Falconi® Sports Agency

Incident Response Overview

Essential Protocols, Strategies, and Cyber Readiness

Presented by: Incident Response Team
In collaboration with: Cyber Essentials and Risk Management Teams

Table of Contents

❑ Team and Strategy

❑ Incident Analysis and Response

FALCONI
SPORTS AGENCY

Team and Strategy

Strengthening Team Readiness and Developing Awareness Initiatives

Incident Response Team

IT/Cybersecurity

- Chief Information Security Officer (CISO)
- Incident Response Manager
- Lead Security Analyst
- SOC Analyst (Tier 1, 2)
- Digital Forensics Investigator
- System Administrator
- Network Administrator

Legal

- Compliance Officer
- Privacy Officer

Human Resources

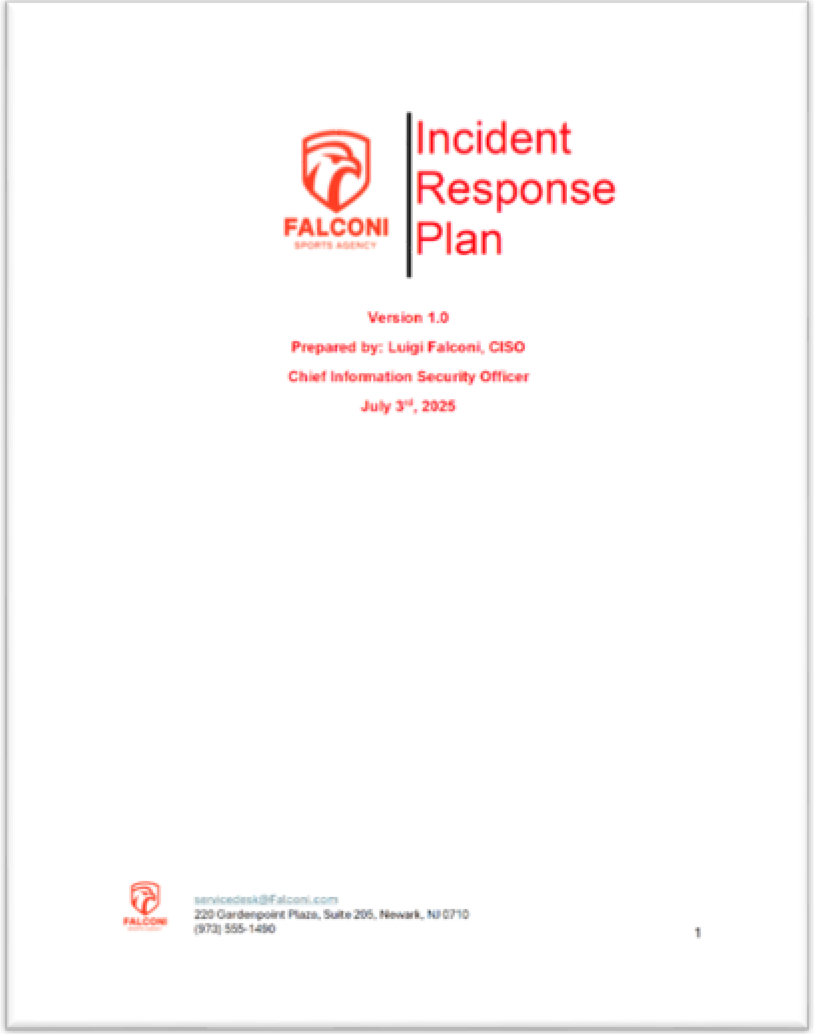
- HR Director

Communications

- Head of External Communications
- Head of Internal Communications
- Social Media Manager

Incident Response Plan

- Modeled after CISA Playbook and NIST 800-171



FALCONI
SPORTS AGENCY

Incident
Response
Plan

Version 1.0

Prepared by: Luigi Falconi, CISO

Chief Information Security Officer

July 3rd, 2025

❖ Purpose

- "The Security Incident Response Plan provides a systematic incident response process for all Information Security Incident(s) that affect any of Falconi's information technology systems, network, or data, including Falconi data held, or services provided by third-party vendors or other service providers."

Incident Response Plan

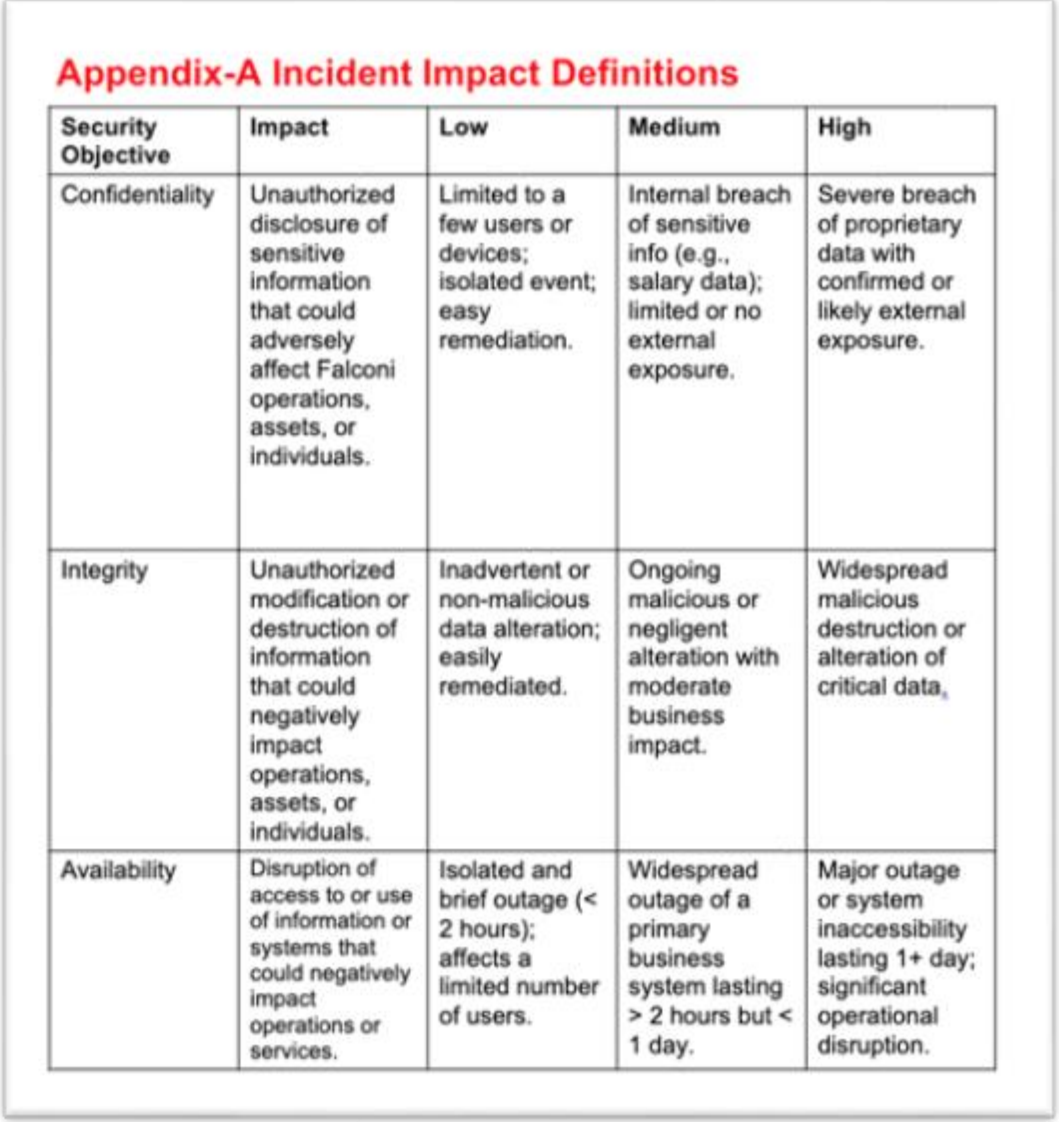
❖ Detection & Reporting

- **Automated Detection**
  - Alerts from Falconi's IDS or SIEM tools
- **Employee Report**
  - Incidents reported to Service Desk
- **External Source**
  - Outside parties notify Falconi

❖ Response Procedures

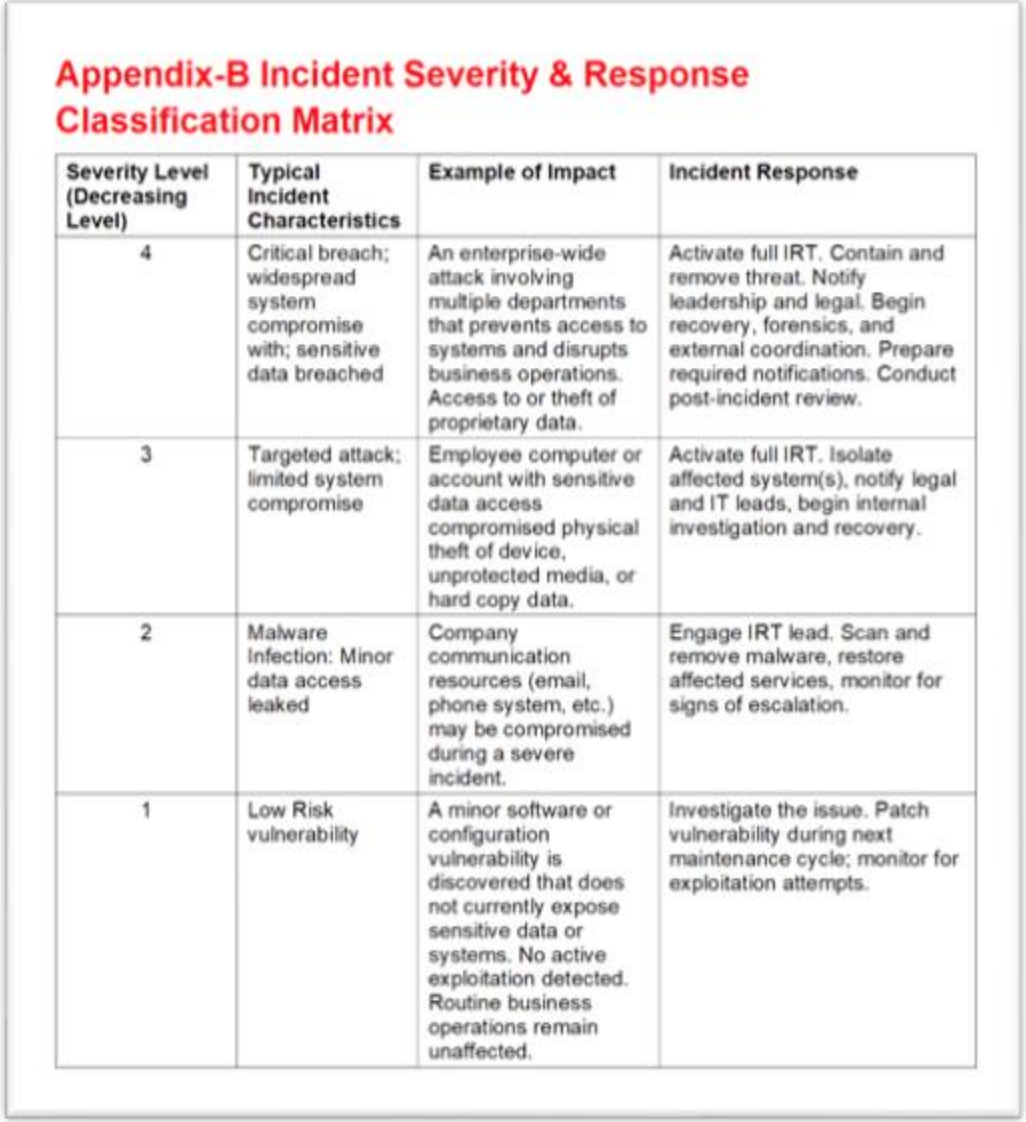
- **Verification**
  - Confirm incident and escalate
- **Assessment**
  - Evaluate scope and impact
- **Containment & Mitigation**
  - Isolate threat and preserve evidence
- **Post-Breach Response**
  - Communicate and comply with laws
- **Post-Mortem**
  - Review, learn, and improve

Incident Response Plan



Appendix-A Incident Impact Definitions

Security Objective	Impact	Low	Medium	High
Confidentiality	Unauthorized disclosure of sensitive information that could adversely affect Falconi operations, assets, or individuals.	Limited to a few users or devices; isolated event; easy remediation.	Internal breach of sensitive info (e.g., salary data); limited or no external exposure.	Severe breach of proprietary data with confirmed or likely external exposure.
Integrity	Unauthorized modification or destruction of information that could negatively impact operations, assets, or individuals.	Inadvertent or non-malicious data alteration; easily remediated.	Ongoing malicious or negligent alteration with moderate business impact.	Widespread malicious destruction or alteration of critical data.
Availability	Disruption of access to or use of information or systems that could negatively impact operations or services.	Isolated and brief outage (< 2 hours); affects a limited number of users.	Widespread outage of a primary business system lasting > 2 hours but < 1 day.	Major outage or system inaccessibility lasting 1+ day; significant operational disruption.



Appendix-B Incident Severity & Response Classification Matrix

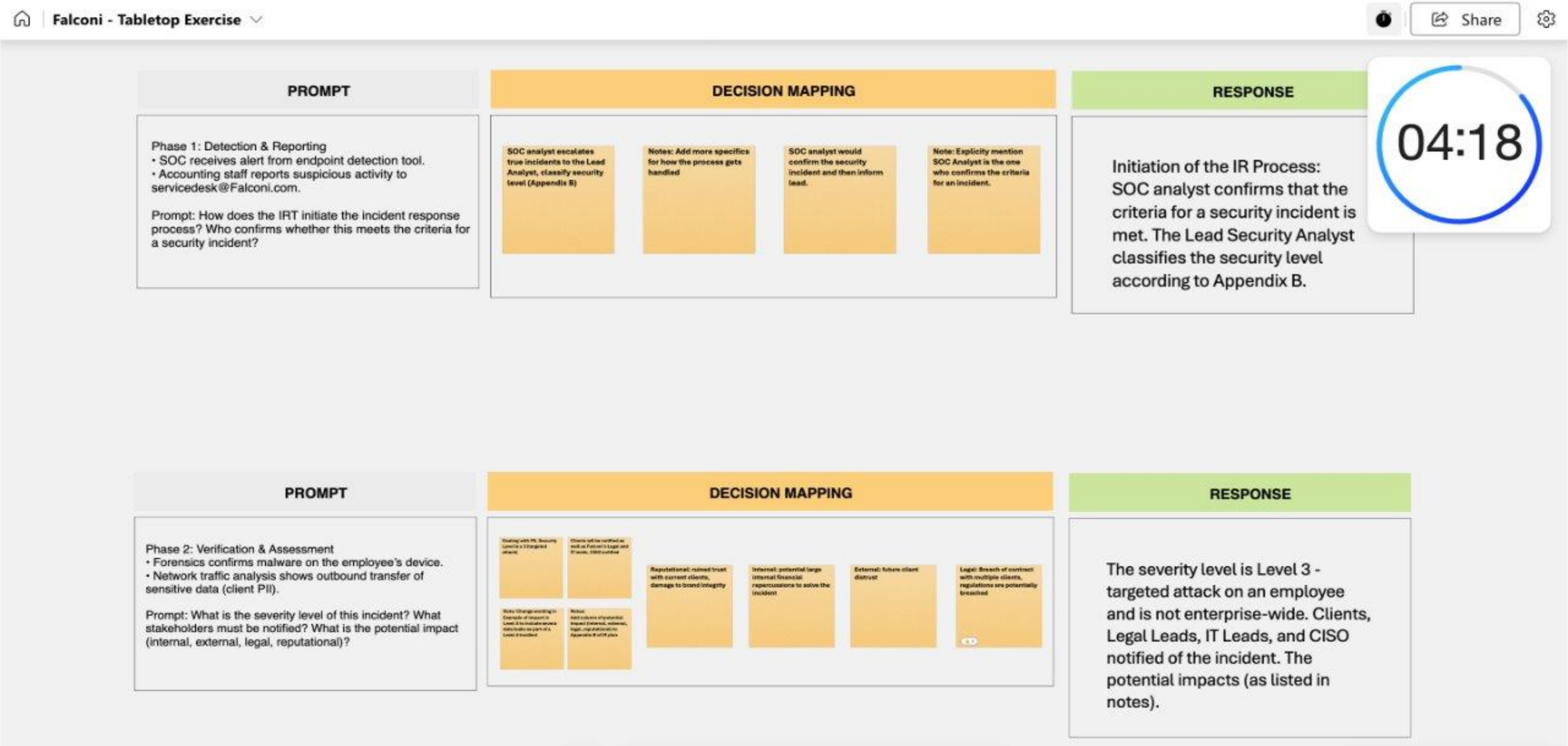
Severity Level (Decreasing Level)	Typical Incident Characteristics	Example of Impact	Incident Response
4	Critical breach; widespread system compromise with; sensitive data breached	An enterprise-wide attack involving multiple departments that prevents access to systems and disrupts business operations. Access to or theft of proprietary data.	Activate full IRT. Contain and remove threat. Notify leadership and legal. Begin recovery, forensics, and external coordination. Prepare required notifications. Conduct post-incident review.
3	Targeted attack; limited system compromise	Employee computer or account with sensitive data access compromised physical theft of device, unprotected media, or hard copy data.	Activate full IRT. Isolate affected system(s), notify legal and IT leads, begin internal investigation and recovery.
2	Malware Infection: Minor data access leaked	Company communication resources (email, phone system, etc.) may be compromised during a severe incident.	Engage IRT lead. Scan and remove malware, restore affected services, monitor for signs of escalation.
1	Low Risk vulnerability	A minor software or configuration vulnerability is discovered that does not currently expose sensitive data or systems. No active exploitation detected. Routine business operations remain unaffected.	Investigate the issue. Patch vulnerability during next maintenance cycle; monitor for exploitation attempts.

FALCONI
SPORTS AGENCY

Tabletop Exercise

- Based on a phishing attack – Employee clicks on a malicious link in a phishing email
- Roles were assigned to interns:
  - Julia - IR Manager / Tabletop Leader / Participant
  - John, Aaron – Notetakers / Whiteboard Managers / Participants
  - Cyber Essentials + Risk Management Teams – Participants
- We worked through 5 phases of Incident Response
  - 8 minutes per phase
- **Goal**: Test for gaps in Incident Response Plan; make revisions based on gaps

Tabletop Exercise



PROMPT

Phase 1: Detection & Reporting
- SOC receives alert from endpoint detection tool.
- Accounting staff reports suspicious activity to servicedesk@Falconi.com.

Prompt: How does the IRT initiate the incident response process? Who confirms whether this meets the criteria for a security incident?

DECISION MAPPING

SOC analyst escalates true incidents to the Lead Analyst, classify security level (Appendix B)

Notes: Add more specifics for how the process gets handled

SOC analyst would confirm the security incident and then inform lead.

Note: Explicity mention SOC Analyst is the one who confirms the criteria for an incident.

RESPONSE

Initiation of the IR Process: SOC analyst confirms that the criteria for a security incident is met. The Lead Security Analyst classifies the security level according to Appendix B.

PROMPT

Phase 2: Verification & Assessment
- Forensics confirms malware on the employee's device.
- Network traffic analysis shows outbound transfer of sensitive data (client PII).

Prompt: What is the severity level of this incident? What stakeholders must be notified? What is the potential impact (internal, external, legal, reputational)?

DECISION MAPPING

Dealing with PII. Security Level is a 3 (targeted attack)

Clients will be notified as well as Falconi's Legal and IT leads. CISO notified

Note: Change wording in Example of impact in Level 3 to [illegible] as part of a Level 3 incident

Notes:
Add column of potential impact (internal, external, legal, reputational) to Appendix B of IR plan

Reputational: ruined trust with current clients, damage to brand integrity

Internal: potential large internal financial repercussions to solve the incident

External: future client distrust

Legal: Breach of contract with multiple clients, regulations are potentially breached

RESPONSE

The severity level is Level 3 - targeted attack on an employee and is not enterprise-wide. Clients, Legal Leads, IT Leads, and CISO notified of the incident. The potential impacts (as listed in notes).

IR Plan - Areas of Improvement

❖ Phase 1 – Detection & Reporting

- Clearly define roles of Lead Security Analyst and SOC analyst

❖ Phase 2 – Verification & Assessment

- Criteria was not specific within our severity levels
- Add a note for 'potential impact' to Appendix-B of IR plan

❖ Phase 3 – Containment & Mitigation

- 'Containment' section of our IR Plan should be expanded to include clearer criteria for system isolation and log preservation protocols

❖ Phase 4 – Communication

- No areas of improvement

❖ Phase 5 – Post-Breach & Response

- The 'Post Breach Response' should be more specific in our IR Plan

FALCONI

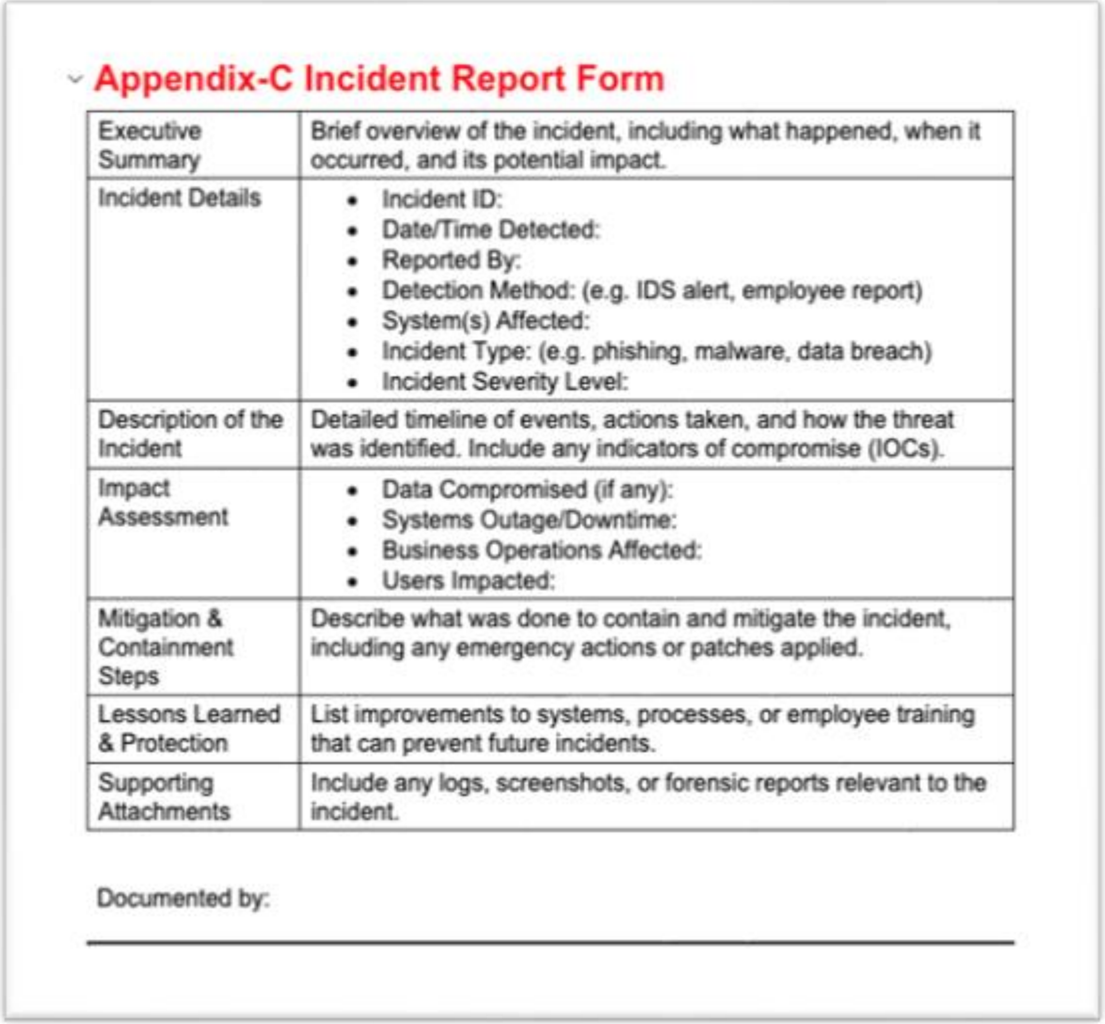
SPORTS AGENCY

Incident Analysis and Response

Analyzing Security Events and Reporting Findings

Incident Report Form

- Executive Summary
- Incident Details
- Description of the Incident
- Indicators of Compromise (IOCs)
- Impact Assessment
- Mitigation and Containment Steps
- Lessons Learned and Protection



Appendix-C Incident Report Form

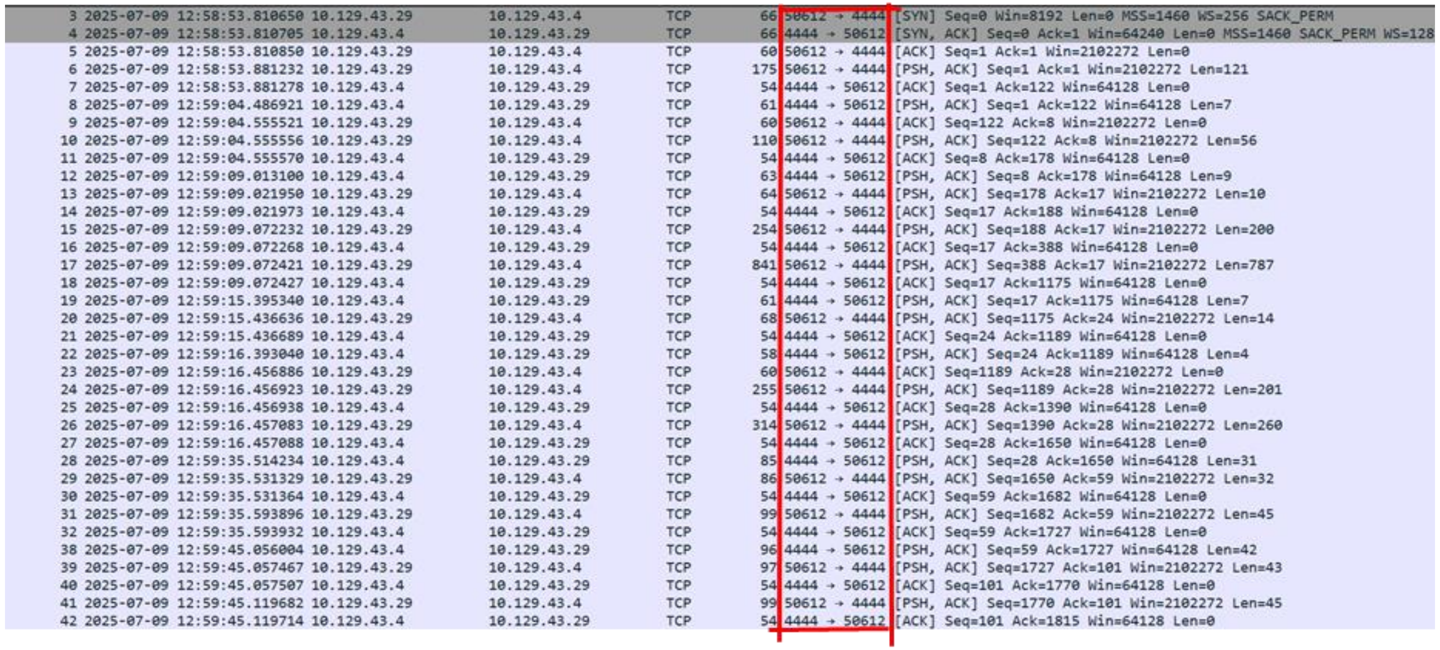
Executive Summary	Brief overview of the incident, including what happened, when it occurred, and its potential impact.
Incident Details	• Incident ID: • Date/Time Detected: • Reported By: • Detection Method: (e.g. IDS alert, employee report) • System(s) Affected: • Incident Type: (e.g. phishing, malware, data breach) • Incident Severity Level:
Description of the Incident	Detailed timeline of events, actions taken, and how the threat was identified. Include any indicators of compromise (IOCs).
Impact Assessment	• Data Compromised (if any): • Systems Outage/Downtime: • Business Operations Affected: • Users Impacted:
Mitigation & Containment Steps	Describe what was done to contain and mitigate the incident, including any emergency actions or patches applied.
Lessons Learned & Protection	List improvements to systems, processes, or employee training that can prevent future incidents.
Supporting Attachments	Include any logs, screenshots, or forensic reports relevant to the incident.

Documented by:

Incident Report #1

FALCONI
SPORTS AGENCY

Unusual TCP Connection



```
 3 2025-07-09 12:58:53.810650 10.129.43.29    10.129.43.4     TCP    66 50612 → 4444 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
 4 2025-07-09 12:58:53.810705 10.129.43.4     10.129.43.29    TCP    66 4444 → 50612 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
 5 2025-07-09 12:58:53.810850 10.129.43.29    10.129.43.4     TCP    60 50612 → 4444 [ACK] Seq=1 Ack=1 Win=2102272 Len=0
 6 2025-07-09 12:58:53.881232 10.129.43.29    10.129.43.4     TCP   175 50612 → 4444 [PSH, ACK] Seq=1 Ack=1 Win=2102272 Len=121
 7 2025-07-09 12:58:53.881278 10.129.43.4     10.129.43.29    TCP    54 4444 → 50612 [ACK] Seq=1 Ack=122 Win=64128 Len=0
 8 2025-07-09 12:59:04.486921 10.129.43.4     10.129.43.29    TCP    61 4444 → 50612 [PSH, ACK] Seq=1 Ack=122 Win=64128 Len=7
 9 2025-07-09 12:59:04.555521 10.129.43.29    10.129.43.4     TCP    60 50612 → 4444 [ACK] Seq=122 Ack=8 Win=2102272 Len=0
10 2025-07-09 12:59:04.555556 10.129.43.29    10.129.43.4     TCP   110 50612 → 4444 [PSH, ACK] Seq=122 Ack=8 Win=2102272 Len=56
11 2025-07-09 12:59:04.555570 10.129.43.4     10.129.43.29    TCP    54 4444 → 50612 [ACK] Seq=8 Ack=178 Win=64128 Len=0
12 2025-07-09 12:59:09.013100 10.129.43.4     10.129.43.29    TCP    63 4444 → 50612 [PSH, ACK] Seq=8 Ack=178 Win=64128 Len=9
13 2025-07-09 12:59:09.021950 10.129.43.29    10.129.43.4     TCP    64 50612 → 4444 [PSH, ACK] Seq=178 Ack=17 Win=2102272 Len=10
14 2025-07-09 12:59:09.021973 10.129.43.4     10.129.43.29    TCP    54 4444 → 50612 [ACK] Seq=17 Ack=188 Win=64128 Len=0
15 2025-07-09 12:59:09.072232 10.129.43.29    10.129.43.4     TCP   254 50612 → 4444 [PSH, ACK] Seq=188 Ack=17 Win=2102272 Len=200
16 2025-07-09 12:59:09.072268 10.129.43.4     10.129.43.29    TCP    54 4444 → 50612 [ACK] Seq=17 Ack=388 Win=64128 Len=0
17 2025-07-09 12:59:09.072421 10.129.43.29    10.129.43.4     TCP   841 50612 → 4444 [PSH, ACK] Seq=388 Ack=17 Win=2102272 Len=787
18 2025-07-09 12:59:09.072427 10.129.43.4     10.129.43.29    TCP    54 4444 → 50612 [ACK] Seq=17 Ack=1175 Win=64128 Len=0
19 2025-07-09 12:59:15.395340 10.129.43.4     10.129.43.29    TCP    61 4444 → 50612 [PSH, ACK] Seq=17 Ack=1175 Win=64128 Len=7
20 2025-07-09 12:59:15.436636 10.129.43.29    10.129.43.4     TCP    68 50612 → 4444 [PSH, ACK] Seq=1175 Ack=24 Win=2102272 Len=14
21 2025-07-09 12:59:15.436689 10.129.43.4     10.129.43.29    TCP    54 4444 → 50612 [ACK] Seq=24 Ack=1189 Win=64128 Len=0
22 2025-07-09 12:59:16.393040 10.129.43.4     10.129.43.29    TCP    58 4444 → 50612 [PSH, ACK] Seq=24 Ack=1189 Win=64128 Len=4
23 2025-07-09 12:59:16.456886 10.129.43.29    10.129.43.4     TCP    60 50612 → 4444 [ACK] Seq=1189 Ack=28 Win=2102272 Len=0
24 2025-07-09 12:59:16.456923 10.129.43.29    10.129.43.4     TCP   255 50612 → 4444 [PSH, ACK] Seq=1189 Ack=28 Win=2102272 Len=201
25 2025-07-09 12:59:16.456938 10.129.43.4     10.129.43.29    TCP    54 4444 → 50612 [ACK] Seq=28 Ack=1390 Win=64128 Len=0
26 2025-07-09 12:59:16.457083 10.129.43.29    10.129.43.4     TCP   314 50612 → 4444 [PSH, ACK] Seq=1390 Ack=28 Win=2102272 Len=260
27 2025-07-09 12:59:16.457088 10.129.43.4     10.129.43.29    TCP    54 4444 → 50612 [ACK] Seq=28 Ack=1650 Win=64128 Len=0
28 2025-07-09 12:59:35.514234 10.129.43.4     10.129.43.29    TCP    85 4444 → 50612 [PSH, ACK] Seq=28 Ack=1650 Win=64128 Len=31
29 2025-07-09 12:59:35.531329 10.129.43.29    10.129.43.4     TCP    86 50612 → 4444 [PSH, ACK] Seq=1650 Ack=59 Win=2102272 Len=32
30 2025-07-09 12:59:35.531364 10.129.43.4     10.129.43.29    TCP    54 4444 → 50612 [ACK] Seq=59 Ack=1682 Win=64128 Len=0
31 2025-07-09 12:59:35.593896 10.129.43.29    10.129.43.4     TCP    99 50612 → 4444 [PSH, ACK] Seq=1682 Ack=59 Win=2102272 Len=45
32 2025-07-09 12:59:35.593932 10.129.43.4     10.129.43.29    TCP    54 4444 → 50612 [ACK] Seq=59 Ack=1727 Win=64128 Len=0
38 2025-07-09 12:59:45.056004 10.129.43.4     10.129.43.29    TCP    96 4444 → 50612 [PSH, ACK] Seq=59 Ack=1727 Win=64128 Len=42
39 2025-07-09 12:59:45.057467 10.129.43.29    10.129.43.4     TCP    97 50612 → 4444 [PSH, ACK] Seq=1727 Ack=101 Win=2102272 Len=43
40 2025-07-09 12:59:45.057507 10.129.43.4     10.129.43.29    TCP    54 4444 → 50612 [ACK] Seq=101 Ack=1770 Win=64128 Len=0
41 2025-07-09 12:59:45.119682 10.129.43.29    10.129.43.4     TCP    99 50612 → 4444 [PSH, ACK] Seq=1770 Ack=101 Win=2102272 Len=45
42 2025-07-09 12:59:45.119714 10.129.43.4     10.129.43.29    TCP    54 4444 → 50612 [ACK] Seq=101 Ack=1815 Win=64128 Len=0
```

Figure 1: TCP-filtered stream of packets with port 4444

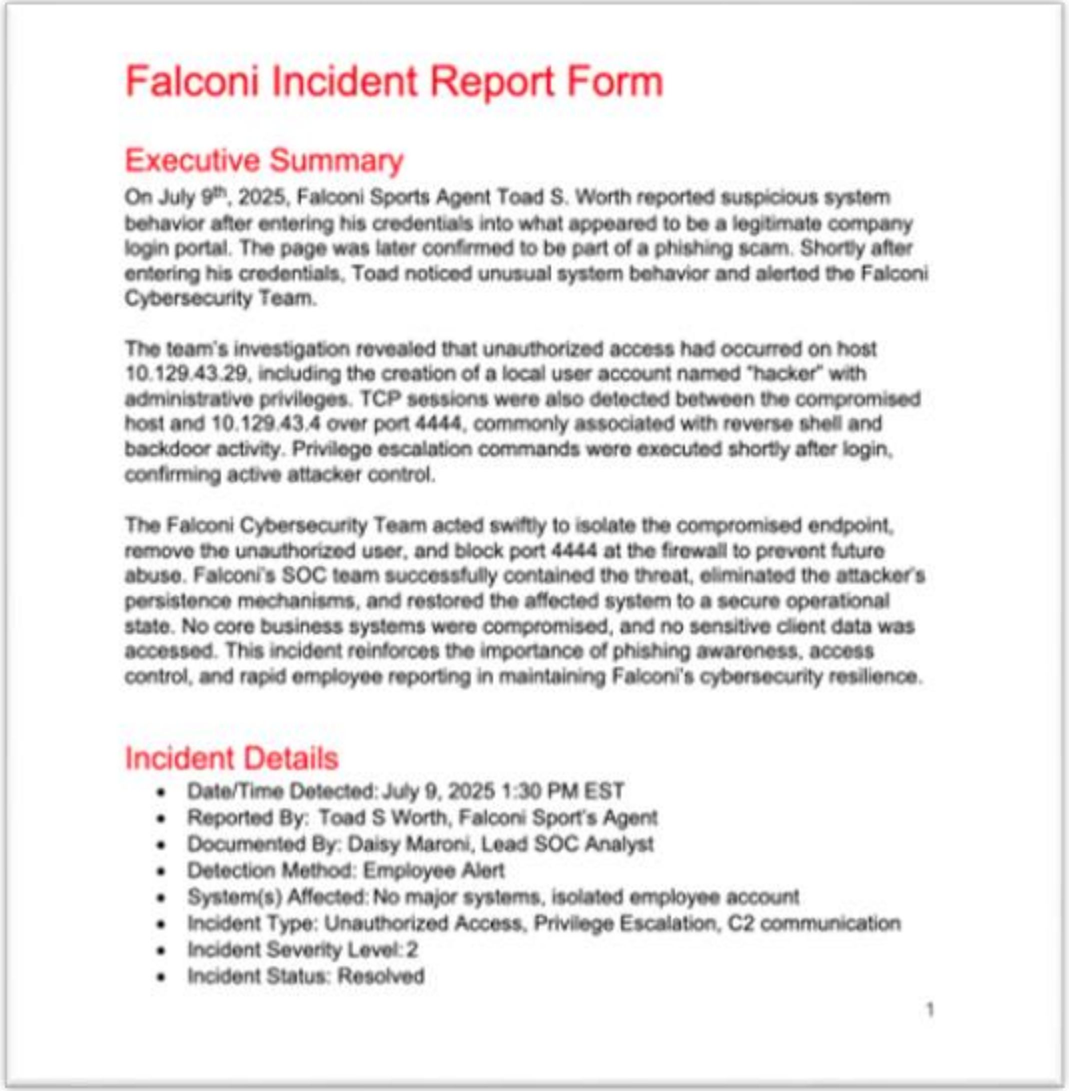
- Using a packet capture from one of our projects, we were able to recognize an unusual TCP connection on a port not frequently used.

- This was caused by a phishing scam in which credentials were entered in a fraudulent company portal.

- A local user account "hacker" was created with administrative privileges.

Incident Response Report

FALCONI
SPORTS AGENCY



Falconi Incident Report Form

Executive Summary

On July 9th, 2025, Falconi Sports Agent Toad S. Worth reported suspicious system behavior after entering his credentials into what appeared to be a legitimate company login portal. The page was later confirmed to be part of a phishing scam. Shortly after entering his credentials, Toad noticed unusual system behavior and alerted the Falconi Cybersecurity Team.

The team's investigation revealed that unauthorized access had occurred on host 10.129.43.29, including the creation of a local user account named "hacker" with administrative privileges. TCP sessions were also detected between the compromised host and 10.129.43.4 over port 4444, commonly associated with reverse shell and backdoor activity. Privilege escalation commands were executed shortly after login, confirming active attacker control.

The Falconi Cybersecurity Team acted swiftly to isolate the compromised endpoint, remove the unauthorized user, and block port 4444 at the firewall to prevent future abuse. Falconi's SOC team successfully contained the threat, eliminated the attacker's persistence mechanisms, and restored the affected system to a secure operational state. No core business systems were compromised, and no sensitive client data was accessed. This incident reinforces the importance of phishing awareness, access control, and rapid employee reporting in maintaining Falconi's cybersecurity resilience.

Incident Details

- Date/Time Detected: July 9, 2025 1:30 PM EST
- Reported By: Toad S Worth, Falconi Sport's Agent
- Documented By: Daisy Maroni, Lead SOC Analyst
- Detection Method: Employee Alert
- System(s) Affected: No major systems, isolated employee account
- Incident Type: Unauthorized Access, Privilege Escalation, C2 communication
- Incident Severity Level: 2
- Incident Status: Resolved

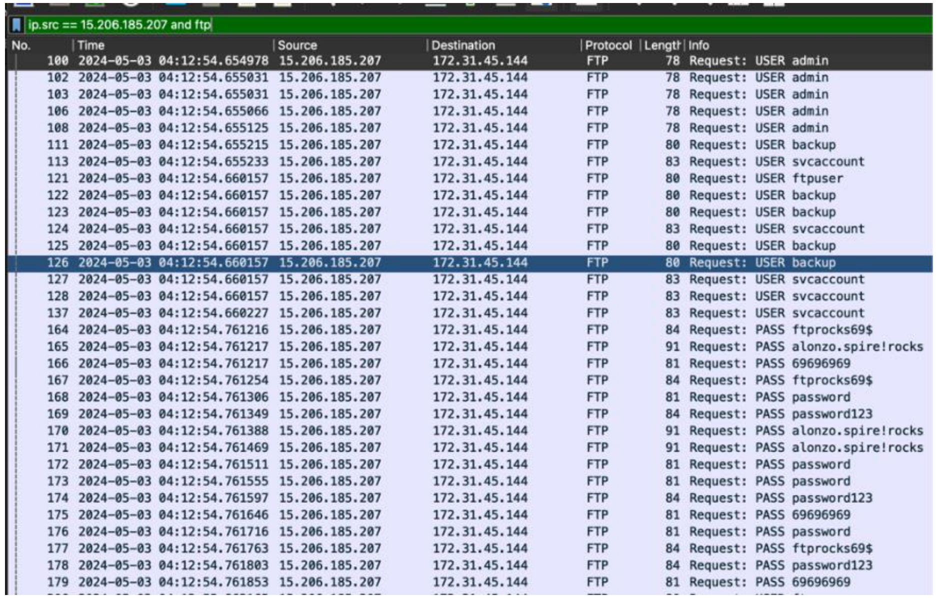
1

- **Indicators of Compromise**
  - Unusual TCP traffic between 10.129.43.29 and 10.129.43.4 over port 4444, a known vector for malware and remote shell activity.
- **Impact Assessment**
  - Possible user data exposed; activity suggests targeted enumeration, though no exfiltration was confirmed.
  - No outages occurred
- **Mitigation and Containment Steps**
  - Computer isolated from system
  - Malicious 'user' removed from system
- **Lessons Learned**
  - Monitor Admin Changes
  - Review Access Control Policies
  - Disable creation of local accounts on standard employee machines

Incident Report #2

FALCONI
SPORTS AGENCY

Sherlock – Brute Force Incident

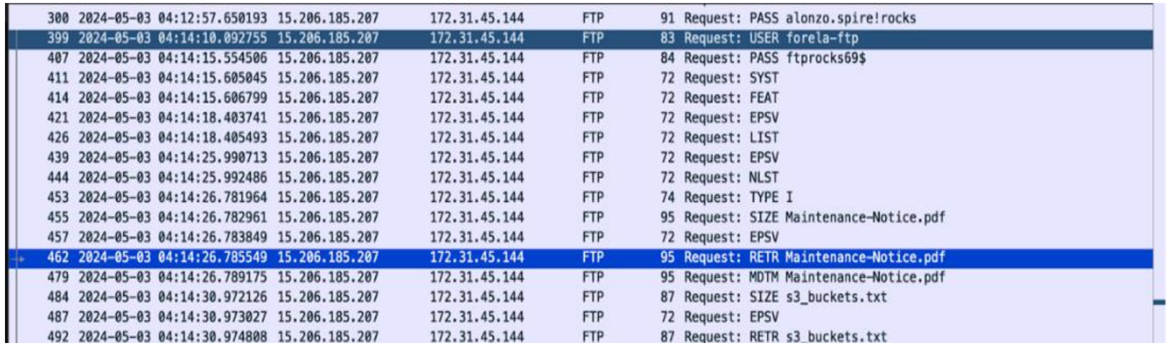


```
ip.src == 15.206.185.207 and ftp
No.   Time                        Source           Destination     Protocol Length Info
  100 2024-05-03 04:12:54.654978  15.206.185.207   172.31.45.144   FTP      78 Request: USER admin
  102 2024-05-03 04:12:54.655031  15.206.185.207   172.31.45.144   FTP      78 Request: USER admin
  103 2024-05-03 04:12:54.655031  15.206.185.207   172.31.45.144   FTP      78 Request: USER admin
  106 2024-05-03 04:12:54.655066  15.206.185.207   172.31.45.144   FTP      78 Request: USER admin
  108 2024-05-03 04:12:54.655125  15.206.185.207   172.31.45.144   FTP      78 Request: USER admin
  111 2024-05-03 04:12:54.655215  15.206.185.207   172.31.45.144   FTP      80 Request: USER backup
  113 2024-05-03 04:12:54.655233  15.206.185.207   172.31.45.144   FTP      83 Request: USER svcaccount
  121 2024-05-03 04:12:54.660157  15.206.185.207   172.31.45.144   FTP      80 Request: USER ftpuser
  122 2024-05-03 04:12:54.660157  15.206.185.207   172.31.45.144   FTP      80 Request: USER backup
  123 2024-05-03 04:12:54.660157  15.206.185.207   172.31.45.144   FTP      80 Request: USER backup
  124 2024-05-03 04:12:54.660157  15.206.185.207   172.31.45.144   FTP      83 Request: USER svcaccount
  125 2024-05-03 04:12:54.660157  15.206.185.207   172.31.45.144   FTP      80 Request: USER backup
  126 2024-05-03 04:12:54.660157  15.206.185.207   172.31.45.144   FTP      80 Request: USER backup
  127 2024-05-03 04:12:54.660157  15.206.185.207   172.31.45.144   FTP      83 Request: USER svcaccount
  128 2024-05-03 04:12:54.660157  15.206.185.207   172.31.45.144   FTP      83 Request: USER svcaccount
  137 2024-05-03 04:12:54.660227  15.206.185.207   172.31.45.144   FTP      83 Request: USER svcaccount
  164 2024-05-03 04:12:54.761216  15.206.185.207   172.31.45.144   FTP      84 Request: PASS ftprocks69$
  165 2024-05-03 04:12:54.761217  15.206.185.207   172.31.45.144   FTP      91 Request: PASS alonzo.spire!rocks
  166 2024-05-03 04:12:54.761217  15.206.185.207   172.31.45.144   FTP      81 Request: PASS 69696969
  167 2024-05-03 04:12:54.761254  15.206.185.207   172.31.45.144   FTP      84 Request: PASS ftprocks69$
  168 2024-05-03 04:12:54.761306  15.206.185.207   172.31.45.144   FTP      81 Request: PASS password
  169 2024-05-03 04:12:54.761349  15.206.185.207   172.31.45.144   FTP      84 Request: PASS password123
  170 2024-05-03 04:12:54.761388  15.206.185.207   172.31.45.144   FTP      91 Request: PASS alonzo.spire!rocks
  171 2024-05-03 04:12:54.761469  15.206.185.207   172.31.45.144   FTP      91 Request: PASS alonzo.spire!rocks
  172 2024-05-03 04:12:54.761511  15.206.185.207   172.31.45.144   FTP      81 Request: PASS password
  173 2024-05-03 04:12:54.761555  15.206.185.207   172.31.45.144   FTP      81 Request: PASS password
  174 2024-05-03 04:12:54.761597  15.206.185.207   172.31.45.144   FTP      84 Request: PASS password123
  175 2024-05-03 04:12:54.761646  15.206.185.207   172.31.45.144   FTP      81 Request: PASS 69696969
  176 2024-05-03 04:12:54.761716  15.206.185.207   172.31.45.144   FTP      81 Request: PASS password
  177 2024-05-03 04:12:54.761763  15.206.185.207   172.31.45.144   FTP      84 Request: PASS ftprocks69$
  178 2024-05-03 04:12:54.761803  15.206.185.207   172.31.45.144   FTP      84 Request: PASS password123
  179 2024-05-03 04:12:54.761853  15.206.185.207   172.31.45.144   FTP      81 Request: PASS 69696969
```

Figure 1: Brute force login attempts

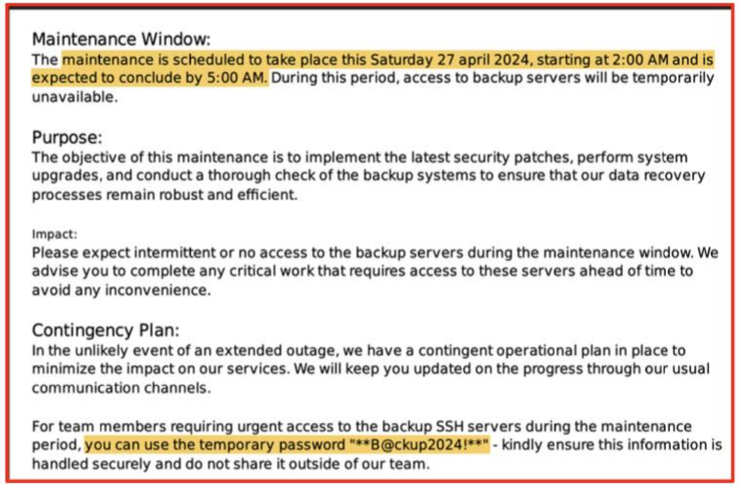
- Attacker downloaded two forms, including a 'Maintenance Notice' PDF and a txt file which contained SSH passwords

- A maintenance time window was exploited; enabled lateral movement into backup systems



```
  300 2024-05-03 04:12:57.650193  15.206.185.207   172.31.45.144   FTP      91 Request: PASS alonzo.spire!rocks
  399 2024-05-03 04:14:10.092755  15.206.185.207   172.31.45.144   FTP      83 Request: USER forela-ftp
  407 2024-05-03 04:14:15.554506  15.206.185.207   172.31.45.144   FTP      84 Request: PASS ftprocks69$
  411 2024-05-03 04:14:15.605045  15.206.185.207   172.31.45.144   FTP      72 Request: SYST
  414 2024-05-03 04:14:15.606799  15.206.185.207   172.31.45.144   FTP      72 Request: FEAT
  421 2024-05-03 04:14:18.403741  15.206.185.207   172.31.45.144   FTP      72 Request: EPSV
  426 2024-05-03 04:14:18.405493  15.206.185.207   172.31.45.144   FTP      72 Request: LIST
  439 2024-05-03 04:14:25.990713  15.206.185.207   172.31.45.144   FTP      72 Request: EPSV
  444 2024-05-03 04:14:25.992486  15.206.185.207   172.31.45.144   FTP      72 Request: NLST
  453 2024-05-03 04:14:26.781964  15.206.185.207   172.31.45.144   FTP      74 Request: TYPE I
  455 2024-05-03 04:14:26.782961  15.206.185.207   172.31.45.144   FTP      95 Request: SIZE Maintenance-Notice.pdf
  457 2024-05-03 04:14:26.783849  15.206.185.207   172.31.45.144   FTP      72 Request: EPSV
  462 2024-05-03 04:14:26.785549  15.206.185.207   172.31.45.144   FTP      95 Request: RETR Maintenance-Notice.pdf
  479 2024-05-03 04:14:26.789175  15.206.185.207   172.31.45.144   FTP      95 Request: MDTM Maintenance-Notice.pdf
  484 2024-05-03 04:14:30.972126  15.206.185.207   172.31.45.144   FTP      87 Request: SIZE s3_buckets.txt
  487 2024-05-03 04:14:30.973027  15.206.185.207   172.31.45.144   FTP      72 Request: EPSV
  492 2024-05-03 04:14:30.974808  15.206.185.207   172.31.45.144   FTP      87 Request: RETR s3_buckets.txt
```

Figure 2: Requests for access to file data



Maintenance Window:
The maintenance is scheduled to take place this Saturday 27 april 2024, starting at 2:00 AM and is expected to conclude by 5:00 AM. During this period, access to backup servers will be temporarily unavailable.

Purpose:
The objective of this maintenance is to implement the latest security patches, perform system upgrades, and conduct a thorough check of the backup systems to ensure that our data recovery processes remain robust and efficient.

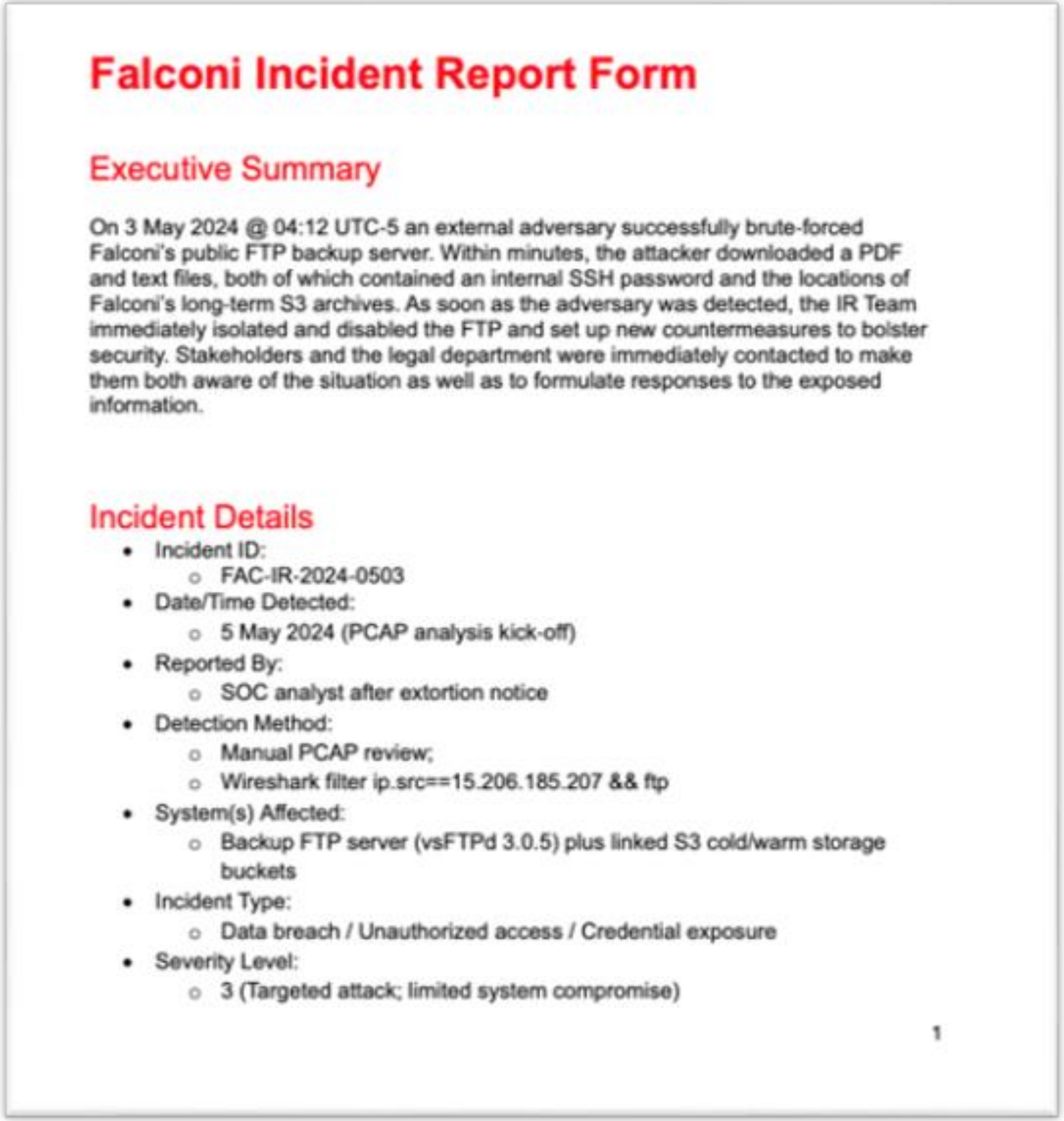
Impact:
Please expect intermittent or no access to the backup servers during the maintenance window. We advise you to complete any critical work that requires access to these servers ahead of time to avoid any inconvenience.

Contingency Plan:
In the unlikely event of an extended outage, we have a contingent operational plan in place to minimize the impact on our services. We will keep you updated on the progress through our usual communication channels.

For team members requiring urgent access to the backup SSH servers during the maintenance period, you can use the temporary password "**B@ckup2024!**" - kindly ensure this information is handled securely and do not share it outside of our team.

Figure 3: Temporary credentials for server access

Incident Response Report



Falconi Incident Report Form

Executive Summary

On 3 May 2024 @ 04:12 UTC-5 an external adversary successfully brute-forced Falconi's public FTP backup server. Within minutes, the attacker downloaded a PDF and text files, both of which contained an internal SSH password and the locations of Falconi's long-term S3 archives. As soon as the adversary was detected, the IR Team immediately isolated and disabled the FTP and set up new countermeasures to bolster security. Stakeholders and the legal department were immediately contacted to make them both aware of the situation as well as to formulate responses to the exposed information.

Incident Details

- Incident ID:
  - FAC-IR-2024-0503
- Date/Time Detected:
  - 5 May 2024 (PCAP analysis kick-off)
- Reported By:
  - SOC analyst after extortion notice
- Detection Method:
  - Manual PCAP review;
  - Wireshark filter ip.src==15.206.185.207 && ftp
- System(s) Affected:
  - Backup FTP server (vsFTPd 3.0.5) plus linked S3 cold/warm storage buckets
- Incident Type:
  - Data breach / Unauthorized access / Credential exposure
- Severity Level:
  - 3 (Targeted attack; limited system compromise)

- **Indicators of Compromise**
  - Brute-force FTP login from 15.206.185.207

- **Impact Assessment**
  - ≈20 GB of backup data exfiltrated; extortion followed
  - No outages; internal credentials and archive paths exposed

- **Mitigation and Containment Steps**
  - FTP disabled, creds rotated, MFA enabled
  - Attacker IP range blocked; forensics captured

- **Lessons Learned**
  - Never store plaintext credentials in files
  - Isolate and monitor backup systems
  - Enforce lockouts, MFA, and data-loss monitoring
  - Treat internal documents as leak-prone

Recapitulation and Acknowledgments

FALCONI
SPORTS AGENCY

✓ Team and Strategy

- Incident Response Team
- Incident Response Plan (Initial)
- Tabletop Exercise
- Incident Response Plan (Revisions)

✓ Incident Analysis and Response

- Incident Report #1
- Incident Report #2

Thanks to the following teams for their contributions:

- **Risk Management Framework**
- **Cyber Essentials**

Special thanks to our partners at:

Solutions³ LLC
Mike Battistella, Kristen Nova, Shannon Conley, and Mark Marino

Hack The Box
Floyd Haynes, Chandler Anderson