# Identification and Scoping

## Introduction

Welcome to the Identification and Scoping phase of the TryHackMe Incident Response module. Just as you've joined us at SwiftSpend Financial (SSF), we've already received notifications about a potential security compromise. There's no time to lose - we must promptly identify the nature of the breach and the scope of its extent!

In this room, we will introduce you to a crucial tool for incident response - the Spreadsheet of Doom (SoD), a comprehensive directory of malicious indicators that can streamline our investigation process.

Learning Objectives

This room covers how we identify and scope security incidents, interpret security alerts and logs, gather additional evidence, and effectively use the Asset Inventory and Spreadsheet of Doom to identify and scope the extent of a security incident.

Identify the nature of security alerts.
Understand the process of gathering additional evidence.
Learn the importance of having an Asset Inventory and the Spreadsheet of Doom in incident response.
Discover how to scope the extent of a security compromise.
Understand the feedback loop between Identification and Scoping in incident response.
Room Prerequisites

Before starting with this room, we recommend you clear the Preparation room, the first part of our Incident Response module.

Join us in this immersive module, where you will develop the expertise needed to promptly identify security compromises and scope their extent, fortifying the security posture of assets across diverse platforms.

## Identification: Unearthing the Existence of a Security Incident

### Connecting to the machine

Start the virtual machine in split-screen view by clicking the green Start Machine button on the upper right section of this task. If the VM is not visible, use the blue Show Split

View button at the top-right of the page. Alternatively, you can connect to the VM via RDP using the credentials below if Split View does not work.

THM Key Credentials

- Username analyst
- Password DFIR321!
- IP MACHINE_IP

IMPORTANT: The attached VM contains artefacts to help us better understand a Security Incident from detection to resolution. Work on the subsequent tasks and experiment with the VM through a case example. Microsoft Outlook will start on its own. Kindly ignore the activation key window by pressing Back, and then proceed by clicking Skip sign in for now ▶️ Use as view only. When asked for a license, click X, for optional data, click Next ▶️ Don't send optional data ▶️ Done in the subsequent pop-up windows.

The Identification phase forms the bedrock of the Incident Response Process. This critical phase combines the technical detection of potential security incidents with the inherent human capacity to recognise and report them.

The speed at which an organisation can spot an incident directly correlates with the pace of response, potentially limiting the damage and shortening recovery time.

**The Triad of Identification: People, Process, and Technology**
Identification is a harmonious concert between people, processes, and technology.

While technology offers the tools to detect potential incidents through alerts, people must interpret these alerts and adhere to established procedures to ensure incidents are correctly identified and managed.

Moreover, all, not solely the IT or Security teams, must report any anomalies and ensure that the relevant parties are alerted by following the appropriate procedures.

Consequently, the success of the identification phase rests on a well-coordinated collaboration among these three elements.

**Understanding Security Alerts and Event Notifications**
Security Alerts, also referred to as Event Notifications, are crucial signals that may hint at the presence of a potential threat or the occurrence of an actual security incident.

These are pivotal in triggering the Incident Response Process and ensuring security and safety.

Understanding the nature of these alerts, including their type and severity, is vital in guiding the incident response process. This understanding is nurtured through technical expertise, effective use of security tools, and a culture of continuous learning and vigilance.

Following the proper procedures when handling these alerts ensures that the right individuals are alerted, bolstering incident response effectiveness.

**Leveraging Technical Expertise and Security Tools**
Effective incident response relies on timely reporting, staff proficiency, and strategic use of security technologies.

Therefore, it's crucial that all employees of an organisation, technical or otherwise, stay alert and promptly report any suspicious activities or anomalies through the appropriate communication channels.

Employing robust security technologies can significantly enhance the detection and deterrence of potential threats, ensuring rapid recognition and response to situations that may escalate into actual security incidents.

It is why TryHackMe is dedicated to supporting those pursuing a career in Blue teaming to master security tools by offering a platform that can aid individuals in developing proficiency in areas specific to Security Operations and Incident Response tooling, such as the following:

- Endpoint Detection and Response (EDR)
    - Intro to Endpoint Security
    - Aurora EDR
    - Wazuh

- Intrusion Detection and Prevention Systems (IDPS)
    - Snort
    - Snort Challenge - The Basics
    - Snort Challenge - Live Attacks

- Security Information and Event Management (SIEM)
    - Investigating with ELK 101
    - Splunk: Basics

- Incident handling with Splunk

Recognising that these security tools truly flourish in the hands of skilled individuals with the necessary information and technical expertise to combat potential threats and manage security incidents is vital.

However, effective communication channels are just as essential to ensure that the right people are quickly alerted with accurate and precise information, which enables them to conduct an investigation and initiate the incident response process, made possible only by well-designed procedures that both technical and non-technical staff can swiftly and seamlessly follow.

**Promoting a Culture of Learning and Vigilance**
Cultivating a culture of learning and vigilance is a top-down initiative. Executive management must prioritise and invest in cyber security, setting clear expectations for following the correct procedures.

Regular education and awareness campaigns can equip personnel to identify and report suspicious activity or technical anomalies they may encounter, contributing to the overall effectiveness of the incident response process.

Moreover, comprehensive policies and procedures related to incident response and reporting, guided by legal counsel, can underscore the importance of following the right procedures in identifying security incidents and communicating them effectively, thereby alerting the relevant people with the necessary information that will enable them to address issues.

**Transitioning from Identification to Scoping**
Once an incident has been identified, the subsequent step is determining its scope.

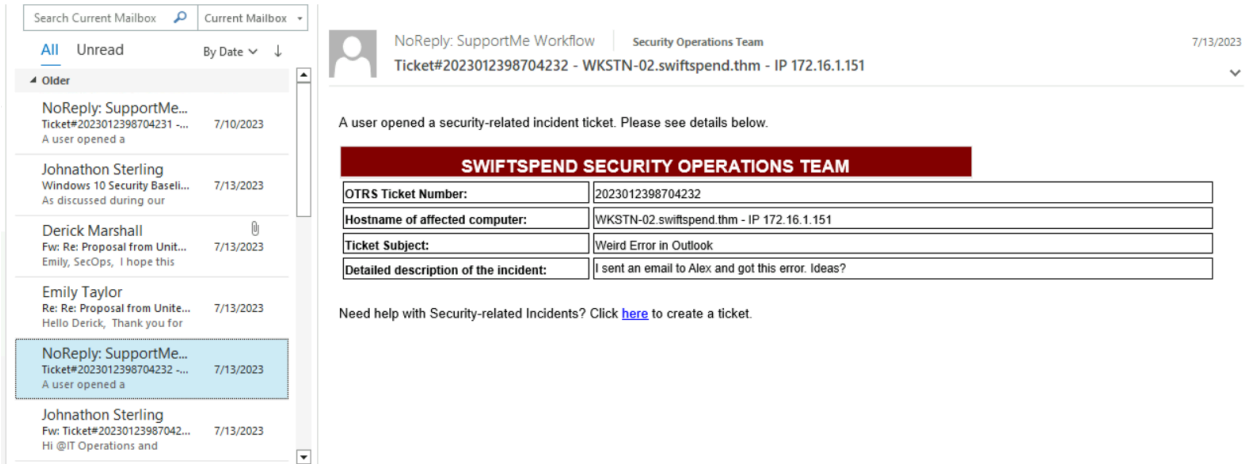
Scoping involves grasping the extent of the incident, including which systems are affected, what data is at risk, and how the incident impacts the organisation.

The transition from identification to scoping is crucial in the Incident Response Process, demanding clear communication, effective collaboration, and a well-defined process. The insights gained from the identification phase will prove instrumental in facilitating this transition and strengthening the effectiveness of the incident response process.

**********

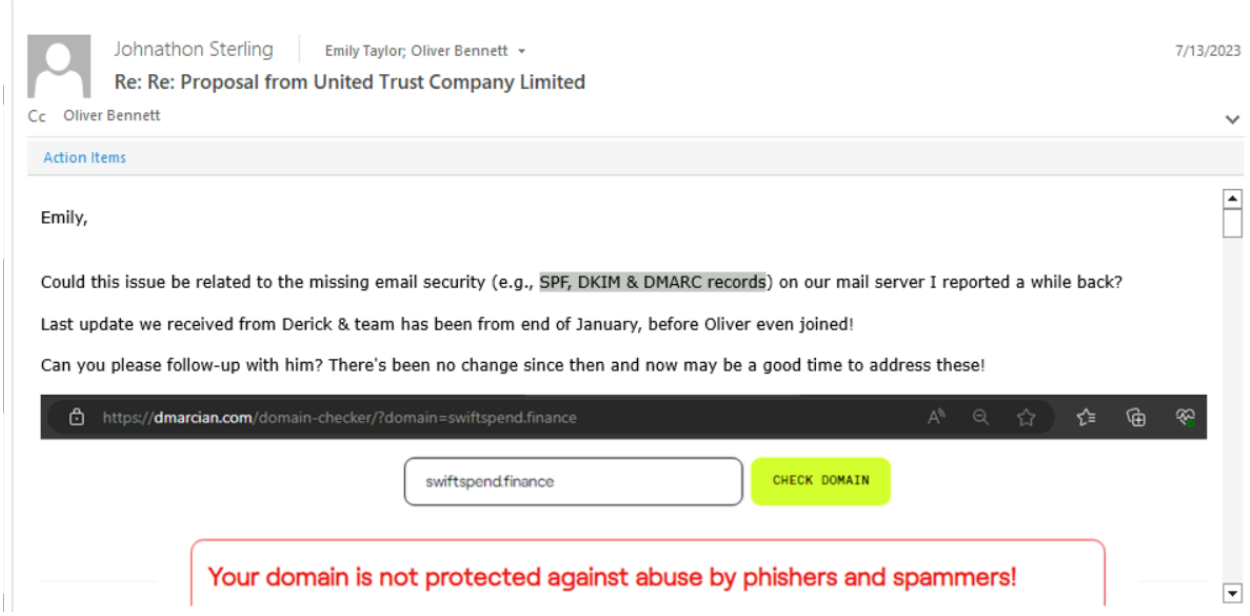
**Answer the questions below:**

**What is the Subject of Ticket#20230123987042 32?**



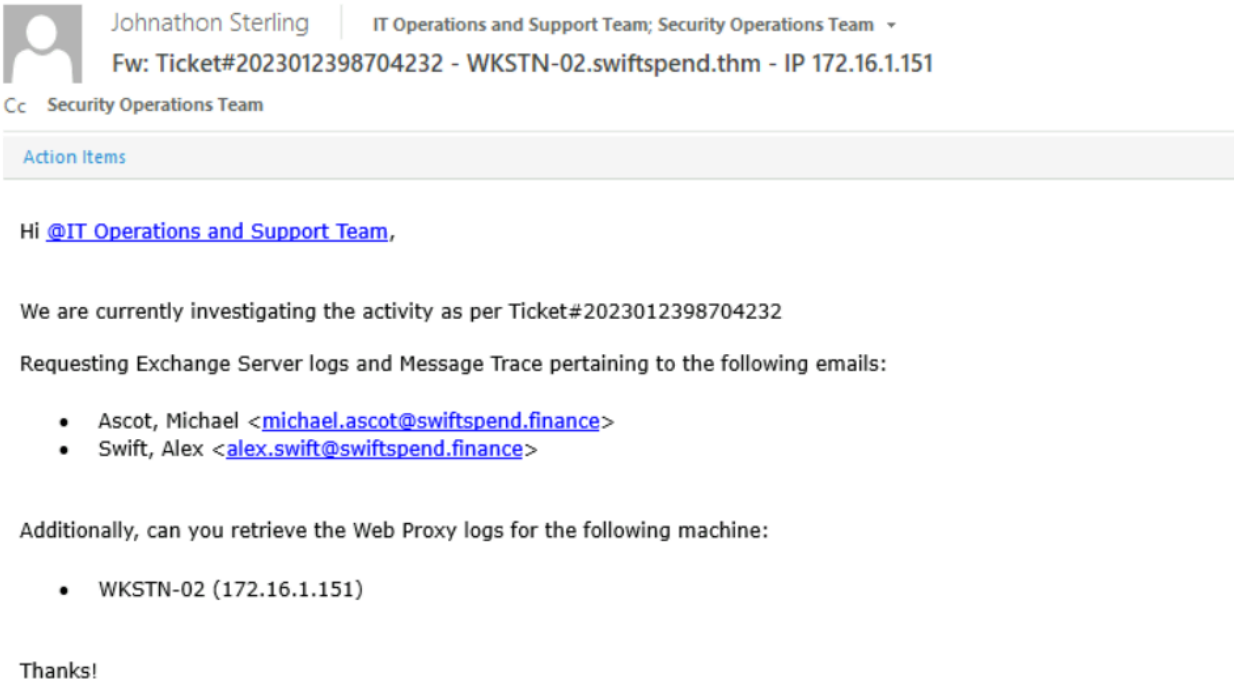

Answer: Weird Error in Outlook

**According to your colleague John, the issue outlined on Ticket#2023012398704232 could be related to what?**




Wasn't found directly in the email thread pertaining to the ticket but searching through all the emails the answer was found.
Answer: SPF, DKIM & DMARC records

**Your colleague requested what kind of data pertaining to the machine WKSTN-02?**



Johnathon Sterling | IT Operations and Support Team; Security Operations Team

Fw: Ticket#2023012398704232 - WKSTN-02.swiftspend.thm - IP 172.16.1.151

Cc Security Operations Team

Action Items

Hi @IT Operations and Support Team,

We are currently investigating the activity as per Ticket#2023012398704232

Requesting Exchange Server logs and Message Trace pertaining to the following emails:

- Ascot, Michael <michael.ascot@swiftspend.finance>
- Swift, Alex <alex.swift@swiftspend.finance>

Additionally, can you retrieve the Web Proxy logs for the following machine:

- WKSTN-02 (172.16.1.151)

Thanks!

Answer: Web Proxy logs

## Scoping: Understanding the Extent of a Security Incident

After identification, the next critical step in the Incident Response Process is Scoping, which involves determining the extent of a security incident, including identifying the affected systems, the type of data at risk, and the potential impact on the organisation.

Scoping is essential as it guides the subsequent steps of the response process and helps formulate an effective mitigation strategy.

### The Asset Inventory: A Quick Reference for Incident Response

The Asset Inventory is a crucial tool in the incident response process. It provides a comprehensive list of all the organisation's assets, aiding in identifying and scoping potential threats. Let's look at a simple representation of the Asset Inventory.

| Asset Type | Asset Name | IP Address | Operating System | Owner |
|---|---|---|---|---|
| Domain Controller | DC-01 | 172.16.1.10 | Windows Server 2019 | Derick Marshall |

| | | | | |
|---|---|---|---|---|
| Mail Server | MAILSVR-01 | 172.16.1.15 | Windows Server 2019 | Stan Simon |
| Web Server | WEBSVR-01 | 172.16.1.110 | Ubuntu Server 20.04 | Damian Hall |
| Proxy Server | PROXY-01 | 172.16.1.119 | Windows Server 2019 | Stan Simon |
| Workstation | WKSTN-02 | 172.16.1.151 | Windows 10 Pro | Michael Ascot |
| Laptop | LPTP-01 | 172.16.1.153 | Windows 10 Pro | Derick Marshall |

**The Spreadsheet of Doom (SoD): Enriching Artefacts for Effective Incident Response**

Identifying, understanding, and responding to potential threats within the known scope of a security incident as swiftly as possible is critical.

The Spreadsheet of Doom (SoD) is designed to aid in these processes, acting as a consolidated, organised source of information about known threats.
It serves as a single reference point, accelerating the incident response procedure.
Each row in this spreadsheet is representative of a unique threat identifier or an Indicator of Compromise (IoC).

| **Indicator Type** | **Indicator** | **Threat Type** | **Source** |
|---|---|---|---|
| IP Address | 188.40.75.132 | Malware Hosting | AlienVault OTX |
| Domain | b24b-158-62-19-6.ngrok-free.app | Phishing Domain | Ticket#2023012398704232 |
| Email Address | alex.swift@swiftspend.finance | Spoofed Email | Ticket#2023012398704232 |
| Email Address | mike.ascot@swiftspend.finance | Spoofed Email | Ticket#2023012398704232 |
| Domain | groupmarketingonline.icu | Phishing Domain | VirusTotal |
| File Hash(SHA 1) | 75ec7d0d1b6b2b4c816cbc1b71cd0f8f06bd8c1b | Malware | ThreatCrowd |

The SoD is essentially a structured list of IoCs, including IP addresses, domain names, URLs, file hashes, and more associated with malicious activity. The data in this spreadsheet is enriched with additional information about each IoC, such as its source, the type of threat it is linked to, and more.

This additional context can aid incident responders in quickly understanding the nature of a security incident and potential threats. Moreover, it provides a historical reference that can be used for tracking recurring threats and observing patterns in cyberattacks.

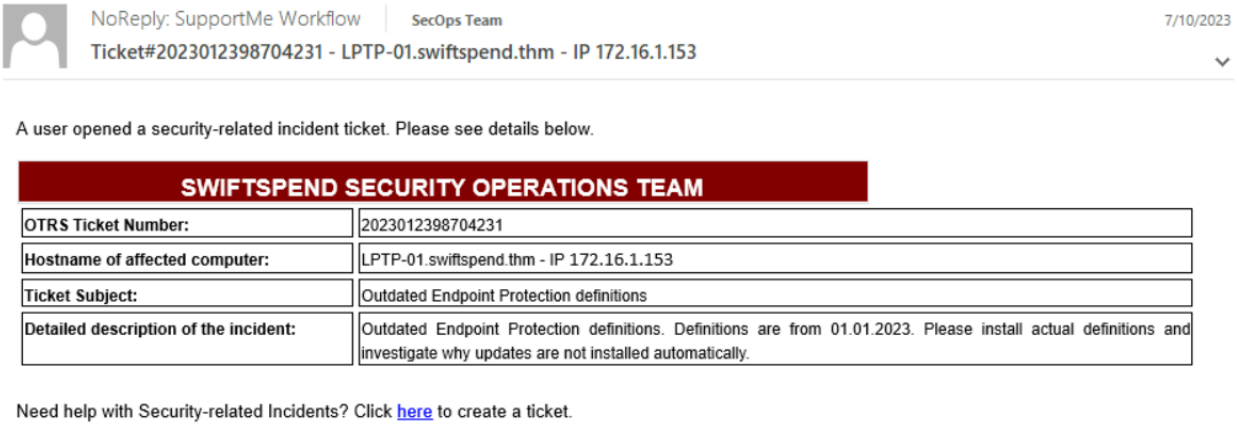
The SoD is more than just a list - it's a dynamic, comprehensive resource that centralises crucial information, streamlines communication among incident response teams, and ultimately empowers faster, more effective responses to potential threats.

The Asset Inventory and Spreadsheet of Doom are indispensable tools in Scoping the extent of a security incident. These tools can be used as quick references and fact sheets, enabling efficient correlation and enrichment of artefacts by providing a comprehensive overview of relevant information about an incident at a glance. By continually updating and referring to both tools, incident response teams can stay one step ahead and take a more proactive approach to incident response.

**********

**Answer the questions below:**

**Based on Ticket#2023012398704231 and Asset Inventory shown in this task, who owns the computer that needs Endpoint Protection definitions updated?**



NoReply: SupportMe Workflow | SecOps Team 7/10/2023

Ticket#2023012398704231 - LPTP-01.swiftspend.thm - IP 172.16.1.153

A user opened a security-related incident ticket. Please see details below.

**SWIFTSPEND SECURITY OPERATIONS TEAM**

| | |
|---|---|
| **OTRS Ticket Number:** | 2023012398704231 |
| **Hostname of affected computer:** | LPTP-01.swiftspend.thm - IP 172.16.1.153 |
| **Ticket Subject:** | Outdated Endpoint Protection definitions |
| **Detailed description of the incident:** | Outdated Endpoint Protection definitions. Definitions are from 01.01.2023. Please install actual definitions and investigate why updates are not installed automatically. |

Need help with Security-related Incidents? Click here to create a ticket.

| | | | | |
|---|---|---|---|---|
| Laptop | LPTP-01 | 172.16.1.153 | Windows 10 Pro | Derick Marshall |

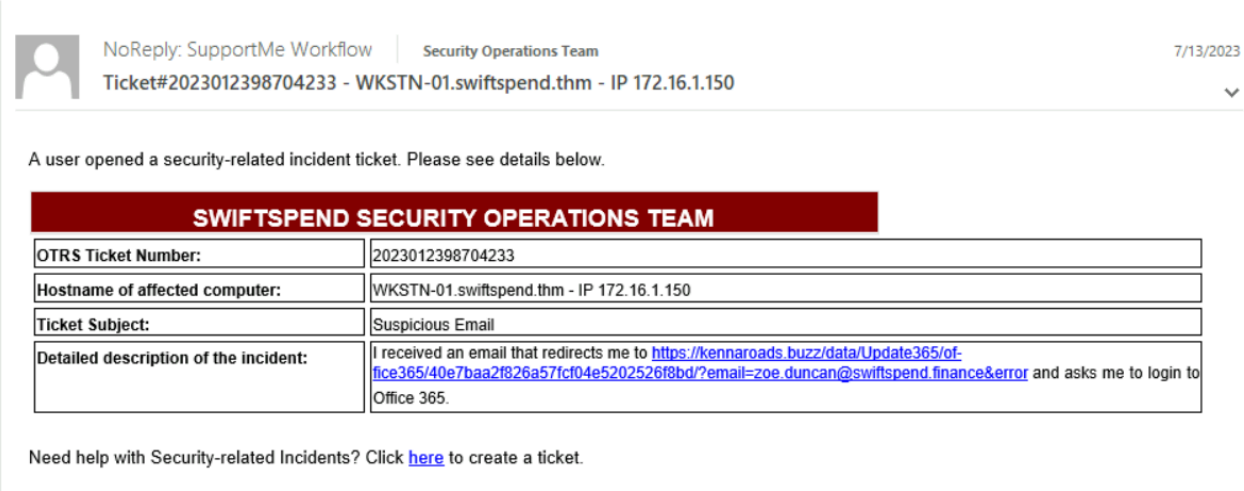
Answer: Derick Marshall

**Based on the email exchanges and SoD shown in this task, what was the phishing domain where the compromised credentials in Ticket#2023012398704232 were submitted?**

| | | | |
|---|---|---|---|
| Domain | b24b-158-62-19-6.ngrok-free.app | Phishing domain | Ticket#2023012398704232 |
| Email address | alex.swift@swiftspend.finance | Spoofed email | Ticket#2023012398704232 |
| Email address | mike.ascot@swiftspend.finance | Spoofed email | Ticket#2023012398704232 |

Answer: b24b-158-62-19-6.ngrok-free.app

**Based on Ticket#2023012398704233, what phishing domain should be added to the SoD?**



NoReply: SupportMe Workflow | Security Operations Team 7/13/2023

Ticket#2023012398704233 - WKSTN-01.swiftspend.thm - IP 172.16.1.150

A user opened a security-related incident ticket. Please see details below.

**SWIFTSPEND SECURITY OPERATIONS TEAM**

| | |
|---|---|
| **OTRS Ticket Number:** | 2023012398704233 |
| **Hostname of affected computer:** | WKSTN-01.swiftspend.thm - IP 172.16.1.150 |
| **Ticket Subject:** | Suspicious Email |
| **Detailed description of the incident:** | I received an email that redirects me to https://kennaroads.buzz/data/Update365/office365/40e7baa2f826a57fcf04e5202526f8bd/?email=zoe.duncan@swiftspend.finance&error and asks me to login to Office 365. |

Need help with Security-related Incidents? Click here to create a ticket.

Answer: kennaroads.buzz

## Identification and Scoping Feedback Loop: An Intelligence-Driven Incident Response Process

The Identification and Scoping phase of the Incident Response Process is not a linear progression but a feedback loop continually refining our understanding of the incident and its scope.

This loop becomes intelligence-driven when it leverages current investigation data, enriching it with information from past incidents, correlated logs from various data sources, advanced analytics and machine learning to enhance awareness by adding more context to a developing situation.

1. Event Notification: The loop begins when an issue has been reported. It triggers the incident response process and sets the stage for the subsequent steps.

2. Documentation: The underlying issue is documented in detail, including information about the nature of the incident, the systems affected, and any potential threats or vulnerabilities. Documentation is a critical step that provides a foundation for the rest of the process.

3. Evidence Collection: Evidence of the incident is collected, including log files, network traffic data, and other relevant information. The collected evidence provides valuable insights into the incident and helps identify potential threats.

4. Artefact Identification: The collected evidence is analysed to identify artefacts related to the incident. These artefacts can provide clues about the threat's nature and the damage's extent.

5. Pivot Point Discovery: Based on the identified artefacts, new areas of investigation may be discovered. These pivot points can lead to new insights and help further refine the incident's scope. After this step, the process loops back to the documentation phase, incorporating the new findings.

**The Power of an Intelligence-Driven Feedback Loop**
A feedback loop driven by intelligence in the Identification and Scoping phase encourages a proactive and dynamic method towards incident response.

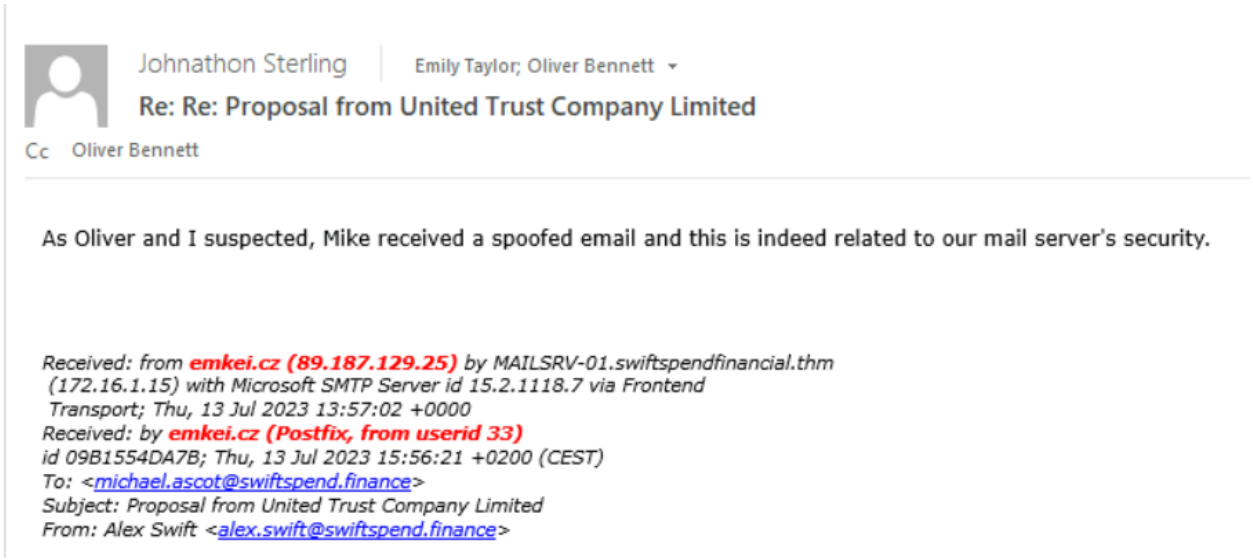
This proactive approach facilitates an ongoing education and exchange of information, enabling organisations to respond to security incidents and safeguard their systems efficiently.

It also ensures compliance with legal obligations for privacy and data protection.

Organisations can boost their incident response prowess and efficiently counteract security incidents by capitalising on real-time data concerning emerging threats, cultivating an environment of ongoing education and exchange of information, and guaranteeing privacy and data protection.

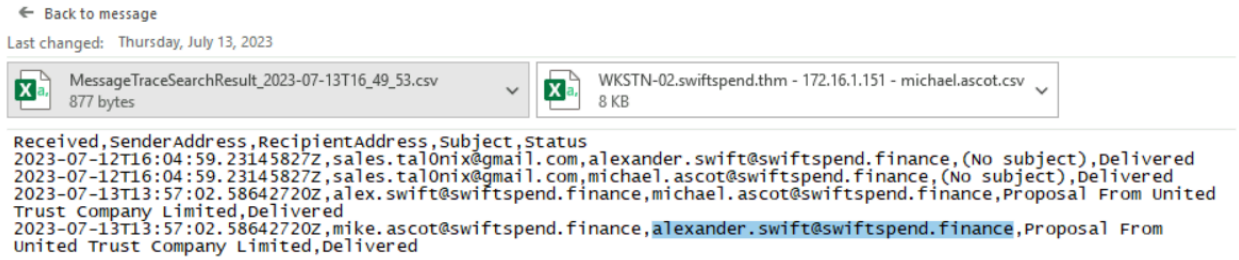
**********
**Answer the questions below:**

**Concerning Ticket#2023012398704232 and according to your colleague John, what domain should be added to the SoD since it was used for email spoofing?**



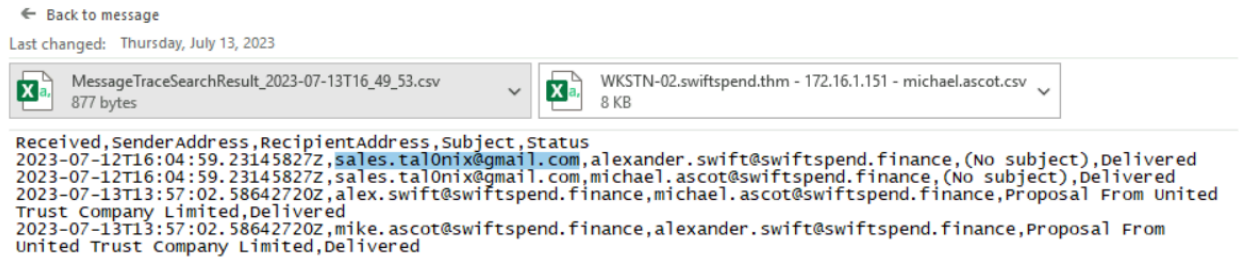

Answer: emkei.cz

**Concerning the available artefacts gathered for analysis of Ticket#2023012398704232, who is the other user that received a similar phishing email but did not open a ticket nor report the issue?**



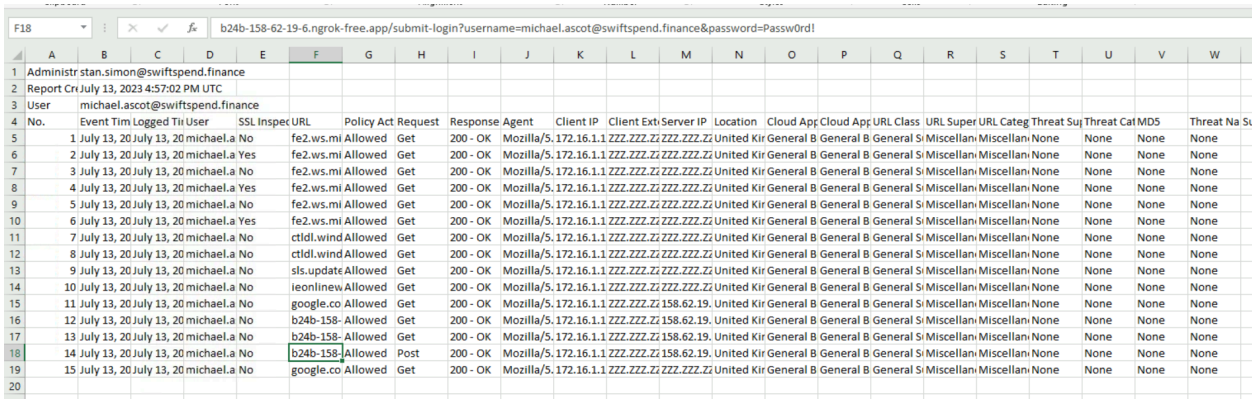

Answer: alexander.swift@swiftspend.finance

**Concerning Ticket#2023012398704232, what additional IoC could be added to the SoD and be used as a pivot point for discovery?**




Answer: sales.tal0nix@gmail.com

**Based on the email exchanges and attachments in those exchanges, what is the password of the compromised user?**



F18 | b24b-158-62-19-6.ngrok-free.app/submit-login?username=michael.ascot@swiftspend.finance&password=Passw0rd!

| | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | Administr | stan.simon@swiftspend.finance | | | | | | | | | | | | | | | | | | | | | |
| 2 | Report Cr | July 13, 2023 4:57:02 PM UTC | | | | | | | | | | | | | | | | | | | | | |
| 3 | User | michael.ascot@swiftspend.finance | | | | | | | | | | | | | | | | | | | | | |
| 4 | No. | Event Tim | Logged Ti | User | SSL Inspec | URL | Policy Act | Request | Response | Agent | Client IP | Client Ext | Server IP | Location | Cloud App | Cloud App | URL Class | URL Super | URL Categ | Threat Su | Threat Cat | MD5 | Threat Na |
| 5 | 1 | July 13, 20 | July 13, 20 | michael.a | No | fe2.ws.mi | Allowed | Get | 200 - OK | Mozilla/5. | 172.16.1.1 | ZZZ.ZZZ.Z | ZZZ.ZZZ.Z | United Kir | General B | General B | General Si | Miscellan | Miscellan | None | None | None | None |
| 6 | 2 | July 13, 20 | July 13, 20 | michael.a | Yes | fe2.ws.mi | Allowed | Get | 200 - OK | Mozilla/5. | 172.16.1.1 | ZZZ.ZZZ.Z | ZZZ.ZZZ.Z | United Kir | General B | General B | General Si | Miscellan | Miscellan | None | None | None | None |
| 7 | 3 | July 13, 20 | July 13, 20 | michael.a | No | fe2.ws.mi | Allowed | Get | 200 - OK | Mozilla/5. | 172.16.1.1 | ZZZ.ZZZ.Z | ZZZ.ZZZ.Z | United Kir | General B | General B | General Si | Miscellan | Miscellan | None | None | None | None |
| 8 | 4 | July 13, 20 | July 13, 20 | michael.a | Yes | fe2.ws.mi | Allowed | Get | 200 - OK | Mozilla/5. | 172.16.1.1 | ZZZ.ZZZ.Z | ZZZ.ZZZ.Z | United Kir | General B | General B | General Si | Miscellan | Miscellan | None | None | None | None |
| 9 | 5 | July 13, 20 | July 13, 20 | michael.a | No | fe2.ws.mi | Allowed | Get | 200 - OK | Mozilla/5. | 172.16.1.1 | ZZZ.ZZZ.Z | ZZZ.ZZZ.Z | United Kir | General B | General B | General Si | Miscellan | Miscellan | None | None | None | None |
| 10 | 6 | July 13, 20 | July 13, 20 | michael.a | Yes | fe2.ws.mi | Allowed | Get | 200 - OK | Mozilla/5. | 172.16.1.1 | ZZZ.ZZZ.Z | ZZZ.ZZZ.Z | United Kir | General B | General B | General Si | Miscellan | Miscellan | None | None | None | None |
| 11 | 7 | July 13, 20 | July 13, 20 | michael.a | No | ctldl.wind | Allowed | Get | 200 - OK | Mozilla/5. | 172.16.1.1 | ZZZ.ZZZ.Z | ZZZ.ZZZ.Z | United Kir | General B | General B | General Si | Miscellan | Miscellan | None | None | None | None |
| 12 | 8 | July 13, 20 | July 13, 20 | michael.a | No | ctldl.wind | Allowed | Get | 200 - OK | Mozilla/5. | 172.16.1.1 | ZZZ.ZZZ.Z | ZZZ.ZZZ.Z | United Kir | General B | General B | General Si | Miscellan | Miscellan | None | None | None | None |
| 13 | 9 | July 13, 20 | July 13, 20 | michael.a | No | sls.update | Allowed | Get | 200 - OK | Mozilla/5. | 172.16.1.1 | ZZZ.ZZZ.Z | ZZZ.ZZZ.Z | United Kir | General B | General B | General Si | Miscellan | Miscellan | None | None | None | None |
| 14 | 10 | July 13, 20 | July 13, 20 | michael.a | No | ieonlinew | Allowed | Get | 200 - OK | Mozilla/5. | 172.16.1.1 | ZZZ.ZZZ.Z | ZZZ.ZZZ.Z | United Kir | General B | General B | General Si | Miscellan | Miscellan | None | None | None | None |
| 15 | 11 | July 13, 20 | July 13, 20 | michael.a | No | google.co | Allowed | Get | 200 - OK | Mozilla/5. | 172.16.1.1 | ZZZ.ZZZ.Z | 158.62.19. | United Kir | General B | General B | General Si | Miscellan | Miscellan | None | None | None | None |
| 16 | 12 | July 13, 20 | July 13, 20 | michael.a | No | b24b-158- | Allowed | Get | 200 - OK | Mozilla/5. | 172.16.1.1 | ZZZ.ZZZ.Z | 158.62.19. | United Kir | General B | General B | General Si | Miscellan | Miscellan | None | None | None | None |
| 17 | 13 | July 13, 20 | July 13, 20 | michael.a | No | b24b-158- | Allowed | Get | 200 - OK | Mozilla/5. | 172.16.1.1 | ZZZ.ZZZ.Z | 158.62.19. | United Kir | General B | General B | General Si | Miscellan | Miscellan | None | None | None | None |
| 18 | 14 | July 13, 20 | July 13, 20 | michael.a | No | b24b-158- | Allowed | Post | 200 - OK | Mozilla/5. | 172.16.1.1 | ZZZ.ZZZ.Z | 158.62.19. | United Kir | General B | General B | General Si | Miscellan | Miscellan | None | None | None | None |
| 19 | 15 | July 13, 20 | July 13, 20 | michael.a | No | google.co | Allowed | Get | 200 - OK | Mozilla/5. | 172.16.1.1 | ZZZ.ZZZ.Z | ZZZ.ZZZ.Z | United Kir | General B | General B | General Si | Miscellan | Miscellan | None | None | None | None |
| 20 | | | | | | | | | | | | | | | | | | | | | | | |

Opening the excel spreadsheet related to WKSTN-02 we see a lot of Get requests but one Post request. Clicking on the cell for the URL of the Post request we can see a username and password saved by the ngrok server.

b24b-158-62-19-6.ngrok-free.app/submit-login?username=michael.ascot@swiftspend.finance&password=Passw0rd!



| Domain | b24b-158-62-19-6.ngrok-free.app | Phishing domain | Ticket#2023012398704232 |
|---|---|---|---|

That specific ngrok server is also logged as a phishing domain in our Spreadsheet of Doom.
Answer: Passw0rd!

## Conclusion

The Identification and Scoping phase of the Incident Response Process is a critical juncture that requires a well-coordinated effort between people, processes, and technology. Here, the nature of security alerts is discerned, and the extent of the incident is determined.

This phase is a balancing act, requiring technical expertise, effective use of security tools, and a culture of continuous learning and vigilance.

We've explored the importance of understanding security alerts, the role of technical expertise and security tools, and cultivating a culture of learning and vigilance. We've also delved into the significance of following proper procedures to ensure that incidents are accurately identified and managed, ensuring that the appropriate individuals capable of addressing them are notified.

Remember, the success of the identification phase hinges on a well-orchestrated collaboration between these elements. You can significantly enhance your

organisation's incident response capabilities by fostering a culture of awareness and vigilance and leveraging the right tools and processes.

**Next Steps**

Now that you've comprehensively understood the Identification and Scoping phase, it's time to proceed to the next room, Intel Creation and Containment.

Here, you'll delve deeper into the Incident Response Process, exploring the subsequent phases and honing your skills further. Remember, continuous learning and practice are essential to mastering incident response. Onwards!