



Falconi[®] Sports Agency

Risk Management Framework Overview

*Proactive Assessment, Strategic Mitigation, and
Operational Resilience*

Presented by: Risk Management Team

In collaboration with: Cyber Essentials and Incident Response Teams

Table of Contents

❑ Risk Register & Web Reconnaissance

- Risk Register 04
- Recon Findings Summary 05

❑ Network Analysis & OSINT

- Network Traffic Analysis 08
- OSINT Risk Exposure 10

❑ Vulnerability Scanning & Analysis

- Vulnerability Scan & Analysis Report 12



Risk Register & Web Reconnaissance

Identifying and Understanding Organizational Risks Through Frameworks and Reconnaissance

Risk Register

- Centralized log of risks with ID's
- Prioritizes threats for focused action
- Tracks mitigation for transparency and compliance
- Provides early warning for emerging risks

Risk	Risk Description	Likelihood	Impact	Mitigation Actions
Unsecure Admin Directory	Use of admin directories and interfaces that contain sensitive unencrypted information that can be found and accessed by an attacker	Medium	High	-Require authentication to access admin areas -Regularly perform scans to find exposed endpoints -Encrypt sensitive information
Forgotten Subdomains	Older or discontinued web applications hosted on forgotten subdomains may contain unpatched vulnerabilities or sensitive information. These neglected applications increase the attack surface and can be exploited to compromise systems or access confidential data.	Medium	High	-Maintain an updated list of all accessible subdomains -Remove discontinued applications and services from servers -Monitor access logs and unusual activity on legacy subdomains
Misconfigured Network Infrastructure	Insecure or misconfigured network components, such as open ports, weak firewall rules, outdated router firmware, or use of unencrypted protocols. May provide attackers with unauthorized access to internal systems and data.	Medium	High	-Regularly scan for open ports -Implement firewalls to restrict network traffic for unauthorized IP addressed. -Close and block unnecessary and unused ports

Recon Findings Summary



Prepared by: Luigi Falconi, CISO
Chief Information Security Officer
July 24th, 2025



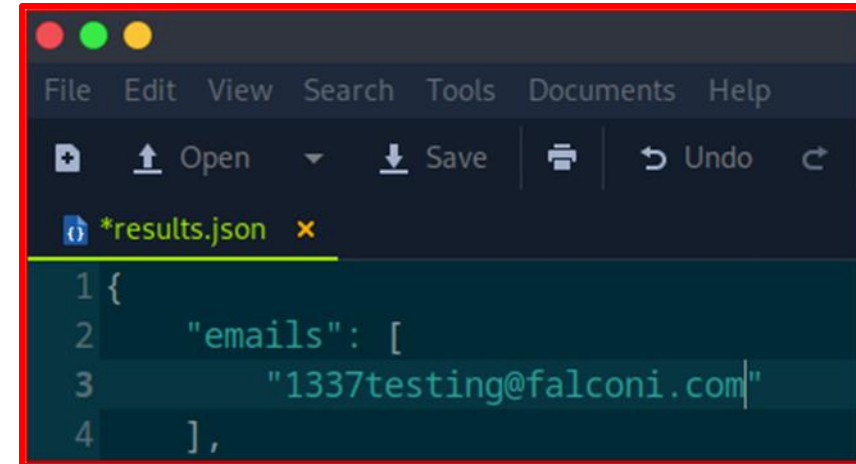
security@falconi.com
220 Gardenpoint Plaza, Suite 205, Newark, NJ 0710
(973) 555-1490

1

- Details publicly discoverable assets and potential security exposures
- Surfaces hidden risks that attackers can exploit (open ports, forgotten subdomains, leaked credential)
- ReconSpider for crawling, Gobuster/dnsenum for subdomain enumeration, FTP brute-forcing
- Linked each discovery to its risk ID

Recon Findings (API Key)

- **Potential Exposure:** API key leaked in public config and hidden admin path (R-6)
- **Impact:** Enables authentication bypass and backend takeover
- **Mitigation:** Remove coded keys, lock down endpoints, rotate credentials



```
1 {  
2   "emails": [  
3     "1337testing@falconi.com"  
4   ],
```

```
105   ],  
106   "external_files": [],  
107   "js_files": [],  
108   "form_fields": [],  
109   "images": [],  
110   "videos": [],  
111   "audio": [],  
112   "comments": [  
113     "<!-- Remember to change the API key to ba988b835be4aa97d068941dc852ff33 -->"  
114   ]  
115 }
```

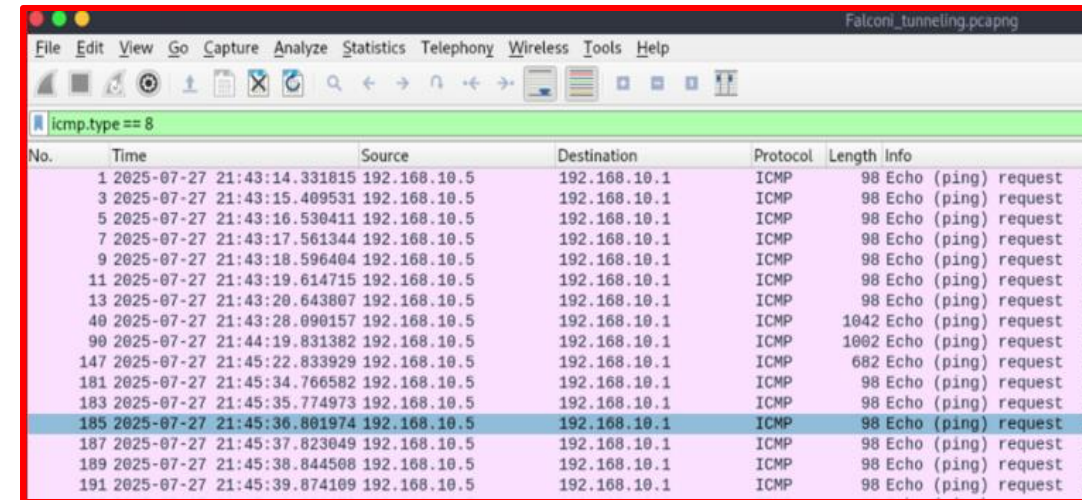


Network Analysis & OSINT

Identifying and Mitigating Risk through Traffic Inspection and Open-Source Intelligence

Network Threat Analysis

- Understanding Threats Through Real-World Traffic Analysis
- Identified three key threats:
 - **ARP spoofing**
 - **ICMP tunneling**
 - **Cross-site scripting**
- Focused on understanding how each threat could impact Falconi's systems



No.	Time	Source	Destination	Protocol	Length	Info
1	2025-07-27 21:43:14.331815	192.168.10.5	192.168.10.1	ICMP	98	Echo (ping) request
3	2025-07-27 21:43:15.409531	192.168.10.5	192.168.10.1	ICMP	98	Echo (ping) request
5	2025-07-27 21:43:16.530411	192.168.10.5	192.168.10.1	ICMP	98	Echo (ping) request
7	2025-07-27 21:43:17.561344	192.168.10.5	192.168.10.1	ICMP	98	Echo (ping) request
9	2025-07-27 21:43:18.596404	192.168.10.5	192.168.10.1	ICMP	98	Echo (ping) request
11	2025-07-27 21:43:19.614715	192.168.10.5	192.168.10.1	ICMP	98	Echo (ping) request
13	2025-07-27 21:43:20.643807	192.168.10.5	192.168.10.1	ICMP	98	Echo (ping) request
40	2025-07-27 21:43:28.090157	192.168.10.5	192.168.10.1	ICMP	1042	Echo (ping) request
90	2025-07-27 21:44:19.831382	192.168.10.5	192.168.10.1	ICMP	1002	Echo (ping) request
147	2025-07-27 21:45:22.833929	192.168.10.5	192.168.10.1	ICMP	682	Echo (ping) request
181	2025-07-27 21:45:34.766582	192.168.10.5	192.168.10.1	ICMP	98	Echo (ping) request
183	2025-07-27 21:45:35.774973	192.168.10.5	192.168.10.1	ICMP	98	Echo (ping) request
185	2025-07-27 21:45:36.801974	192.168.10.5	192.168.10.1	ICMP	98	Echo (ping) request
187	2025-07-27 21:45:37.823049	192.168.10.5	192.168.10.1	ICMP	98	Echo (ping) request
189	2025-07-27 21:45:38.844508	192.168.10.5	192.168.10.1	ICMP	98	Echo (ping) request
191	2025-07-27 21:45:39.874109	192.168.10.5	192.168.10.1	ICMP	98	Echo (ping) request

Findings and Impact



- Duplicate IPs, large packets, and suspicious traffic uncovered
- Indicated interception, data theft and malicious browser activity
- Risked operational disruption and exposure of sensitive player data

[Response time: 2.619 ms]	
- Data (48000 bytes)	
Data: 56476870637942706379426849484e6c5935356795a5342725a586b364945746c	
[Length: 48000]	
0030	51 31 4e 6a 63 34 4f 51 6f 3d 56 47 68 70 63 79 Q1Njc40Q o=Vghpcy
0040	42 70 63 79 42 68 49 48 4e 6c 59 33 56 79 5a 53 BpcyBhIH nLy3VyZS
0050	42 72 5a 58 6b 36 49 45 74 6c 65 54 45 79 4d 7a BrZXk6IE tleTeyMz
0060	51 31 4e 6a 63 34 4f 51 6f 3d 56 47 68 70 63 79 Q1Njc40Q o=Vghpcy
0070	42 70 63 79 42 68 49 48 4e 6c 59 33 56 79 5a 53 BpcyBhIH nLy3VyZS
0080	42 72 5a 58 6b 36 49 45 74 6c 65 54 45 79 4d 7a BrZXk6IE tleTeyMz
0090	51 31 4e 6a 63 34 4f 51 6f 3d 56 47 68 70 63 79 Q1Njc40Q o=Vghpcy
00a0	42 70 63 79 42 68 49 48 4e 6c 59 33 56 79 5a 53 BpcyBhIH nLy3VyZS
00b0	42 72 5a 58 6b 36 49 45 74 6c 65 54 45 79 4d 7a BrZXk6IE tleTeyMz
00c0	51 31 4e 6a 63 34 4f 51 6f 3d 56 47 68 70 63 79 Q1Njc40Q o=Vghpcy
00d0	42 70 63 79 42 68 49 48 4e 6c 59 33 56 79 5a 53 BpcyBhIH nLy3VyZS
00e0	42 72 5a 58 6b 36 49 45 74 6c 65 54 45 79 4d 7a BrZXk6IE tleTeyMz
00f0	51 31 4e 6a 63 34 4f 51 6f 3d 56 47 68 70 63 79 Q1Njc40Q o=Vghpcy
0100	42 70 63 79 42 68 49 48 4e 6c 59 33 56 79 5a 53 BpcyBhIH nLy3VyZS
Frame (682 bytes)	Reassembled IPv4 (48008 bytes)

```

[us-trial-dedi-1]-[10.10.14.3]-[jesus8a7@htb-ip1bqzwfbo]-[~]
[*]$ echo "RmFsY29uaSBTZWN1cm10eSBub2t1bjogU0VudLVRPSy0yMDI1MDcyOC1BbHB0YQ==" | base64 -d
Falconi Security Token: SEC-TOK-20250728-Alpha[us-trial-dedi-1]-[10.10.14.3]-[jesus8a7@htb-ip1bqzwfbo]-[~]

```

OSINT Risk Exposure

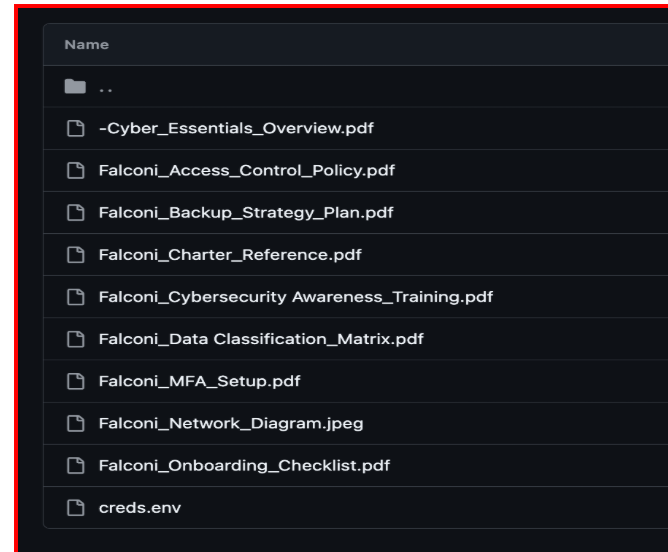
Publicly available information revealed potential risks across Falconi's digital footprint

People & Presence



Public posts and employee interactions reveal names, roles, and relationships that attackers could use for targeting

Internal Data Leaks



Screen capture of public Falconi Github repository containing internal strategy documents and credentials

Cloud Infrastructure

```
"mayor": {
  "count": 16,
  "user": {
    "id": "[REDACTED]",
    "firstName": "[REDACTED]",
    "lastName": "[REDACTED]",
    "photo": "http://[REDACTED].s3.amazonaws.com/[REDACTED]",
    "gender": "[REDACTED]",
    "homeCity": "[REDACTED]"
  }
}
```

JSON response revealing a publicly accessible Amazon S3 URL hosting user photo metadata that if misconfigured, could expose sensitive information.



Vulnerability Scanning & Analysis

*Strengthening Technical Skills for Risk
Identification and Investigation*

Vulnerability Scan Report

- Summarized the results of an assessment conducted on Solutions³'s external digital assets
- Scanned public-facing services and subdomains to identify potential security weaknesses.
- Checked for known vulnerabilities across web infrastructure that could be exploited by attackers.

Vulnerabilities					
SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
MEDIUM	6.5	-	-	104743	TLS Version 1.0 Protocol Detection
MEDIUM	6.5	-	-	157288	TLS Version 1.1 Deprecated Protocol

Figure 2: Nessus Scan Findings

















Issue	Factor	Threat level	Breach risk	Impact	Findings	Source	Attestation
Content Security Policy (CSP) Missing	Application Security	 Medium	 Low	 1.1	2		
Insecure HTTPS Redirect Pattern	Application Security	 Medium	 Low	 0.2	1		
Website Does Not Implement HSTS Best Practices	Application Security	 Medium	 Low	 0.2	2		
Unsafe Implementation Of Subresource Integrity	Application Security	 Info	 Low	 2.2	2		

Figure 3: Security Scorecard findings

Vulnerability: Missing Content Security Policy

Vulnerability:

- CSP's are added to HTTP headers to tell browsers which sources of content are safe
- Site exposed to unauthorized content and code execution

Risks:

- Cross Site Injection Attacks
- Sensitive user data can be stolen, altered, or misused.
- Monetary and reputational damage

Recommendations:

- Deploy CSP via HTTP headers
- Whitelist only trusted sources
- Monitor and update sites regularly



Next Steps

Remediation Actions

Based on our assessment, the following three remediation actions should be prioritized to address the most impactful vulnerabilities and significantly improve Solutions3's overall security posture:

1. Disable TLS 1.0 and 1.1. Configure systems to use TLS 1.2 or 1.3 exclusively.
2. Deploy a CSP header to restrict content sources, starting in report-only mode to test for conflicts before enforcement.
3. Enable HSTS to require HTTPS for all site access and subdomains

Conclusions

- Several easily preventable, low severity security vulnerabilities present
- No high severity vulnerabilities found
- Highlights Solutions3's strong cybersecurity posture

Recapitulation and Acknowledgments



✓ Risk Register & Web Recon

- Risk Register
- Recon Findings Summary

✓ Network Analysis & OSINT

- Network Traffic Analysis
- Risk Exposure Summary

✓ Vulnerability Scanning & Analysis

- Vulnerability Scan & Analysis Report

Thanks to the following teams for their contributions:

- Cyber Essentials
- Incident Response

Special thanks to our partners at:

Solutions³ LLC 

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

Hack The Box 

Floyd Haynes, Chandler Anderson