Red Teaming – Theoretical Knowledge Report

# 1. Advanced Threat Analysis

## Core Concepts

• Threat Modeling: Master STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege) to identify threats by mapping assets, entry points, and trust boundaries.  
 Example: Apply STRIDE to a web application to identify spoofing risks in user authentication.

• MITRE ATT&CK Framework: Understand tactics (e.g., Initial Access, Execution) and techniques (e.g., T1059 - Command and Scripting Interpreter) to analyze adversary behaviors and align with defensive measures.  
 Example: Map a phishing attack to T1566.

• Advanced Attack Vectors: Study Advanced Persistent Threats (APTs) for long-term targeted attacks, supply chain attacks for third-party compromise, and zero-day exploits for undisclosed vulnerabilities.  
 Example: Analyze the SolarWinds attack for supply chain tactics.

## Key Objectives

• Build skills to model threats.  
• Map attacks to MITRE ATT&CK.  
• Understand sophisticated attack vectors for proactive defense.

# 2. Security Frameworks in Depth

## Core Concepts

• NIST Cybersecurity Framework (CSF): Five functions – Identify, Protect, Detect, Respond, Recover.  
 Example: Use Identify to catalog critical assets in a mock organization.

• ISO 27001 Controls: 114 controls across 14 domains (e.g., A.12.4 - Logging and Monitoring, A.14.2 - Security in Development).  
 Example: Apply A.12.3 (Backup) to mitigate ransomware risks.

• Framework Application: Map controls to real-world scenarios, such as ransomware mitigation.

## Key Objectives

• Apply NIST CSF and ISO 27001 to design/evaluate cybersecurity programs.  
• Understand compliance and defense alignment.

# 3. Incident Response Fundamentals

## What to Learn

• Incident Lifecycle: Preparation, Detection, Containment, Eradication, Recovery.  
• Role of playbooks, SOC workflows, and incident prioritization.

# 4. Risk Management Advanced Concepts

## What to Learn

• Concepts: Quantitative vs. qualitative risk assessment, Business Impact Analysis (BIA).

## Key Objectives

• Quantify risks and assess business impacts effectively.

# Screenshots

Insert relevant screenshots here for threat modeling, frameworks, incident response, and risk management exercises.

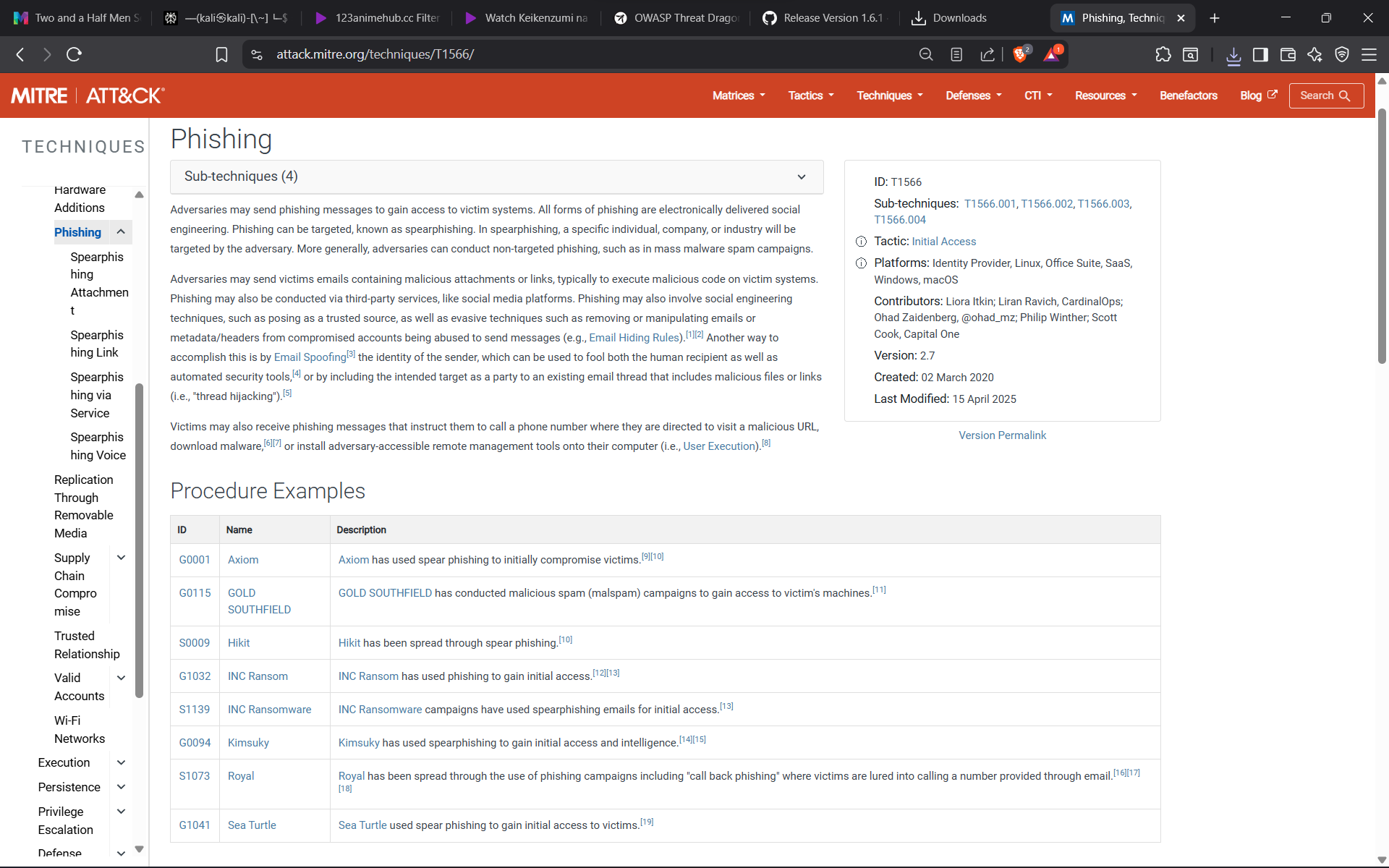


Figure: Screenshot 2025-08-20 091943.png related to Advanced Threat Analysis

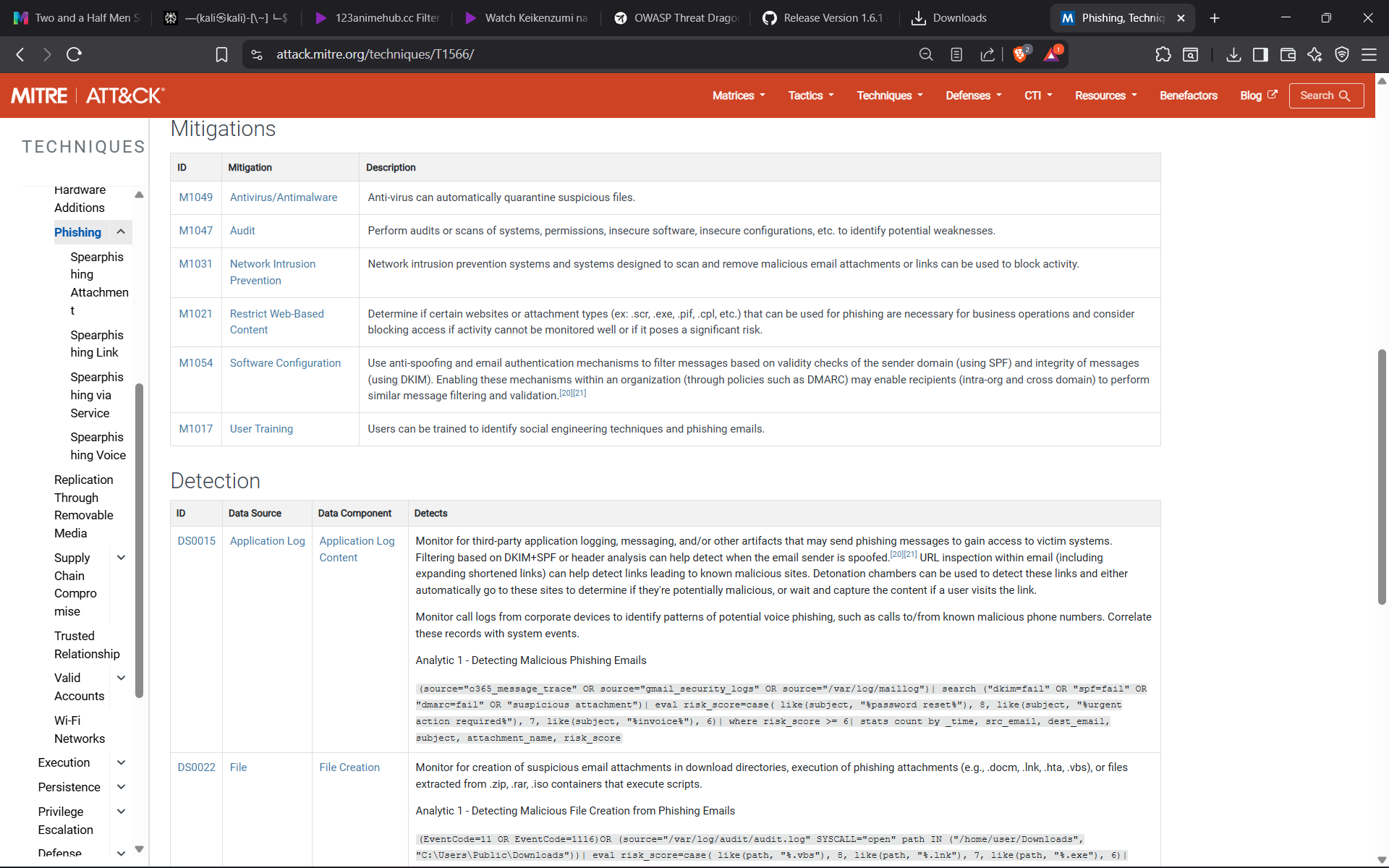


Figure: Screenshot 2025-08-20 091956.png related to Advanced Threat Analysis

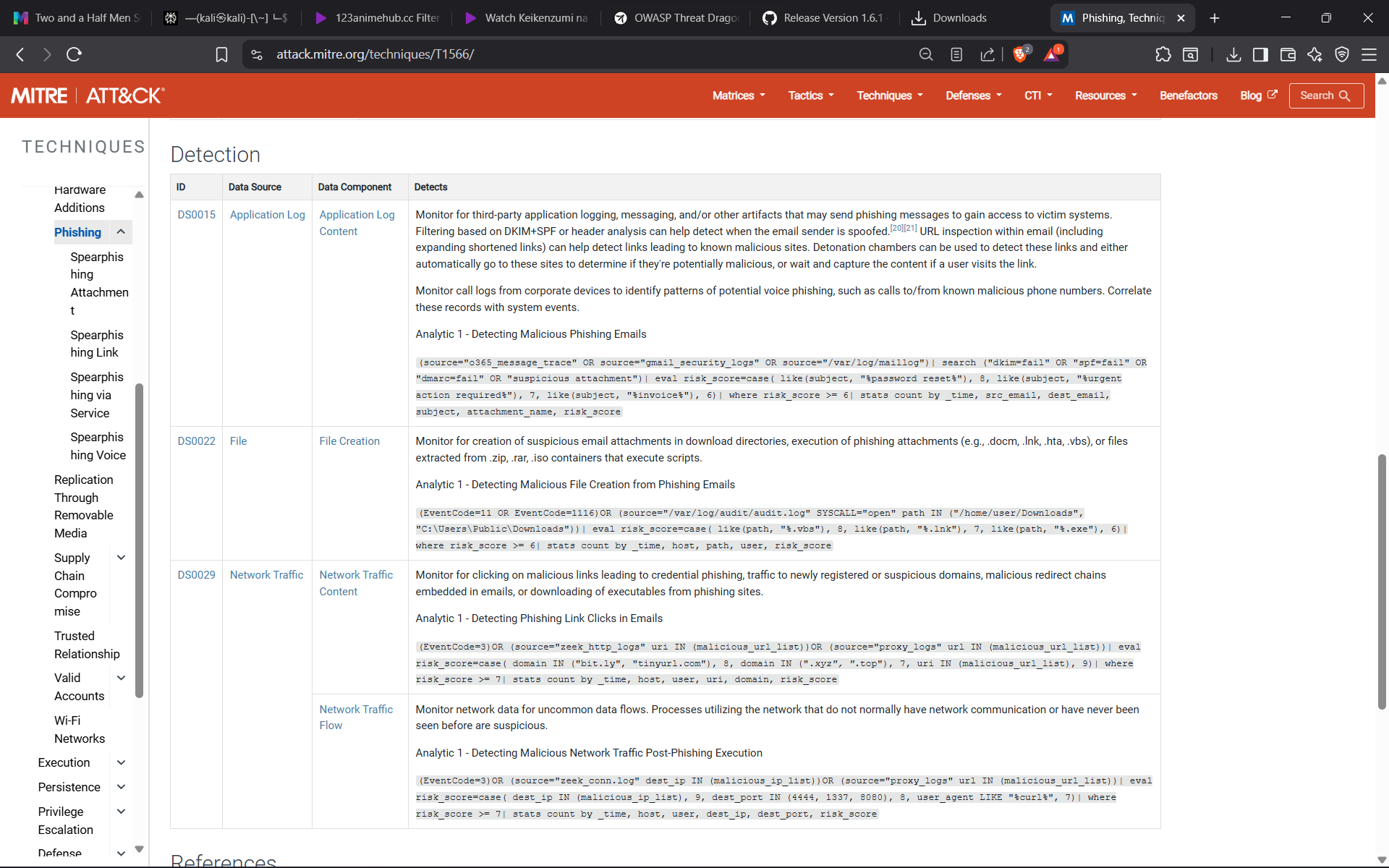


Figure: Screenshot 2025-08-20 092008.png related to Advanced Threat Analysis

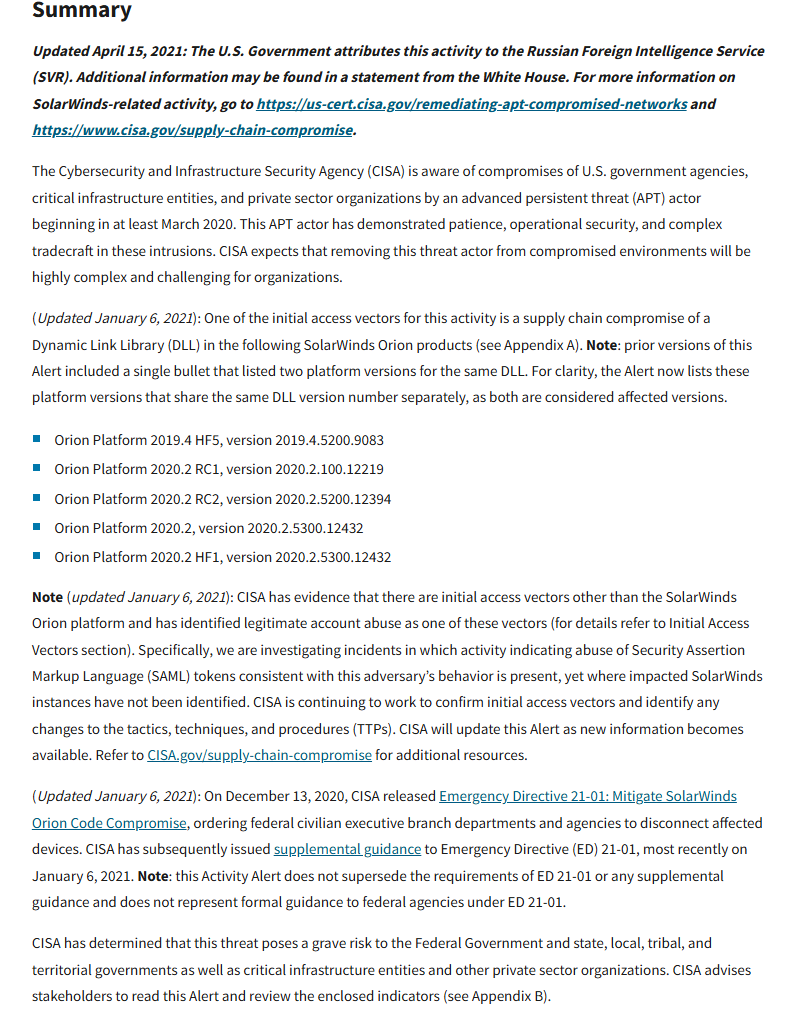


Figure: Screenshot 2025-08-20 092201.png related to Advanced Threat Analysis

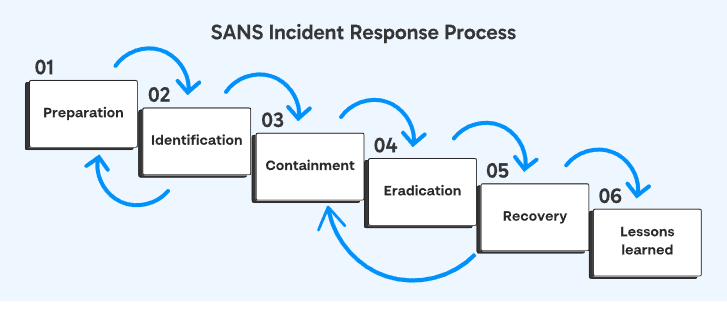


Figure: Screenshot 2025-08-20 095325.png related to Advanced Threat Analysis

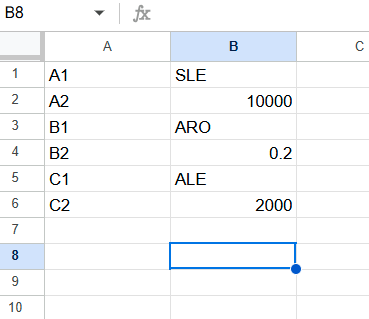


Figure: Screenshot 2025-08-20 095950.png related to Advanced Threat Analysis

[Error inserting /mnt/data/red\_team\_screens/14-domains-819x1024.webp]

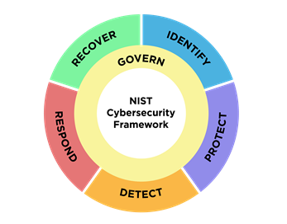


Figure: CSFwheel.png related to Security Frameworks in Depth

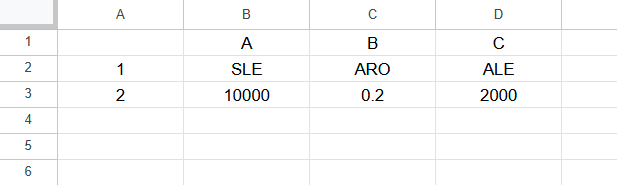


Figure: Screenshot 2025-08-21 121123.png related to Incident Response Fundamentals

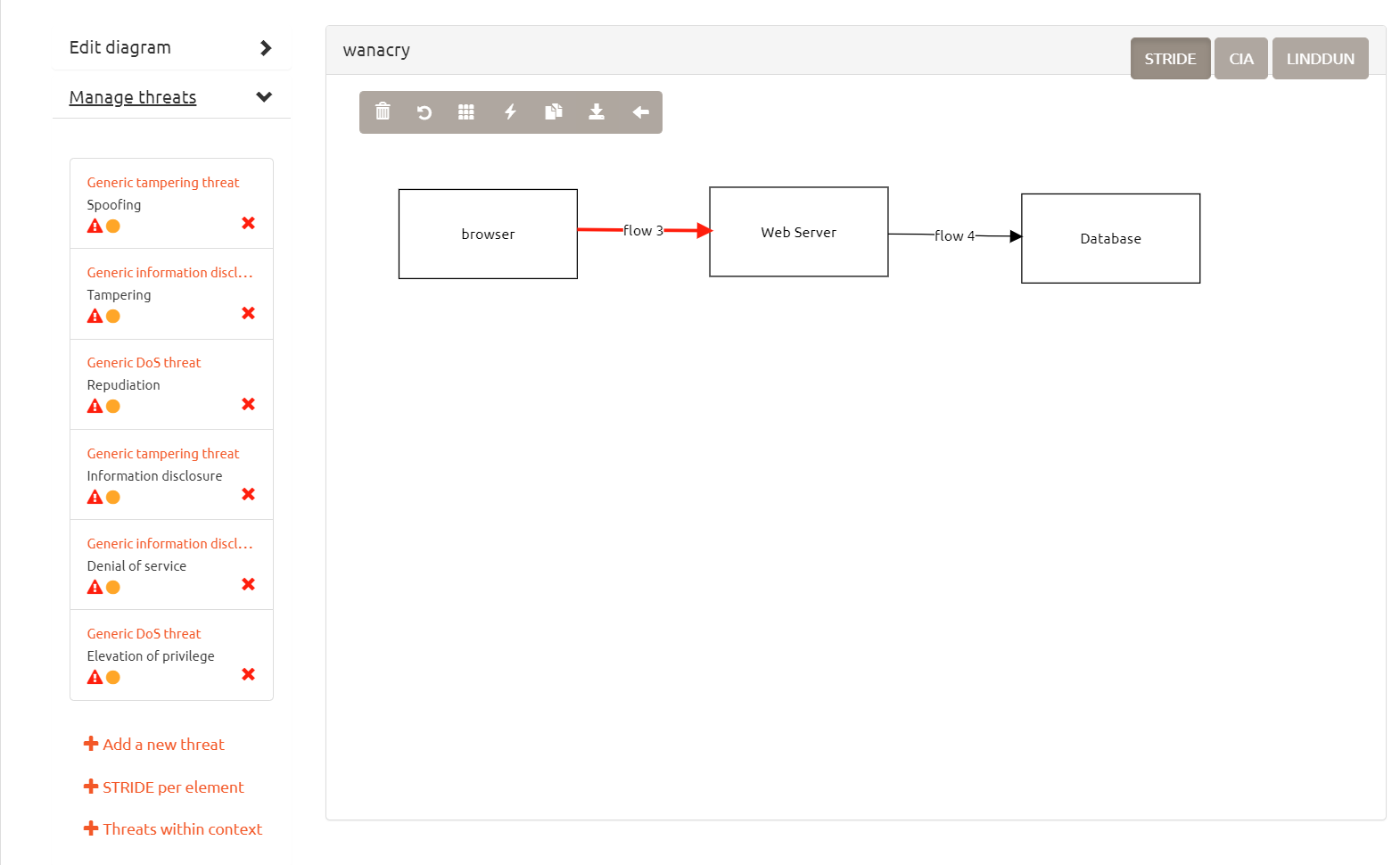


Figure: Screenshot 2025-08-21 121940.png related to Incident Response Fundamentals

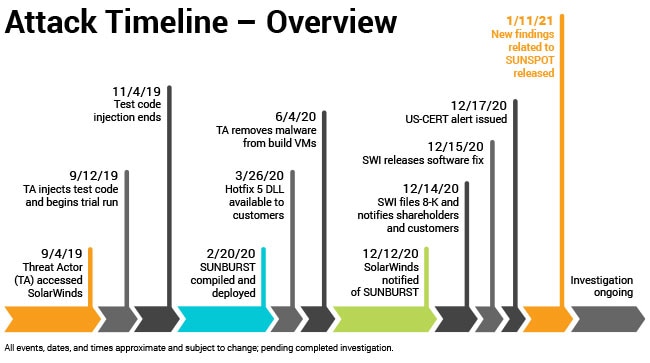


Figure: TimelineGraphic8.jpg related to Incident Response Fundamentals

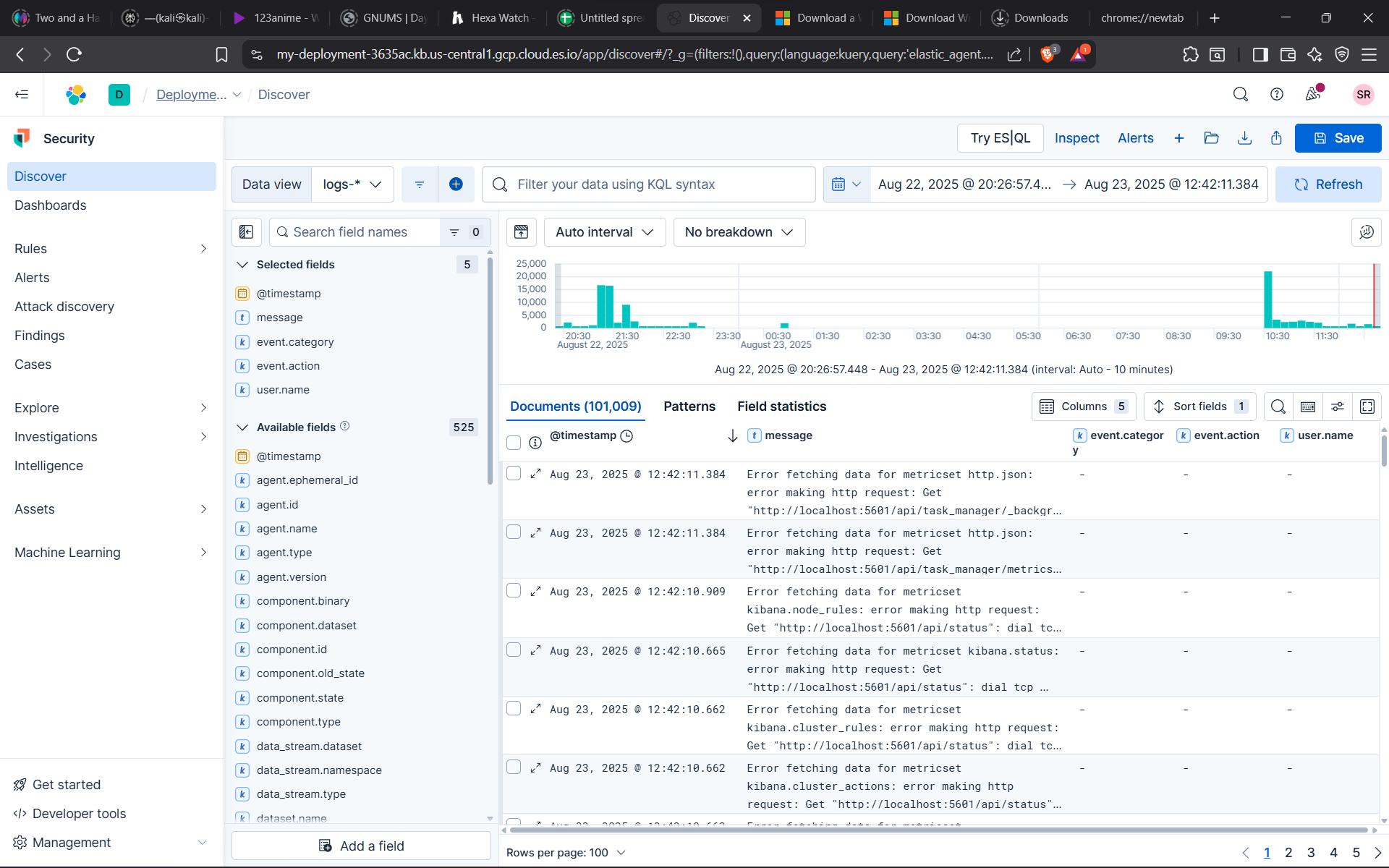


Figure: Screenshot 2025-08-23 124241.png related to Risk Management Advanced Concepts

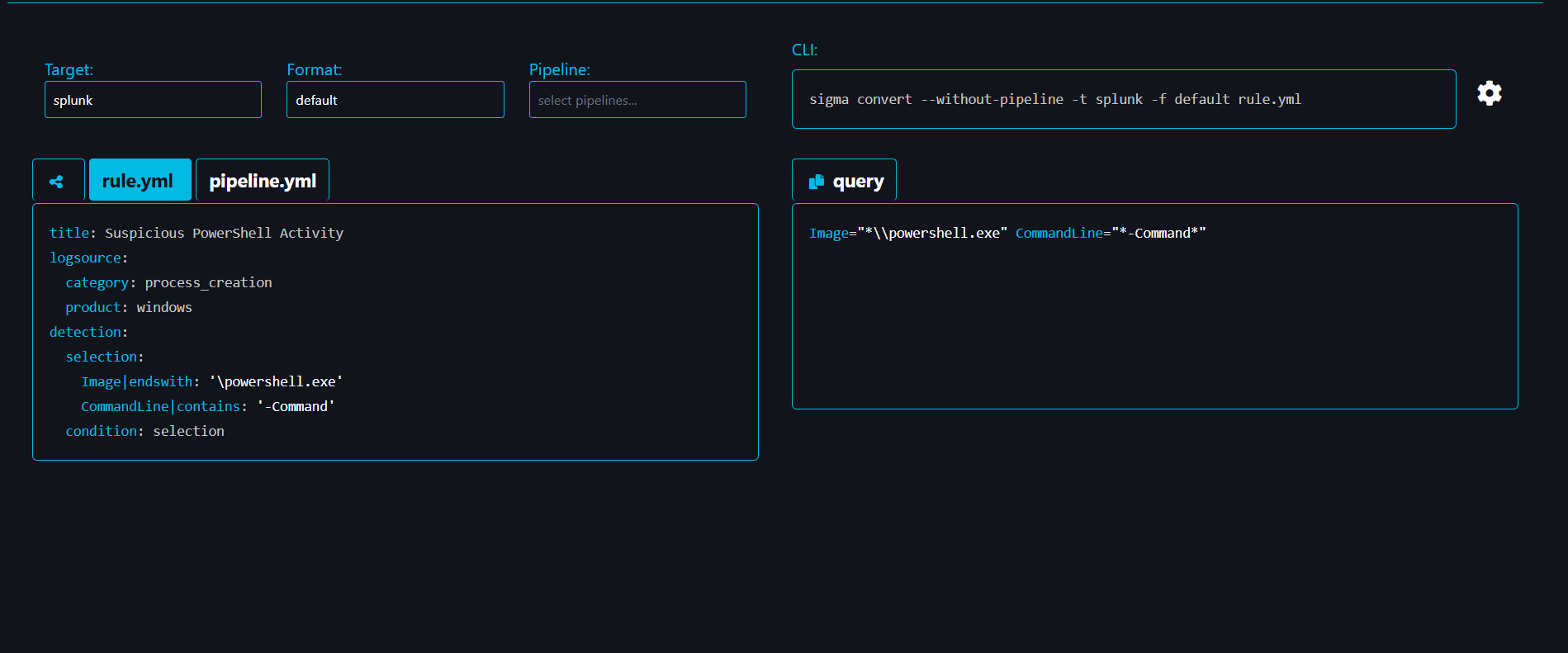


Figure: Screenshot 2025-08-23 124941.png related to Risk Management Advanced Concepts

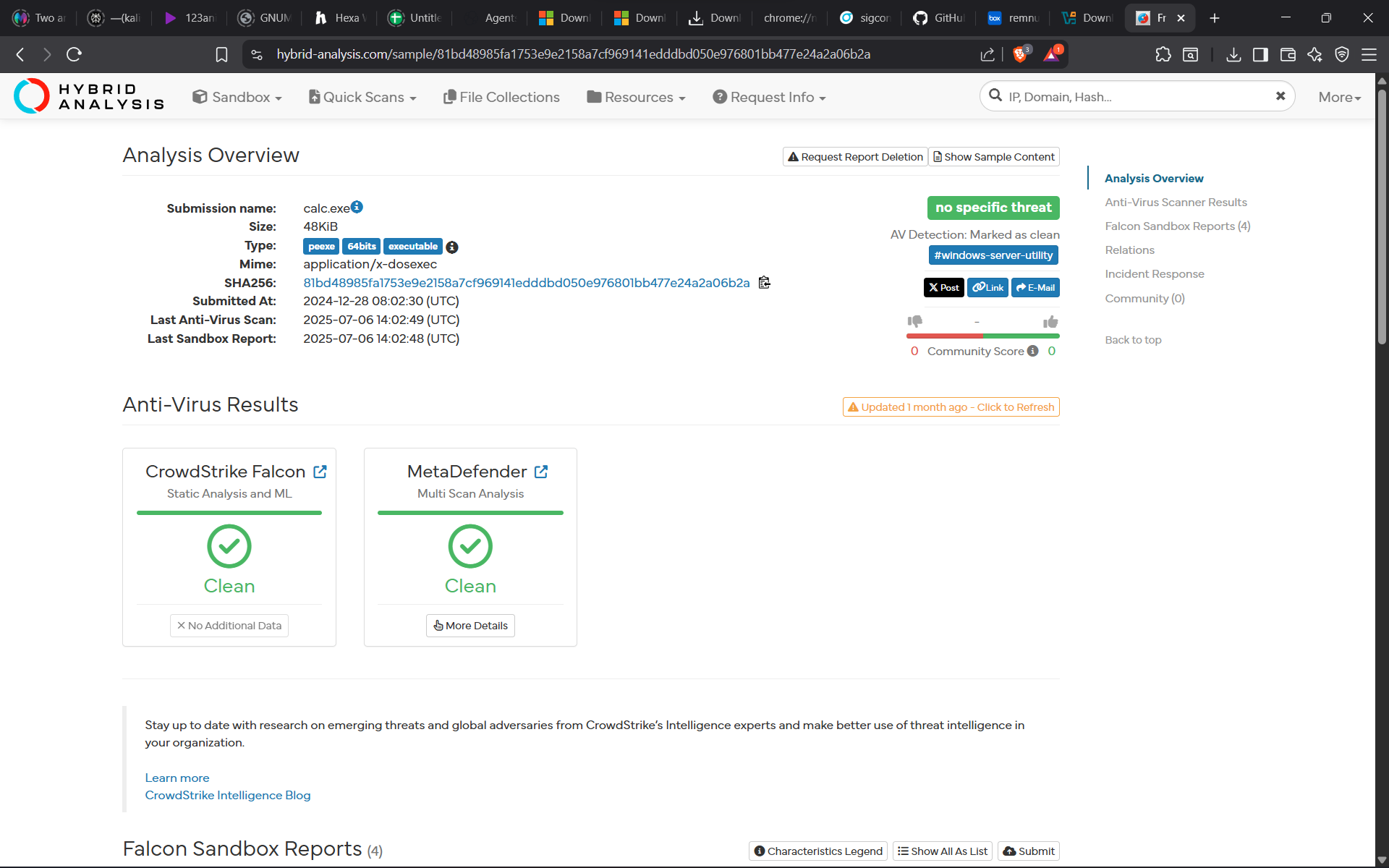


Figure: Screenshot 2025-08-23 143556.png related to Risk Management Advanced Concepts

[Error inserting /mnt/data/red\_team\_screens/how-ransomware-works.avif]