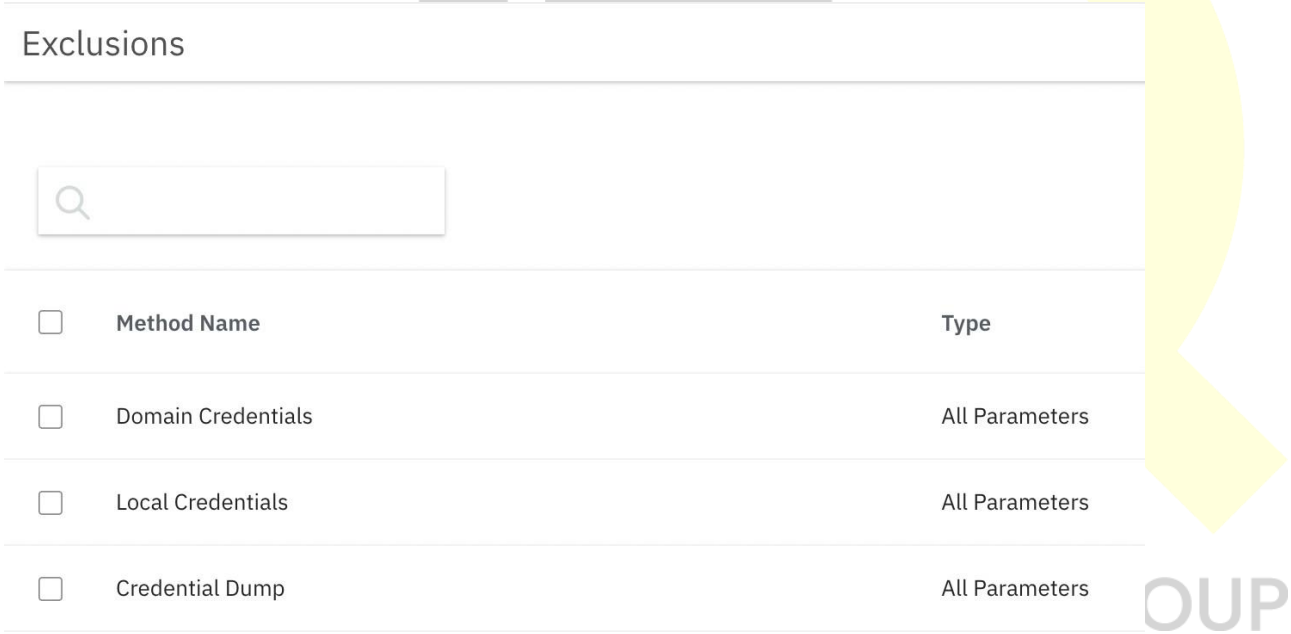
Simulated Remediation

Following the Tech Review Sessions during the timeline and additional meetings beyond, the client and the SITS-Group team have identified remediation activities to increase the environment's Security Level.

Due to the limited timeframe, those recommendations were not yet implemented.
However, through simulated remediation, the platform can showcase the result of the remediation for each attack technique. This is based on exclusions of Attack Techniques for each Scenario.

Overview

- The Scenario, “Risk from Clients to Domain Controllers”, has been chosen for the Simulated Remediation
- The following Attack Techniques have been chosen for the Simulated Remediation
  - Domain Credentials
  - Local Credentials and
  - Credential Dump



Before the simulated remediation

Based on the criticality and the impact on the client's environment, the attack mentioned beforehand should be remediated.

Before remediation

Results
73% of the network is compromised 78% of all critical assets are compromised

Campaign Security Score
D – 68

Assets from the following Domains can be compromised
acme.com, office.acme.com

Assets from the following Domains cannot be compromised
security.acme.com

SECURITY
PART OF SWISS IT SECURITY GROUP

After the simulated remediation

After simulated remediation:

Results
7% of the network is compromised 13% of all critical assets are compromised

Campaign Security Score
B – 87

Assets from the following Domains can be compromised
office.acme.com

Assets from the following Domains cannot be compromised
security.acme.com, acme.com

SECURITY
PART OF SWISS IT SECURITY GROUP

Conclusion of Recommendations & Simulated Remediation

As seen above, implementing the remediations for the outlined Attack Techniques can increase the Security Level even further.

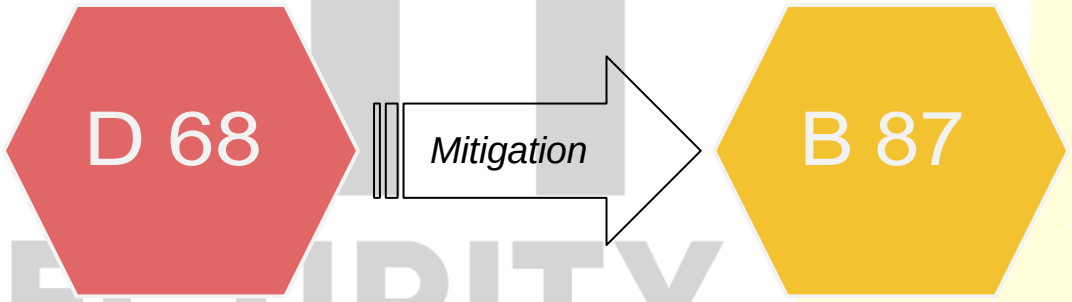
Current Production[5] Statistics:

- 73% of the network is compromised
- 78% of all critical assets are compromised
- Security Score: D – 68

Simulated Remediation Statistics:

- 7% of the network is compromised (improvement by 66%)
- 13% of the Critical Assets are compromised (improvement by 65%)
- Security Score: B – 87 (improvement by 19%)

The simulated implementation of the remediations shows not only the overall impact to the network and the critical assets but also the elevation of the Security Score has also been observed:



[5] In the scope of the assessment

Attack Vector Visualizations by the Platform

This chapter gives insight and graphical visualisation from any defined Breach Points towards the critical assets. These represent only specific examples as there were more attack paths available.

For this chapter, only one scenario has been taken as an example – all other open attack vectors are continuously evaluated in the platform. Moreover, they can be investigated interactively as well.

Scenario: Risk from Clients to Domain Controllers (00001)

Breach Point:	WKS1.acme.com
Critical Asset:	ACME-DC1.acme.com
Compromise Methods:	Domain Credentials, PrintNightmare – Windows Print Spooler (CVE-2021-34527)
Harvested User Accounts:	acme.com\IT-Support Attack Steps needed: 2

Battleground:

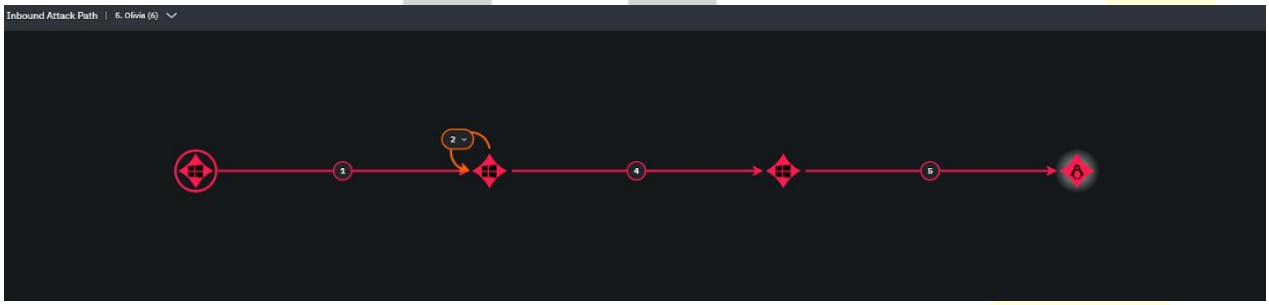
Inbound Attack Path:

1. Domain Credentials (acme.com\IT-Support)
2. PrintNightmare - Windows Print Spooler (CVE-2021-34527)

Outbound Attack Path:

After an attacker can compromise the critical asset ACME-DC1.acme.com, outbound attack paths are being opened so that an attacker can use that to compromise other assets.

In the following case, ACME-DC1.acme.com is being used to compromise ACME- FS1.acme.com.



1. Domain Credentials (acme.com\IT-Support)
2. Credential Harvesting (acme.com\Administrator)
3. Credential Reuse (acme.com\IT-Support)
4. PrintNightmare - Windows Print Spooler (CVE-2021-34527)
5. Oracle DB Known Passwords

SWISS IT SECURITY PART OF SWISS IT SECURITY GROUP

Top Critical Assets at Risk

As per the definition of each scenario, the following critical assets have been identified with the client's technical team. The table below shows the top 5 Critical Assets at risk.

Name – Critical Asset	Top Compromising Methods	Recommended Remediation
ACME-DC1.acme.com	Domain Credentials | Local Credentials | Credentials Relay | BlueKeep (CVE-2019-0708)	BlueKeep - Apply Patch
ACME-SQL1.acme.com	Domain Credentials | Local Credentials | Credentials Relay	
ACME-FS1.acme.com	Domain Credentials | Credentials Relay	Local Credentials: Disable User User1
ACME-SRV1.acme.com	Domain Credentials | Local Credentials	Remove Users from Administrators Group
ACME-SRV2.acme.com	Domain Credentials | Local Credentials | BlueKeep (CVE-2019-0708)	Local Credentials: Disable User User1

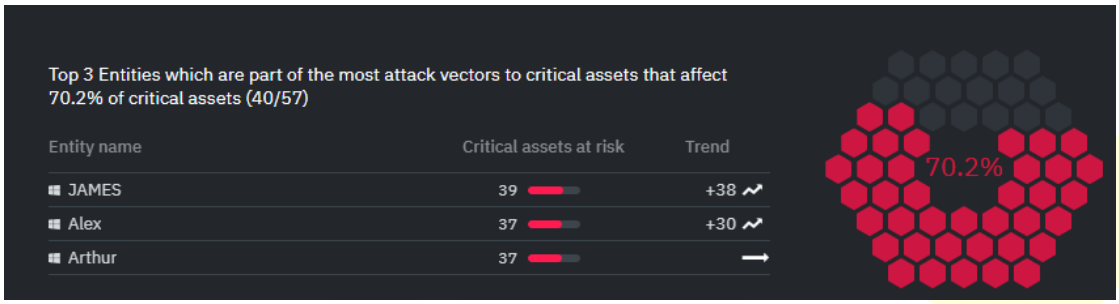
The full report for the Critical Assets is located here: *XM Cyber Hyperlink*

SWISS IT SECURITY
PART OF SWISS IT SECURITY GROUP

Top Choke Points

A chokepoint is an entity that is part of the most attack vectors towards critical assets. Pivotal points in the environment create bottlenecks and impact many entities from a single location.
Mitigating risks and implementing remediations on those entities first will enable the client "to do more with less" - this is high-impact remediation.

The following are the top 3 choke points that take part in the most attack vectors to affect 70.2% of the client's critical assets.



The table and graph below show the top 5 choke points and the impact on the entities and critical assets in the environment; the complexity of the attack vector sorts the table.

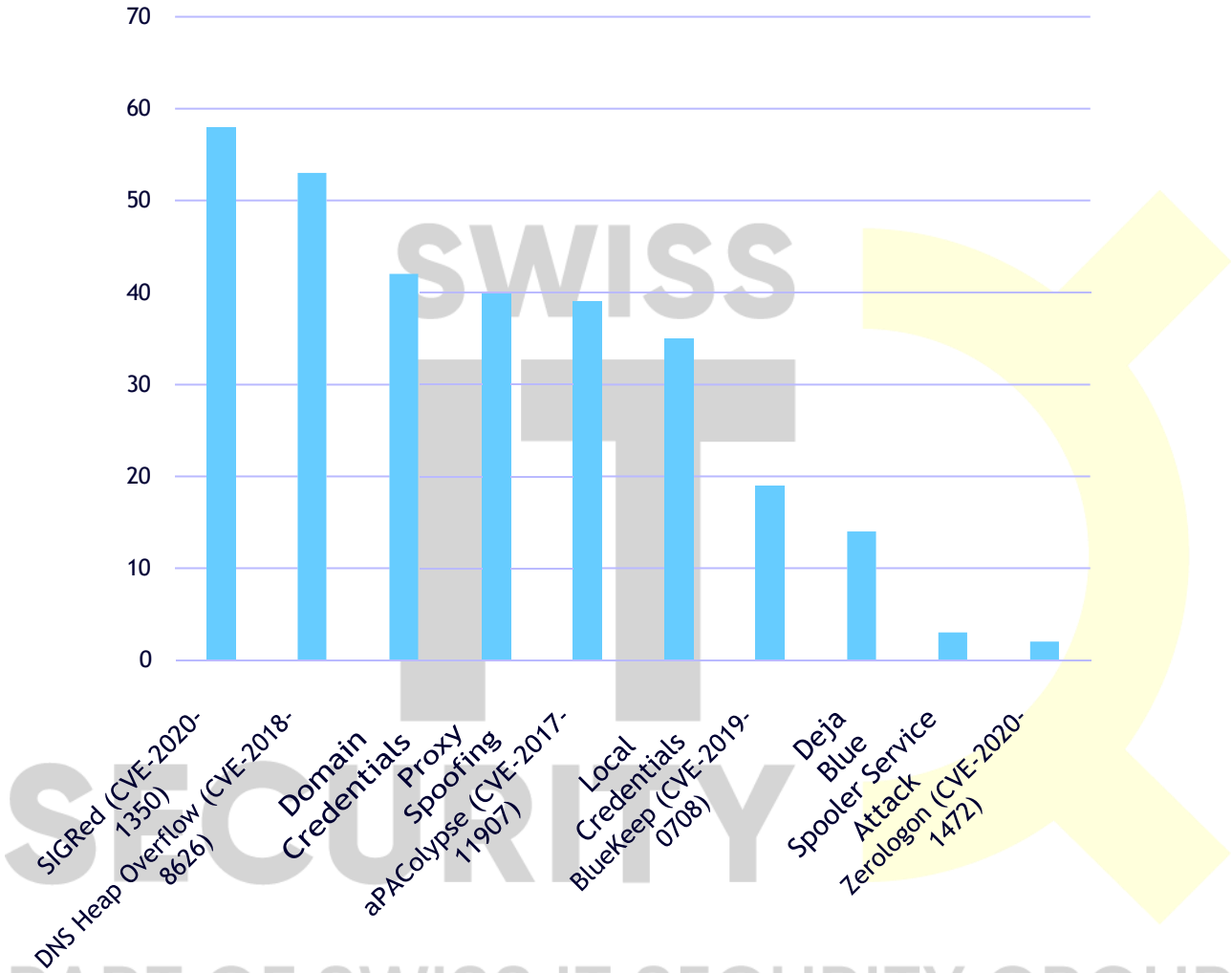
Name – Choke Point	Top Compromising Methods	Critical Assets at Risk ↓	Affected Entities
WKS1.acme.com	Domain Credentials | Local Credentials | Credentials Relay | BlueKeep (CVE- 2019-0708)	25	38
JUMPHOST1.acme.co m	Domain Credentials | Local Credentials | Credentials Relay | BlueKeep (CVE- 2019-0708)	23	25
KIOSK.acme.com	Domain Credentials | Local Credentials | Credentials Relay	12	15
HOST1.acme.com	Domain Credentials | Local Credentials	11	12
HOST2.acme.com	Domain Credentials | Local Credentials | BlueKeep (CVE-2019-0708)	8	11

The full report for the Choke Points is located here: *Platform Hyperlink*

SECURITY
PART OF SWISS IT SECURITY GROUP

Top Impacting Attack Techniques & Categories

The platform uses different Attack Techniques safely and securely to show and visualise the attack vectors towards assets and entities within the client's organisation. The graph below shows the top 10 impacting Attack Techniques towards critical assets.



SWISS IT SECURITY
PART OF SWISS IT SECURITY GROUP

Top Impacted Users

Attackers use domain, SQL, and other credentials to move laterally in environments. Reducing the administrator or privileged access for credentials and protecting the accounts from being harvested will minimise the risk of credential attacks.

The credentials below were not brute-forced, cracked (i.e., no evaluation of weak passwords), or any other invasive way gathered. However, with Credential Harvesting Technique, an attacker can find those credentials (e.g., in Machine Memory/RAM), dump password hashes, and revert them to actual passwords within split seconds.

Domain Credentials

Name – Domain Credentials	Domain	Found on X devices ↓	Critical Assets at Risk	Affected Entities
Marry	ACME.COM	20	29	96
Harry	ACME.COM	15	29	91
Mike	ACME.COM	8	29	41
John	ACME.COM	7	27	17
Administrator	ACME.COM	6	6	17

Local Credentials

Name – Local Credentials	Number of Hosts	Critical Assets at Risk	Affected Entities
Administrator	#6	29	96
Helpdesk	#4	29	91
Backupadmin	#3	29	41

SWISS IT SECURITY PART OF SWISS IT SECURITY GROUP


SWISS
IT
SECURITY
PART OF SWISS IT SECURITY GROUP