Security Operation Center Analyst L1

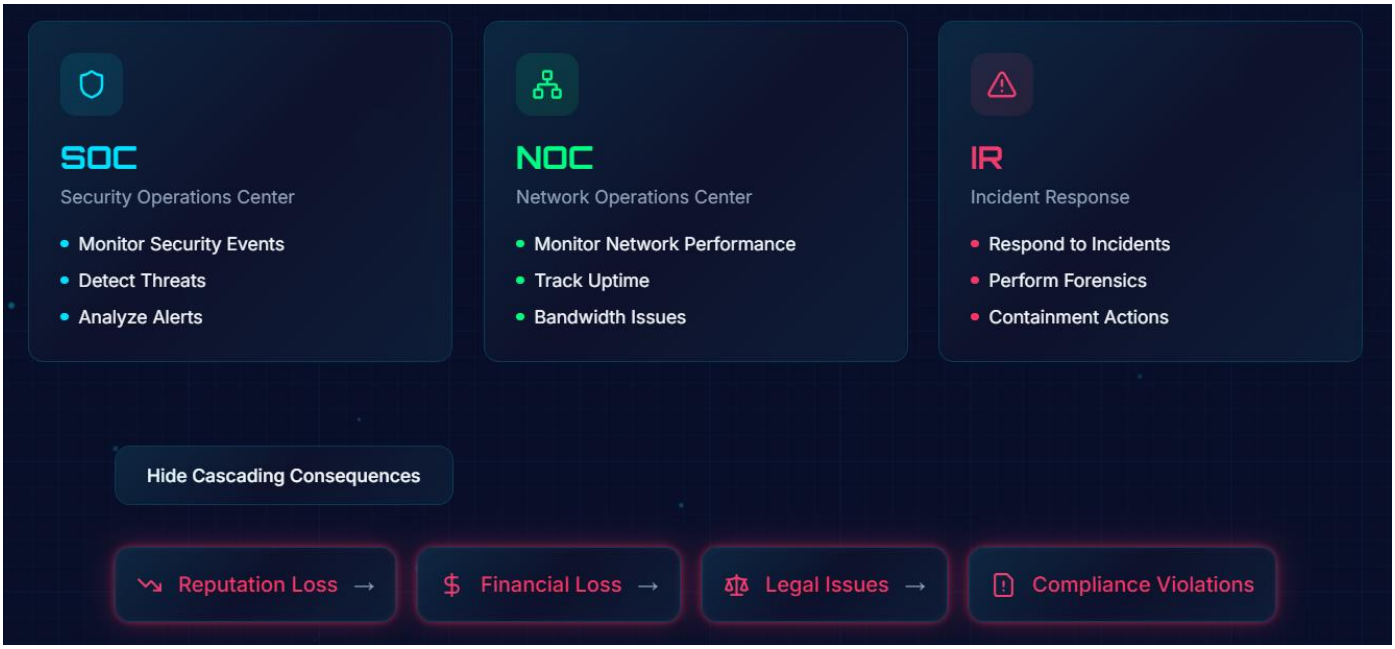
Why SOC Exists?

Organization bleed data and money. The SOC exists to minimize DWELL-Time (the time an attacker stay hidden). Without SOC, breacher are discovered by customers or FBI causing massive reputation and financial loss.

SOC: Monitor Security Events, Detect Threats, Analyze Alerts

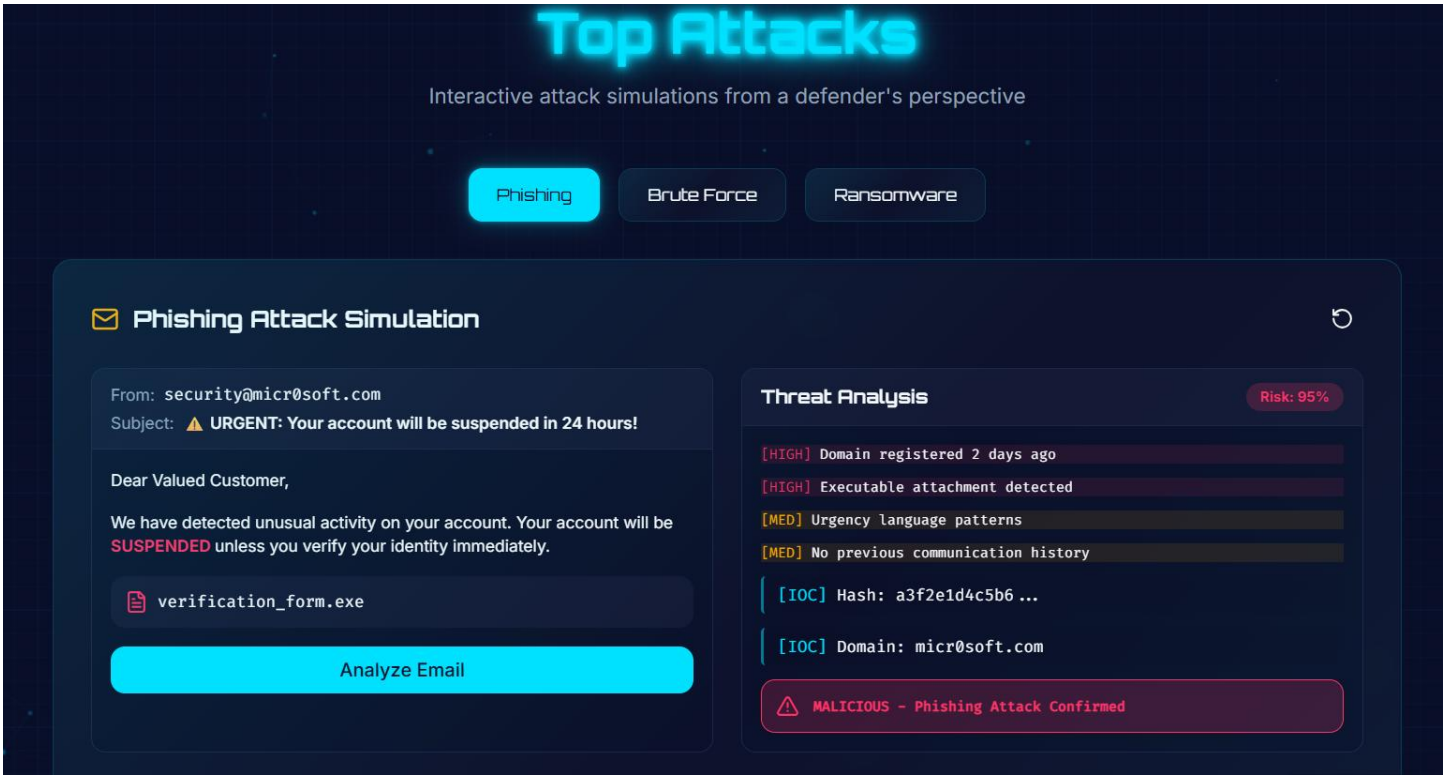
NOC (Network Operation Center): Monitor Network Performance, Uptime, Bandwidth Issues

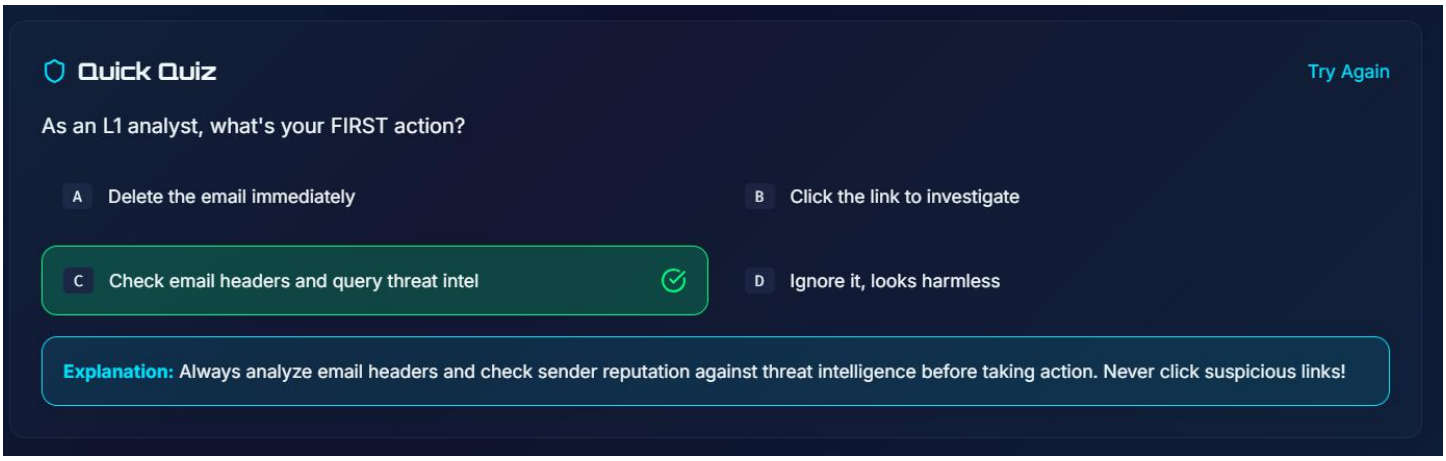
IR (Incidence Response) Team: Responds to Confirmed Incidents, Performs Forensics, Containment



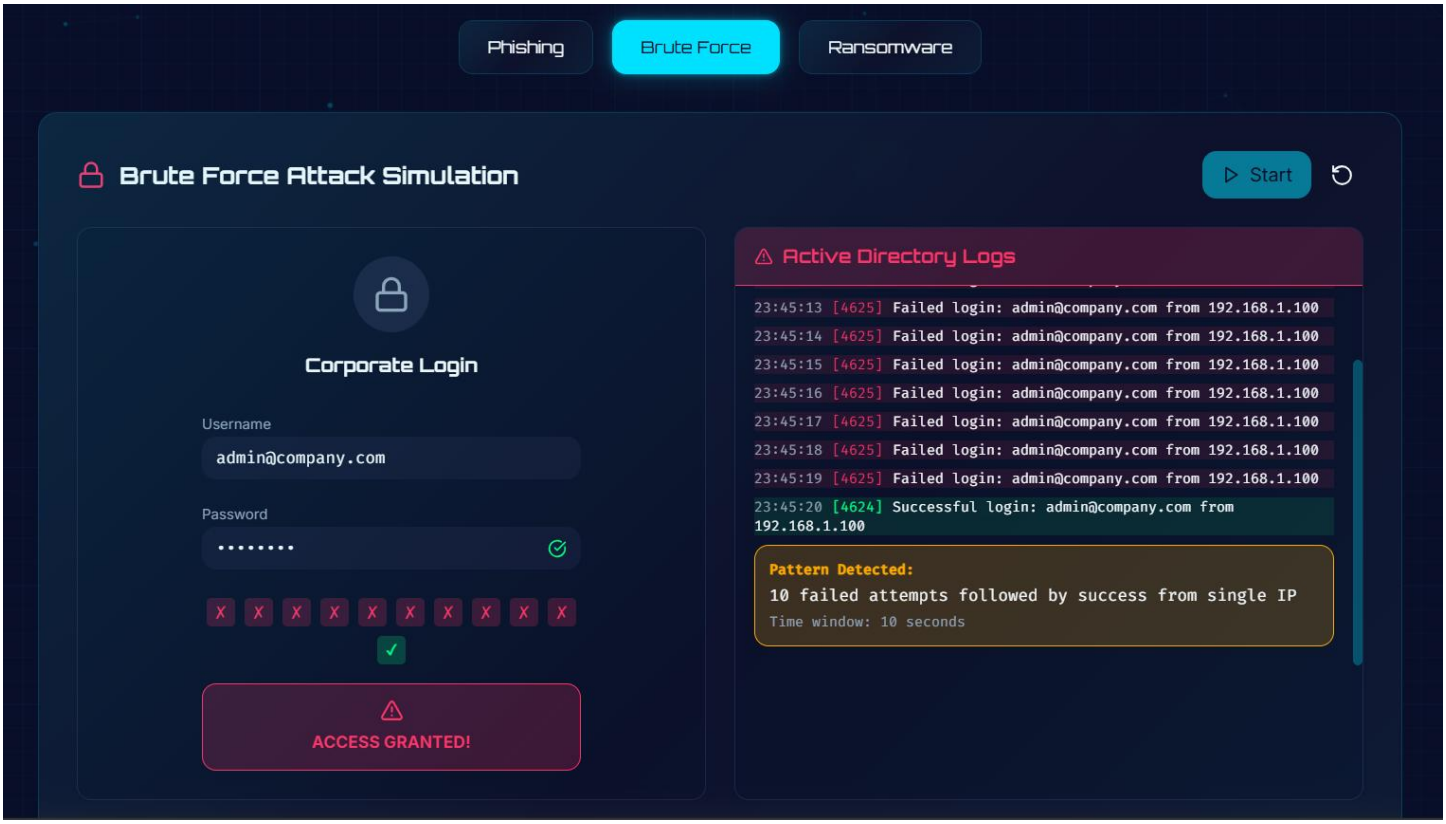
Top Attacks that SOC Analyst Deals with

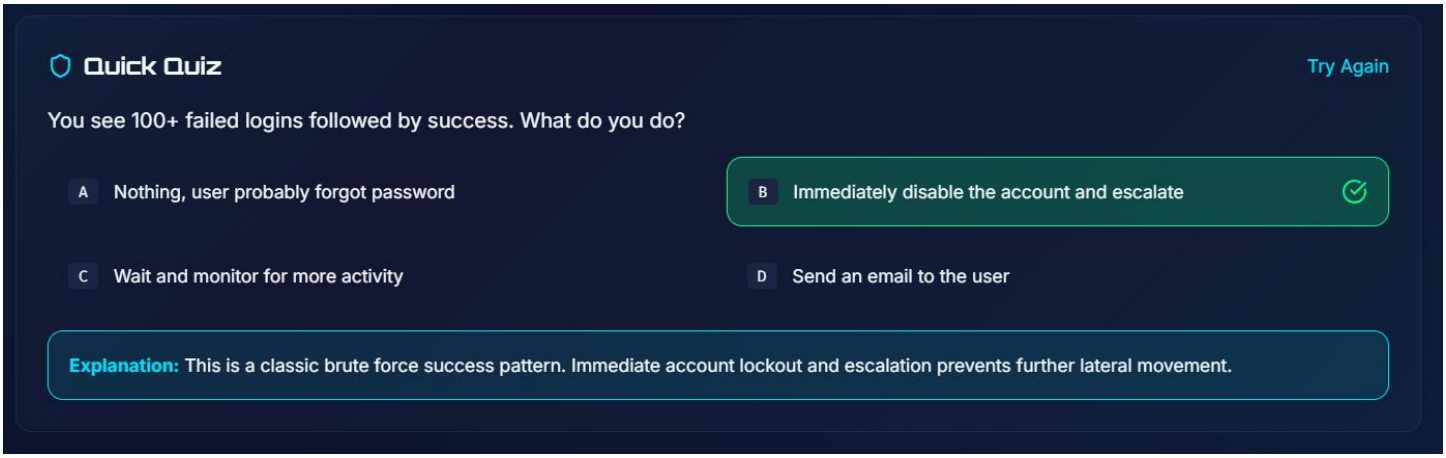
1. **Phishing Attack**
   Log: Email Gateway
   Look For: Typos squatting domains, urgency in subject, suspicious attachments (.iso,.exe)



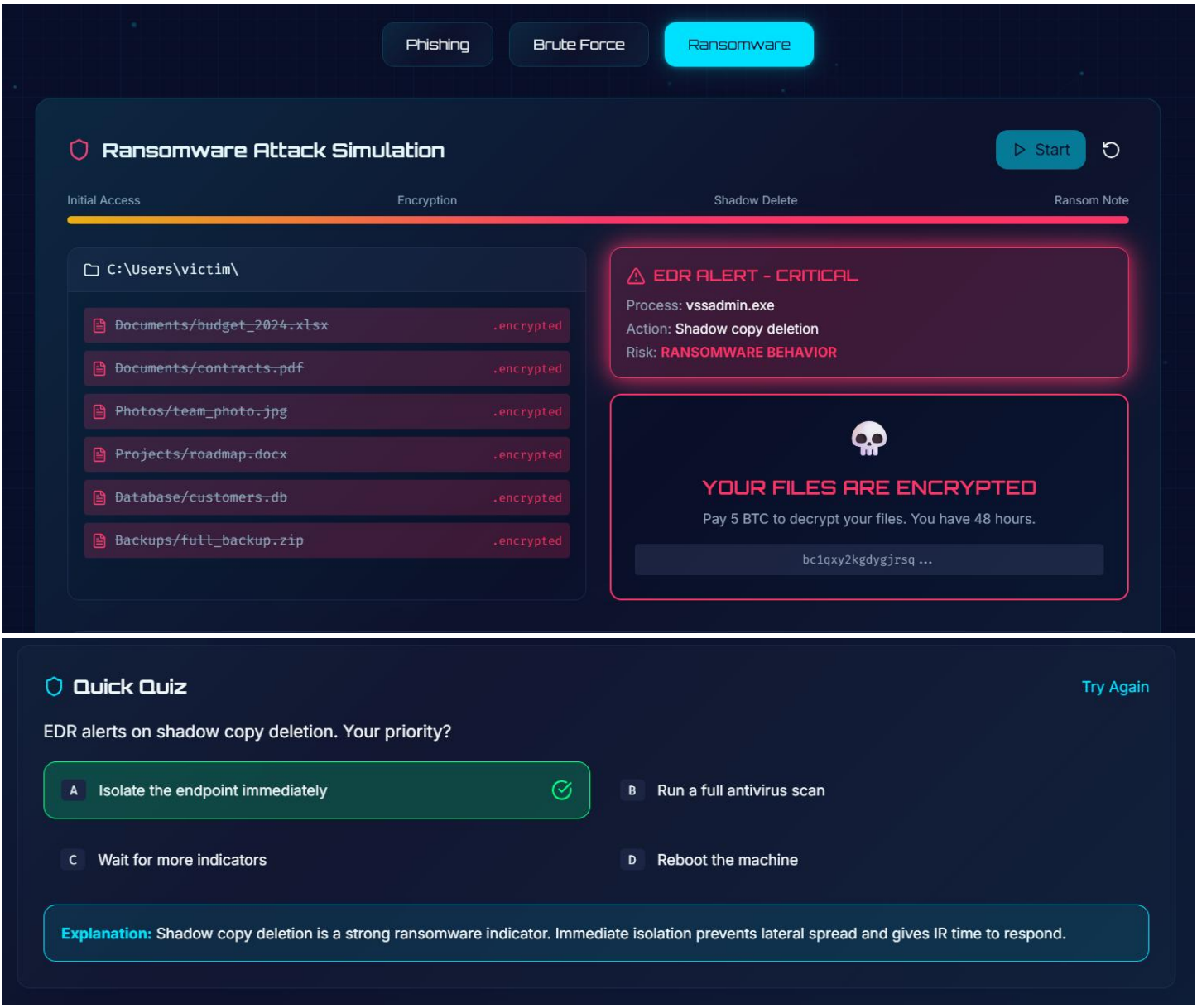


2. **Brute Force**
   Log: Active Directory, Azure AD
   Look For: 4625 (failed login) x 100 followed by 4624 (Success)





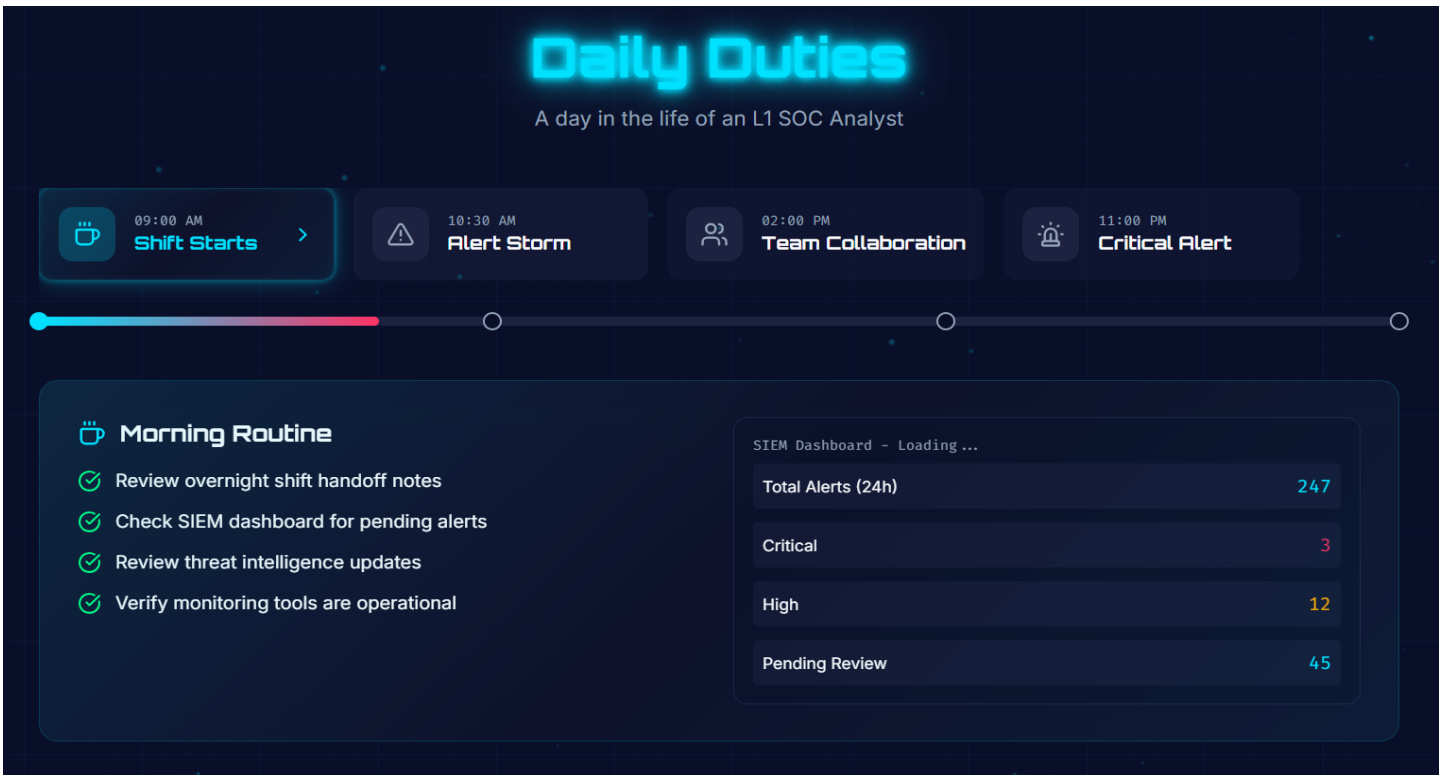
3. **Ransomware**
   Log: EDR/File server.
   Look For: Mass file notification, Volume shadow copy deletion (“vssadmin delete shadows”).

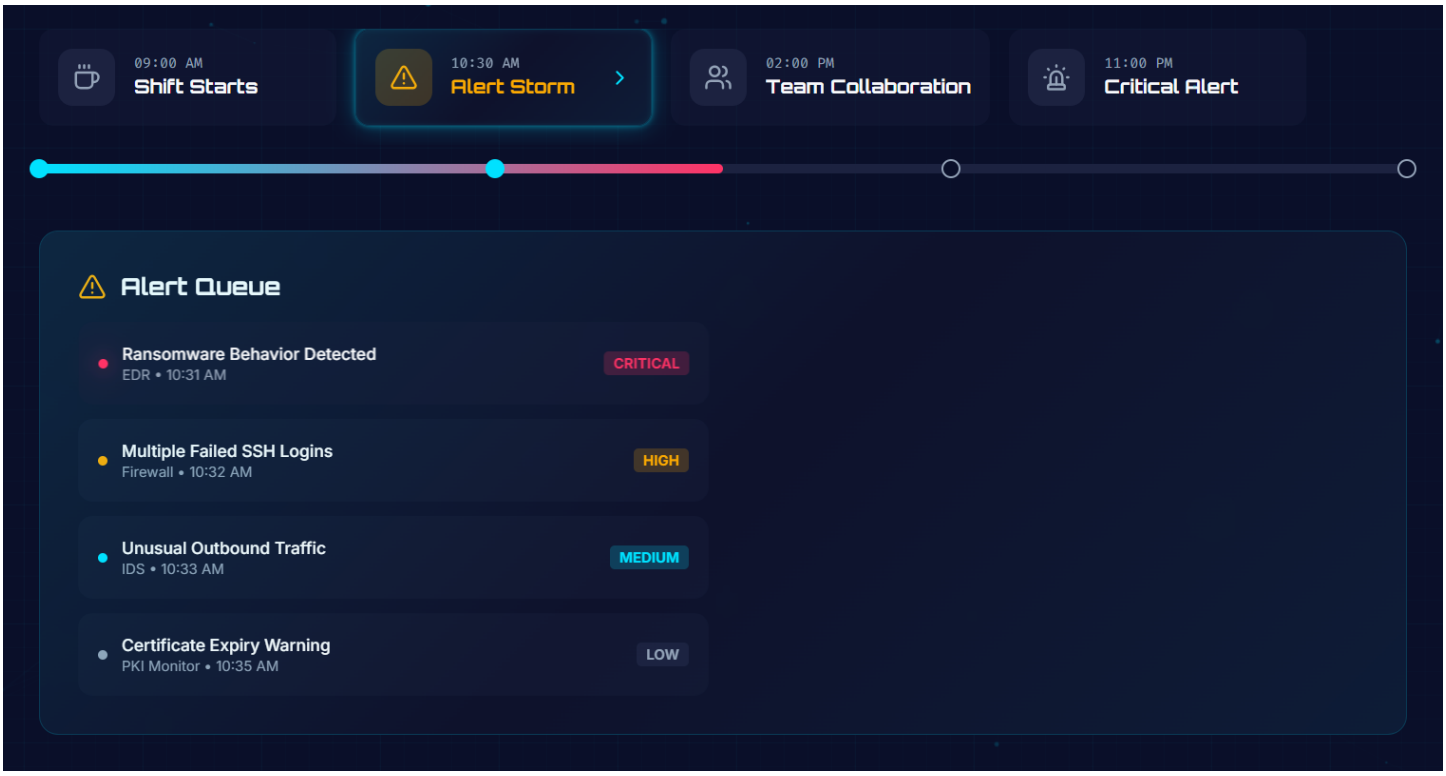


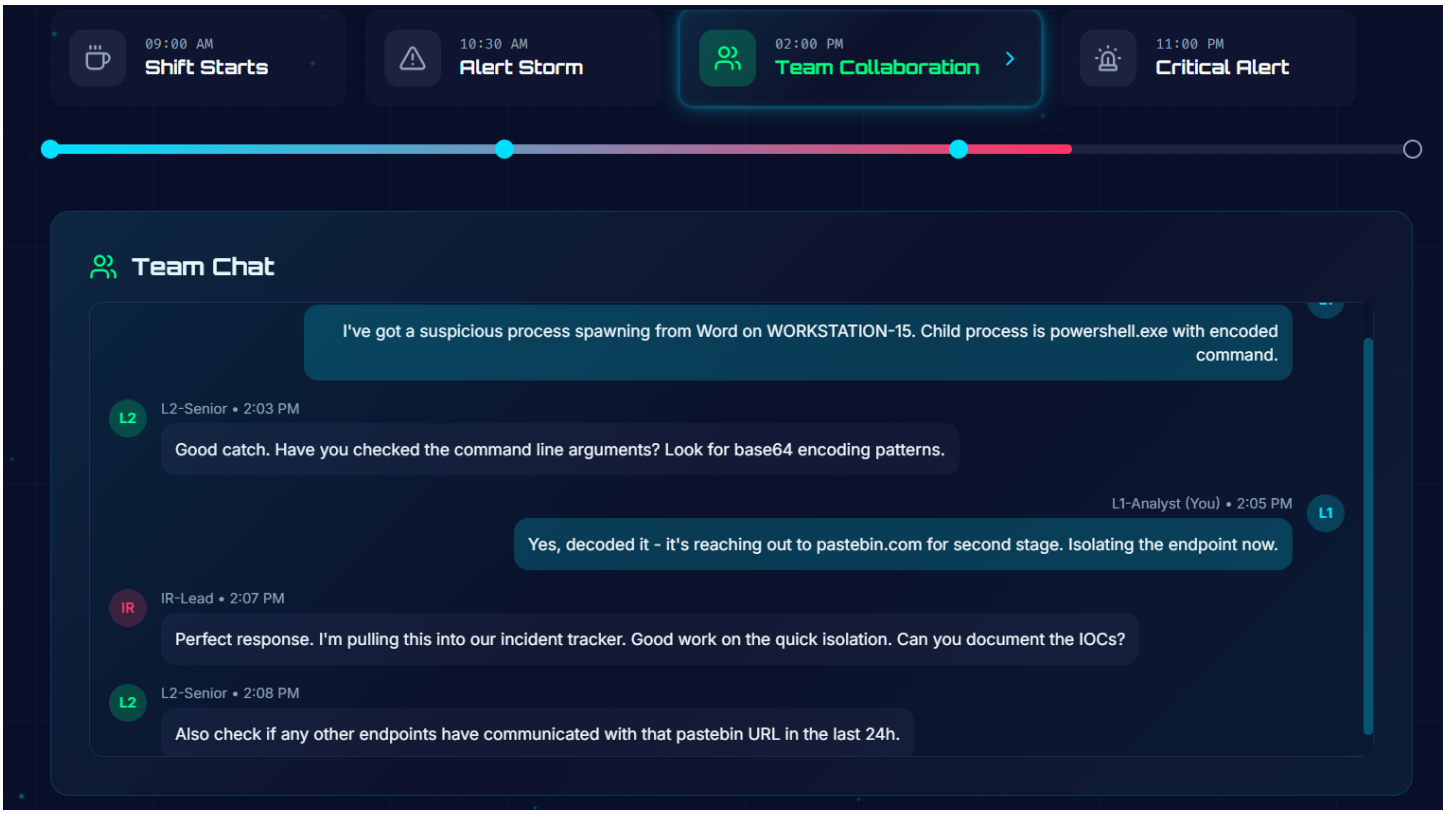
Daily Duties of SOC L1

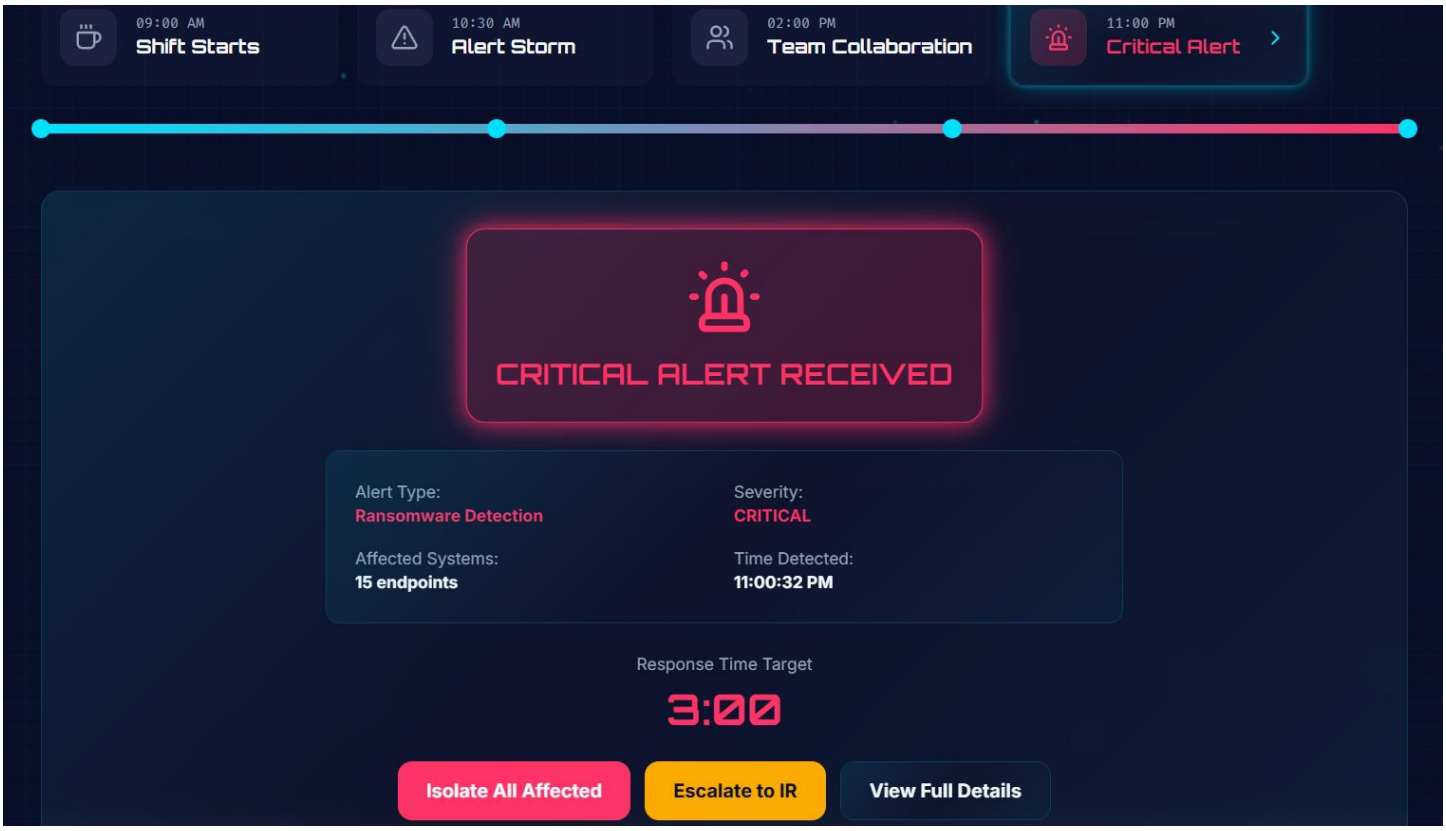
During work shift, SOC would typically:

- **Monitor and investigate various security alerts.**
  1. Primary responsibility is watching SIEM dashboards for security alerts. When an alert fires, you perform initial triage, is this a real threat or false positive? You gather context, check logs, and make the critical first decision.
  2. Analyze and document for each alert, you analyze relevant logs (windows event, firewall, proxy), identify indicators of compromise (IOCs), and document findings clearly. Your documentation helps L2/L3 analysts or incident responders take action.
  3. Escalate or Close based on your analysis, you decide: close as false positive, or escalate to L2/L3 for deeper requires solid understanding of attack patterns and organizational risk.
- Participates in SOC brainstorms and workshops
- Cooperate with other teams to keep your company safe
- Constantly learn and discover new attacks and defenses




09:00 AM
Shift Starts
10:30 AM
Alert Storm
02:00 PM
Team Collaboration
11:00 PM
Critical Alert
Alert Queue
Ransomware Behavior Detected
EDR • 10:31 AM
CRITICAL
Multiple Failed SSH Logins
Firewall • 10:32 AM
HIGH
Unusual Outbound Traffic
IDS • 10:33 AM
MEDIUM
Certificate Expiry Warning
PKI Monitor • 10:35 AM
LOW


09:00 AM
Shift Starts
10:30 AM
Alert Storm
02:00 PM
Team Collaboration
11:00 PM
Critical Alert
Team Chat
I've got a suspicious process spawning from Word on WORKSTATION-15. Child process is powershell.exe with encoded command.
L2
L2-Senior • 2:03 PM
Good catch. Have you checked the command line arguments? Look for base64 encoding patterns.
L1-Analyst (You) • 2:05 PM
L1
Yes, decoded it - it's reaching out to pastebin.com for second stage. Isolating the endpoint now.
IR
IR-Lead • 2:07 PM
Perfect response. I'm pulling this into our incident tracker. Good work on the quick isolation. Can you document the IOCs?
L2
L2-Senior • 2:08 PM
Also check if any other endpoints have communicated with that pastebin URL in the last 24h.

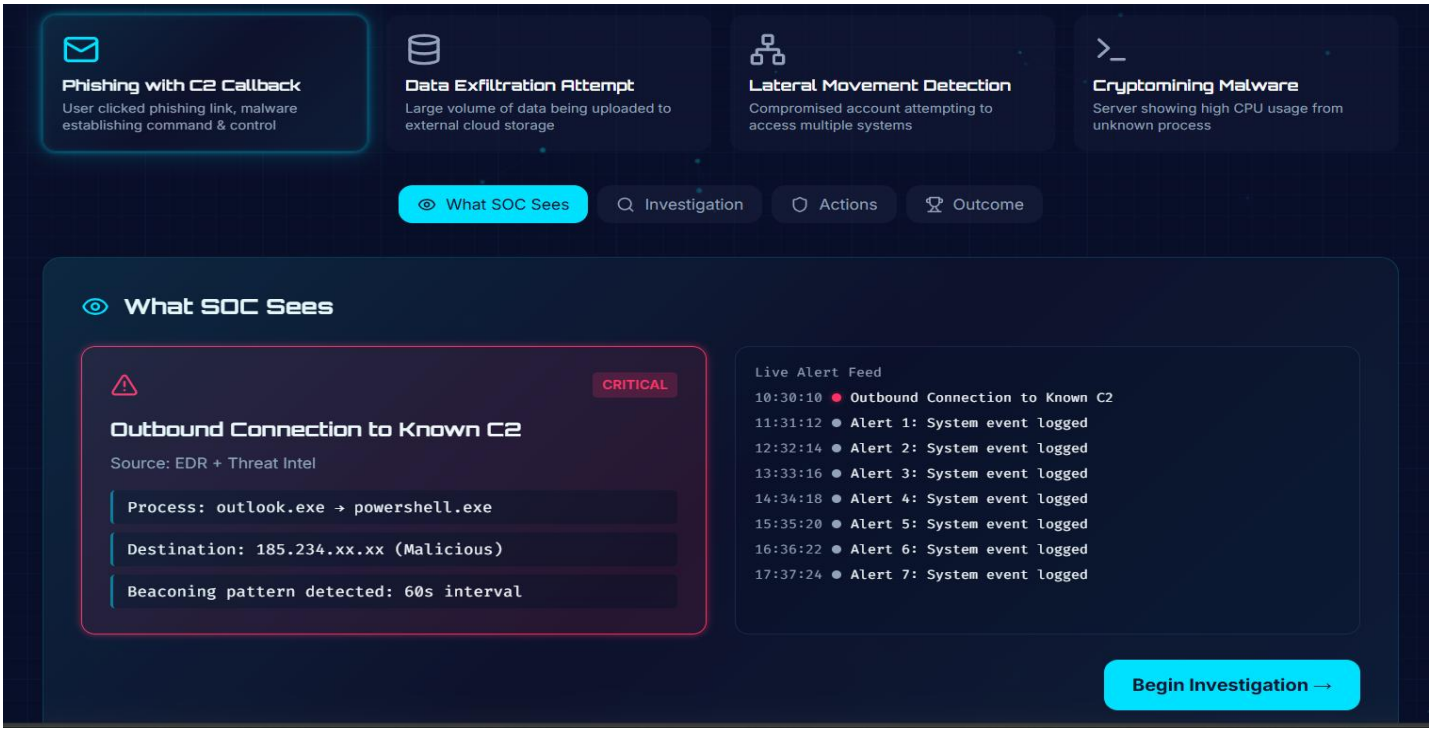


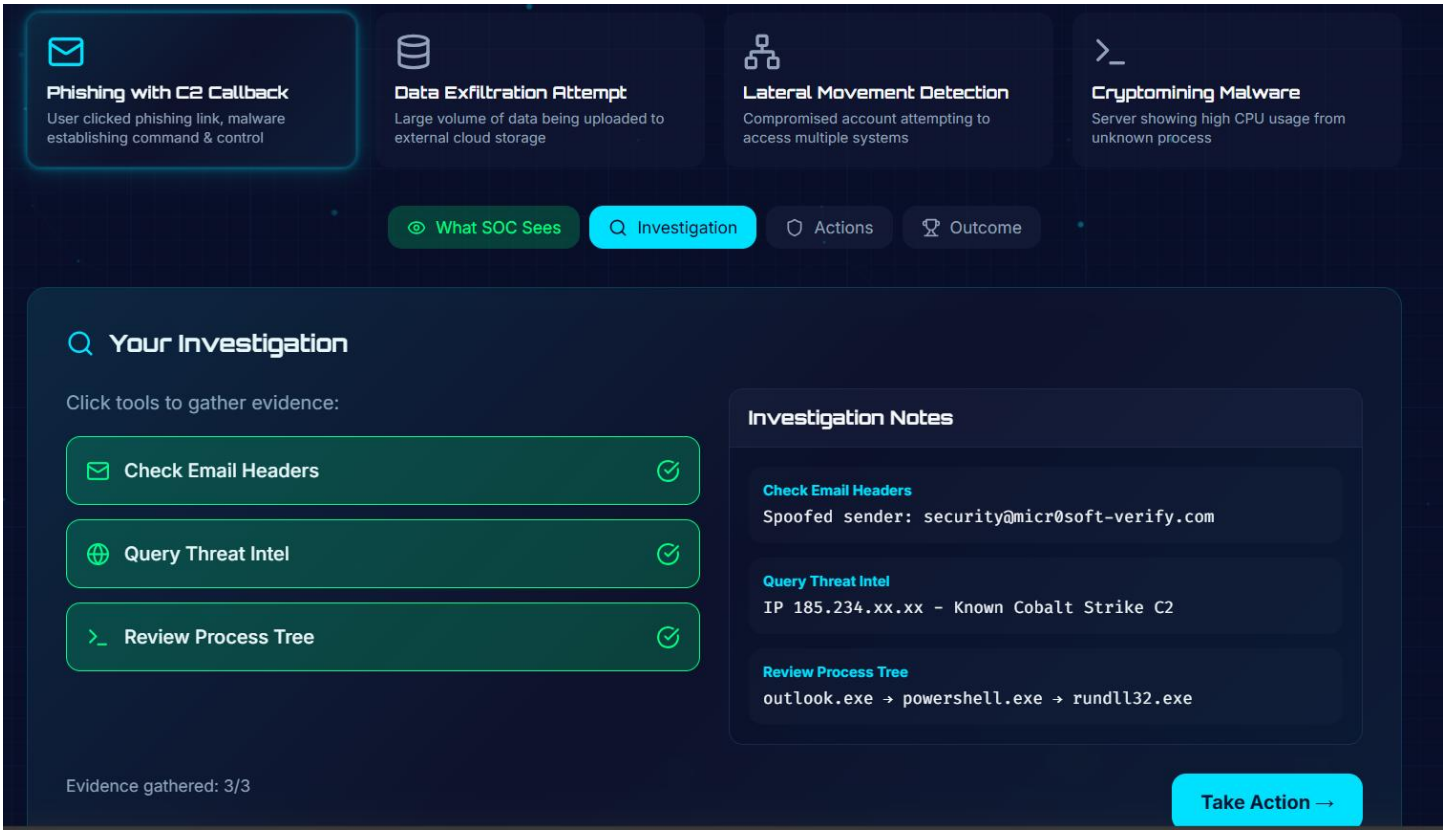
Attack scenarios from defenders' perspective

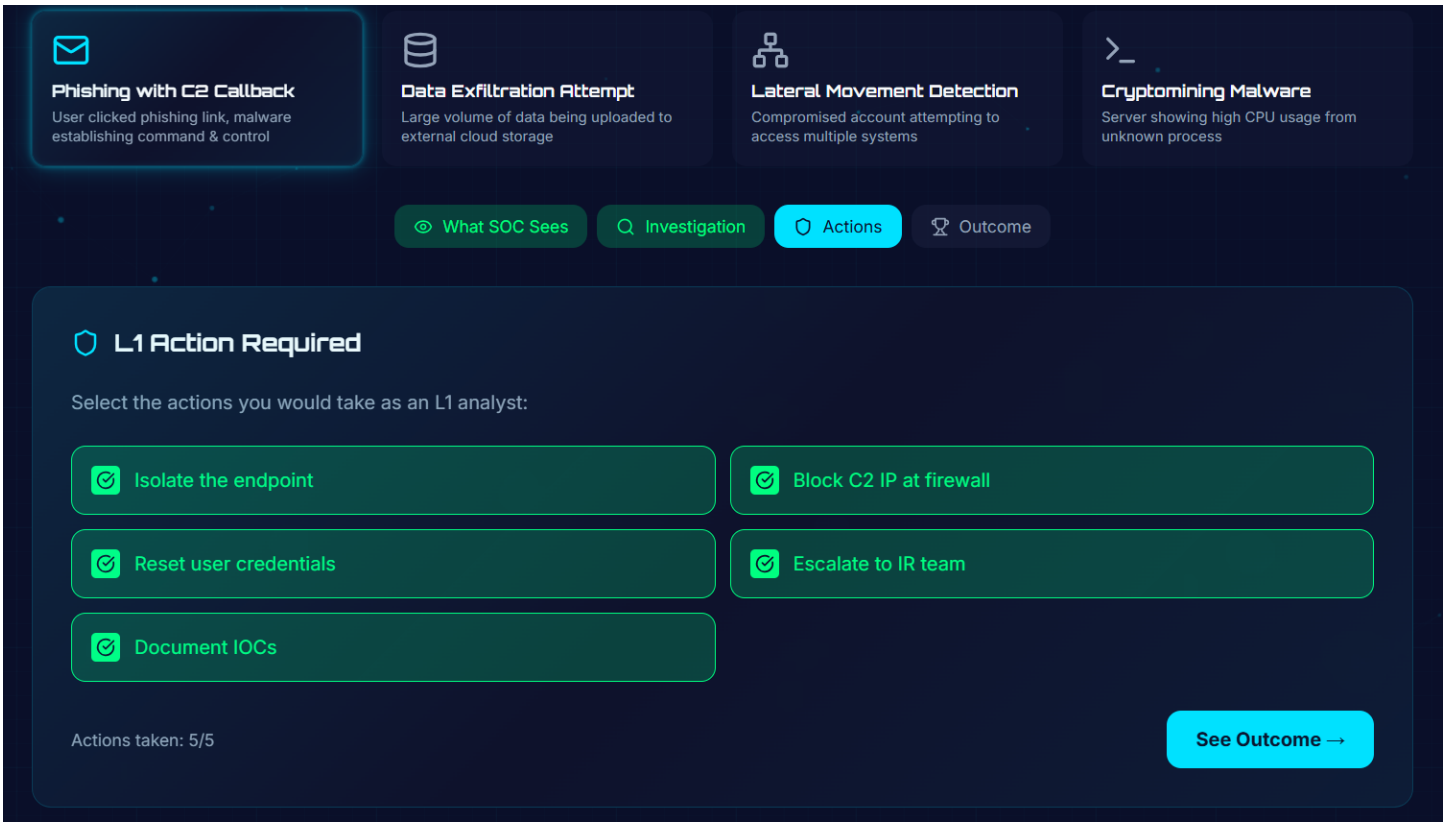
Phishing Attack

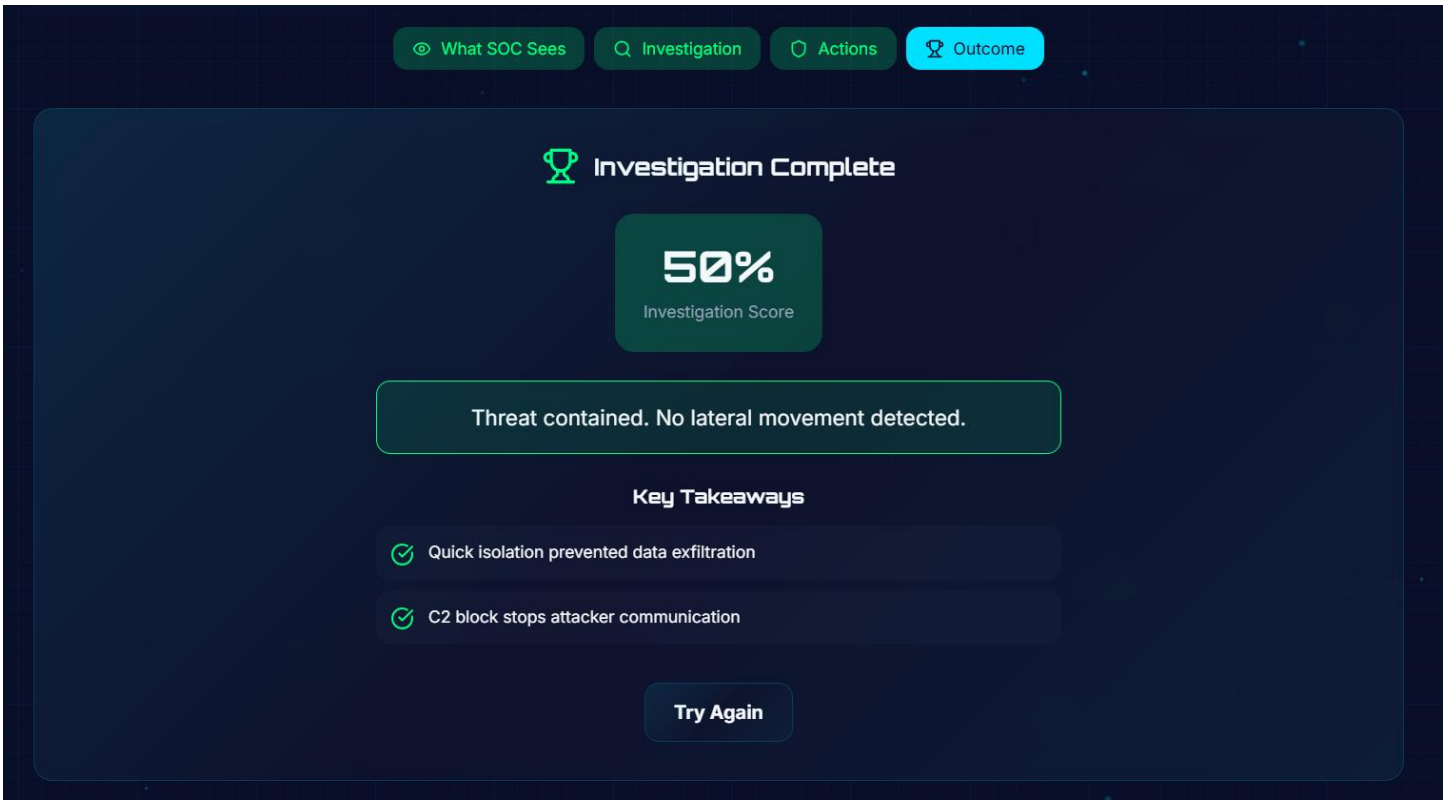
What SOC sees: Email gateway alerts, user clicking suspicious link, outbound connection to newly registered domain

L1 action: check email headers, verify domain reputation, isolates user endpoint if compromise suspected




Phishing with C2 Callback
User clicked phishing link, malware establishing command & control
Data Exfiltration Attempt
Large volume of data being uploaded to external cloud storage
Lateral Movement Detection
Compromised account attempting to access multiple systems
Cryptomining Malware
Server showing high CPU usage from unknown process
What SOC Sees
Investigation
Actions
Outcome
Your Investigation
Click tools to gather evidence:
Check Email Headers
Query Threat Intel
Review Process Tree
Investigation Notes
Check Email Headers
Spoofed sender: security@micr0soft-verify.com
Query Threat Intel
IP 185.234.xx.xx - Known Cobalt Strike C2
Review Process Tree
outlook.exe → powershell.exe → rundll32.exe
Evidence gathered: 3/3
Take Action →

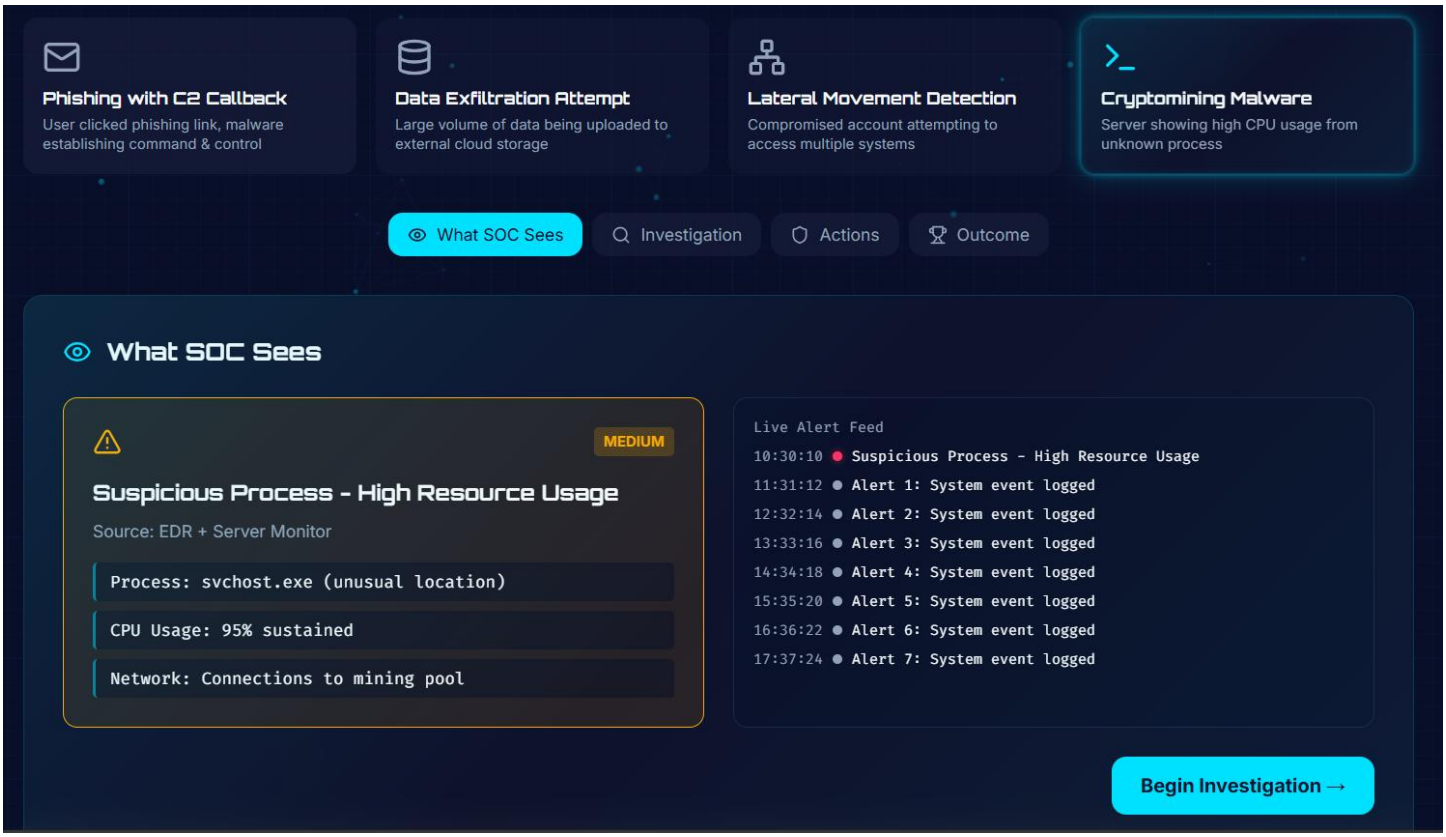

Phishing with C2 Callback
User clicked phishing link, malware establishing command & control
Data Exfiltration Attempt
Large volume of data being uploaded to external cloud storage
Lateral Movement Detection
Compromised account attempting to access multiple systems
Cryptomining Malware
Server showing high CPU usage from unknown process
What SOC Sees
Investigation
Actions
Outcome
L1 Action Required
Select the actions you would take as an L1 analyst:
Isolate the endpoint
Block C2 IP at firewall
Reset user credentials
Escalate to IR team
Document IOCs
Actions taken: 5/5
See Outcome →

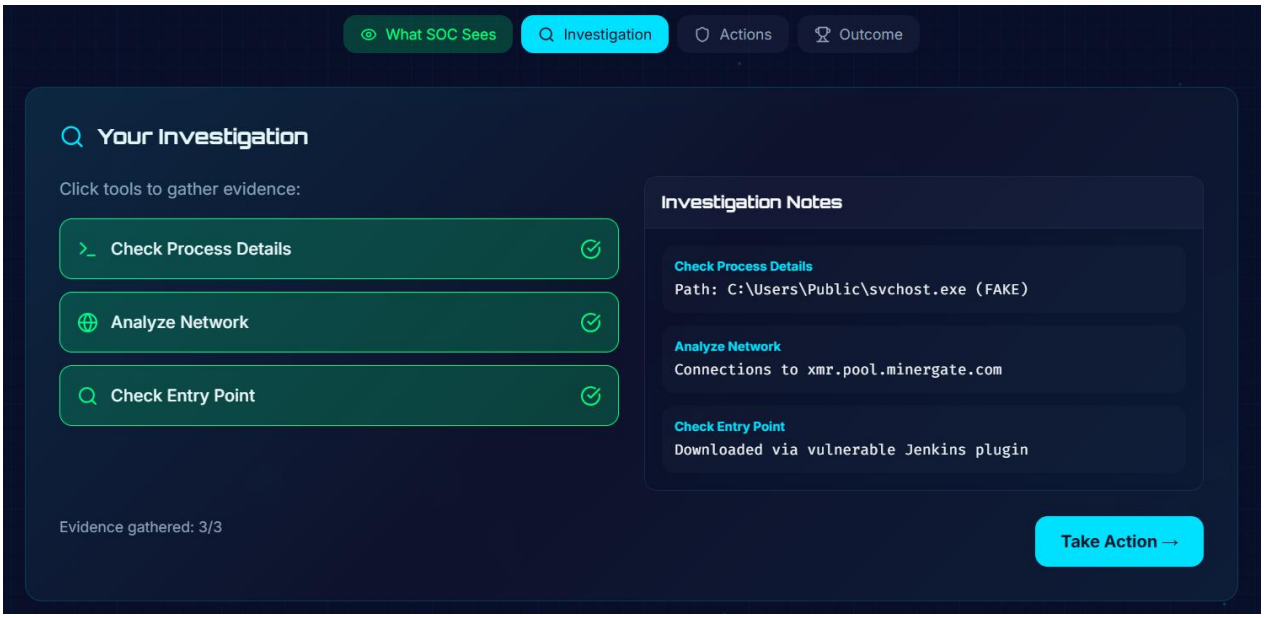


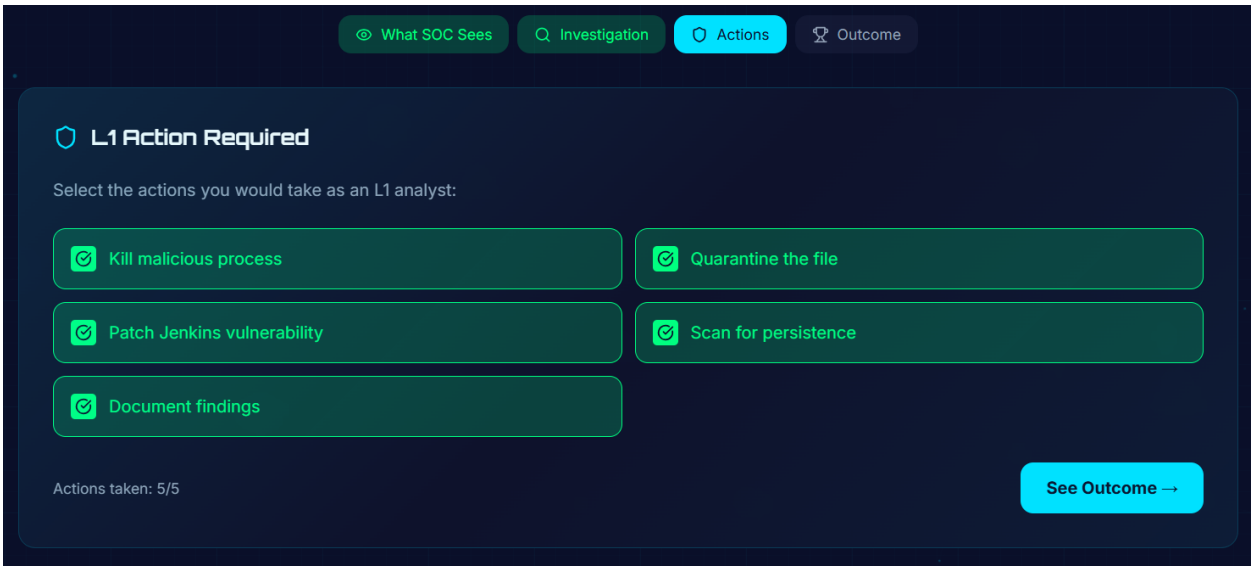
Malware execution

What SOC sees: EDR alert in suspicious process, unsigned executable, Outbound beacon to c2 server

L1 action: Quarantine file, check virus total hash, documents IOCs(indicators of compromises), escalate for forensics




What SOC Sees
Investigation
Actions
Outcome
Your Investigation
Click tools to gather evidence:
Check Process Details
Analyze Network
Check Entry Point
Investigation Notes
Check Process Details
Path: C:\Users\Public\svchost.exe (FAKE)
Analyze Network
Connections to xmr.pool.minergate.com
Check Entry Point
Downloaded via vulnerable Jenkins plugin
Evidence gathered: 3/3
Take Action →


What SOC Sees
Investigation
Actions
Outcome
L1 Action Required
Select the actions you would take as an L1 analyst:
Kill malicious process
Quarantine the file
Patch Jenkins vulnerability
Scan for persistence
Document findings
Actions taken: 5/5
See Outcome →


What SOC Sees
Investigation
Actions
Outcome
Investigation Complete
100%
Investigation Score
Cryptominer removed. Vulnerability patched.
Key Takeaways
Not ransomware, but still unauthorized access
Patch management prevents future exploitation
Try Again

Ransomware Attack

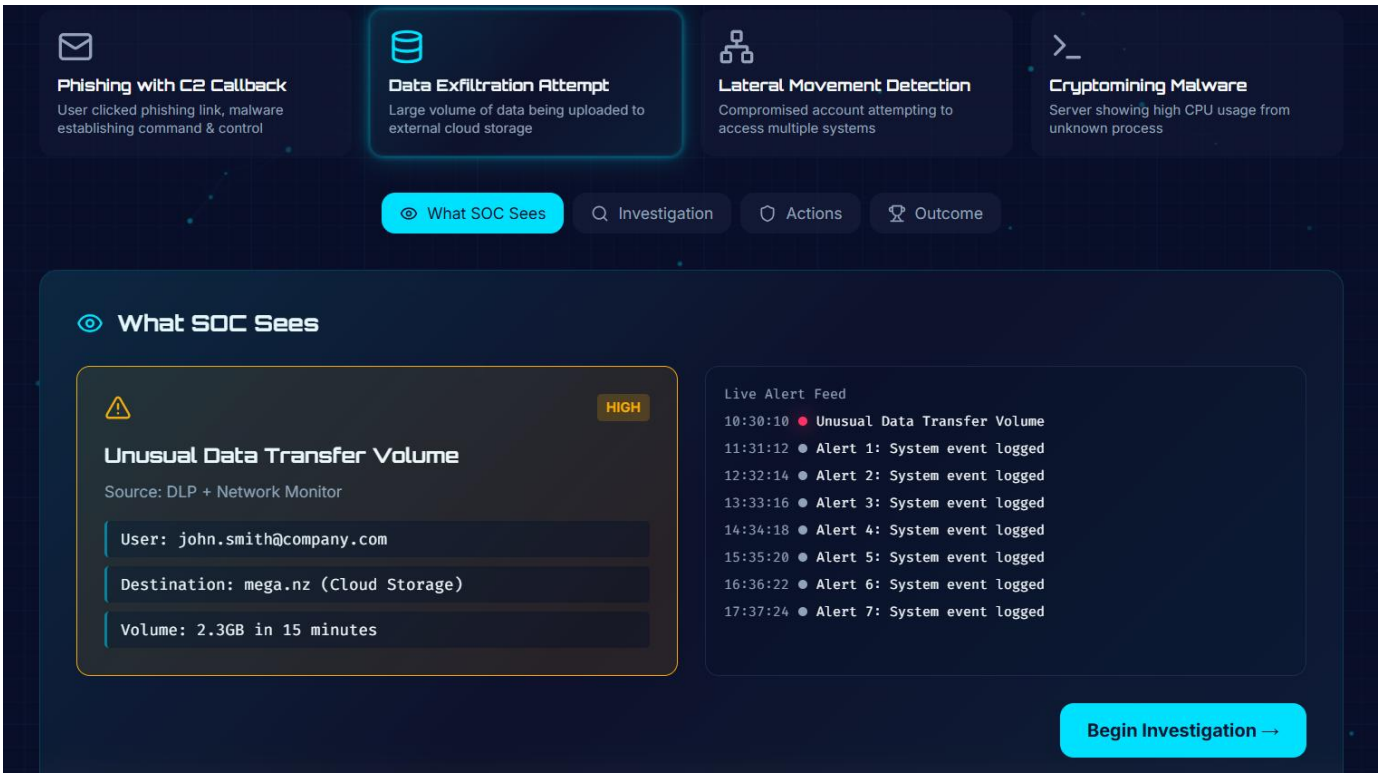
What SOC sees: Mass file encryption, ransom note creation, unusual disk activity, backup deletion attempts

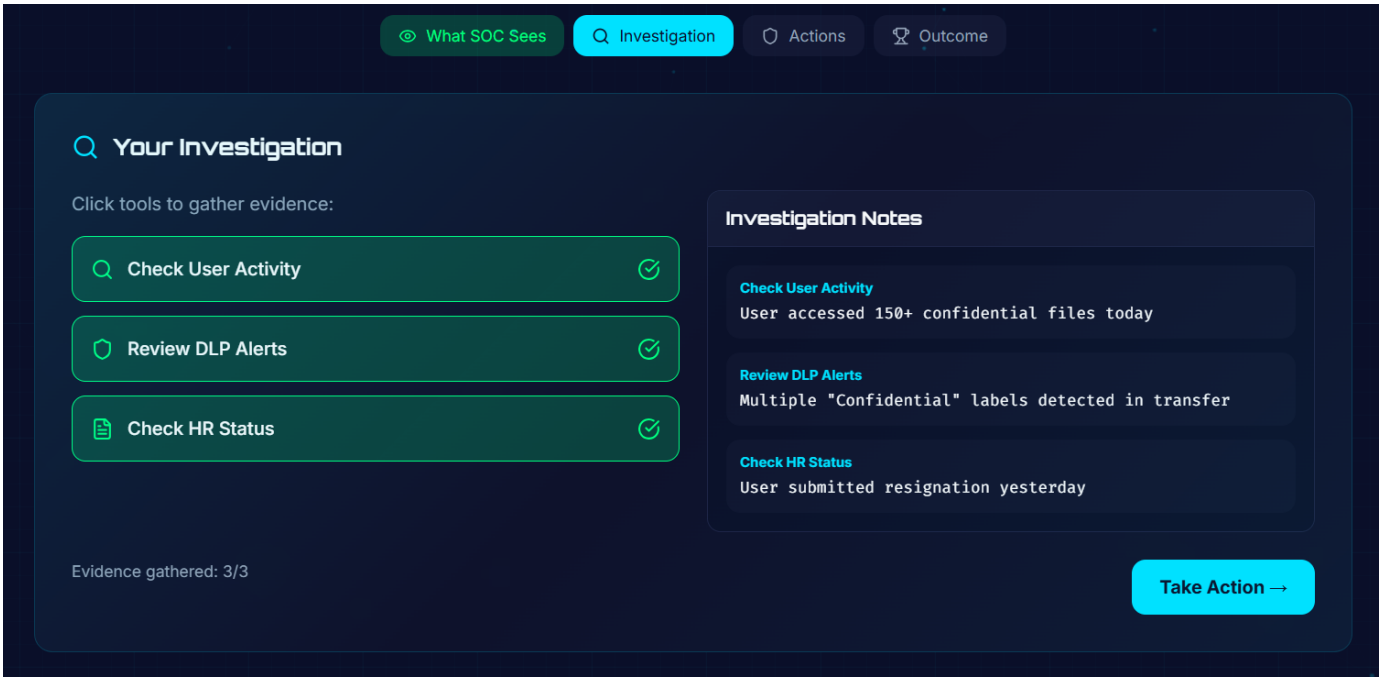
L1 action: Immediate escalation, time critical. Isolate affected systems, document timeline, notify IR team

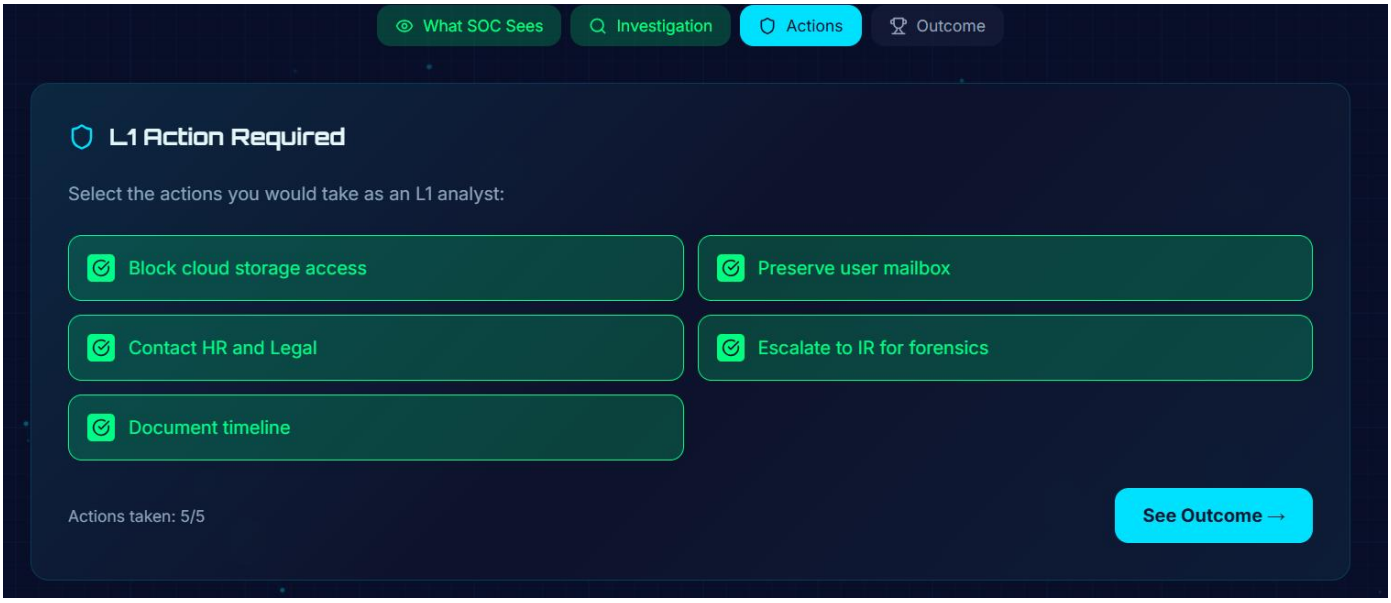
Brute Force

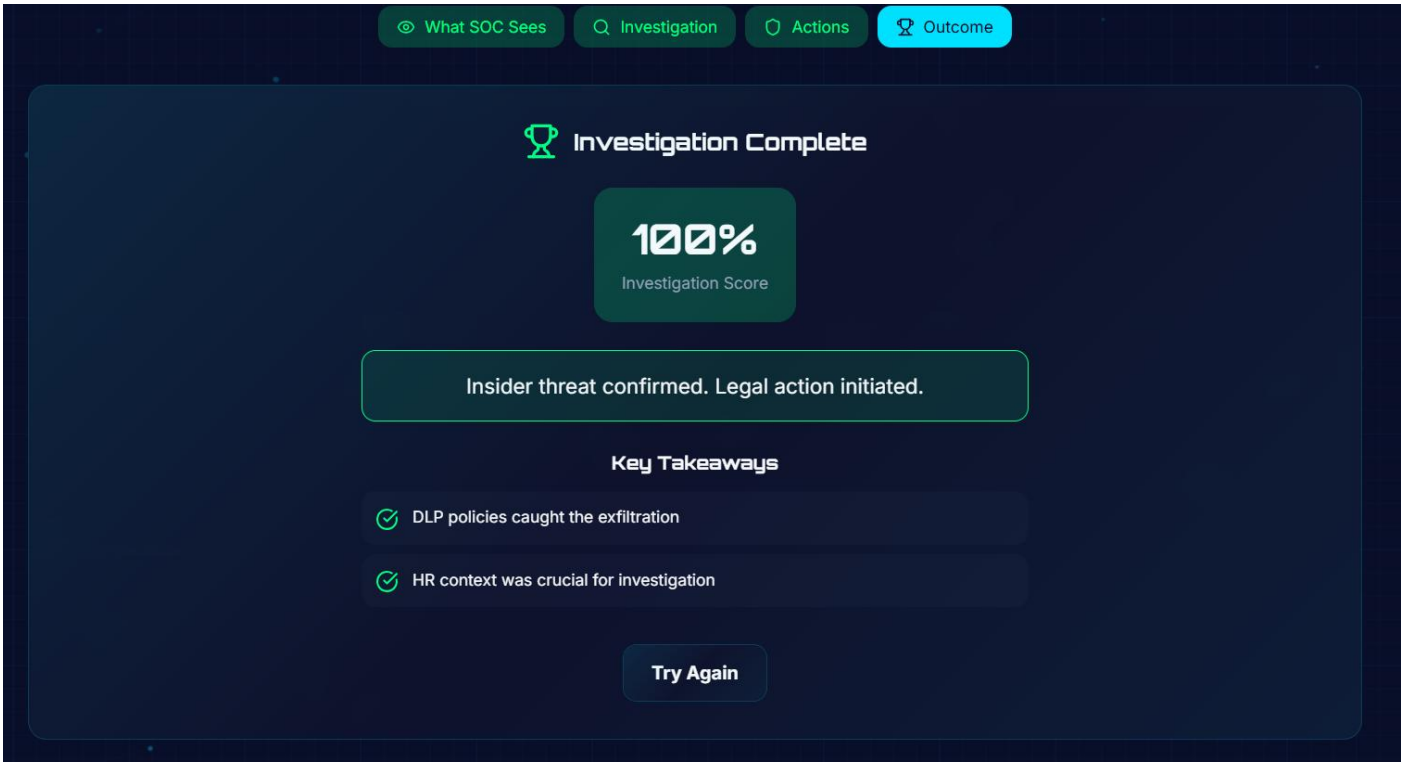
What SOC sees: Multiple failed login attempts (Event ID), account lockouts, login from unusual locations

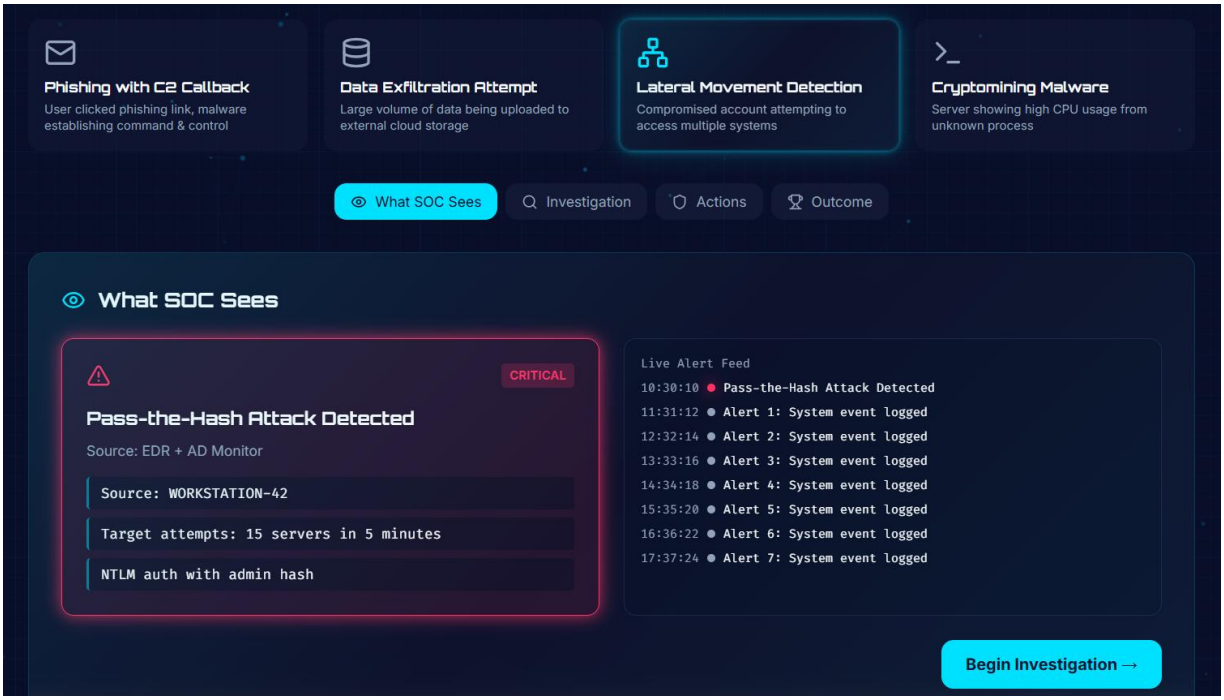
L1 action: verify legitimate user activity, block source IP address, check successful compromise, reset credentials if needed

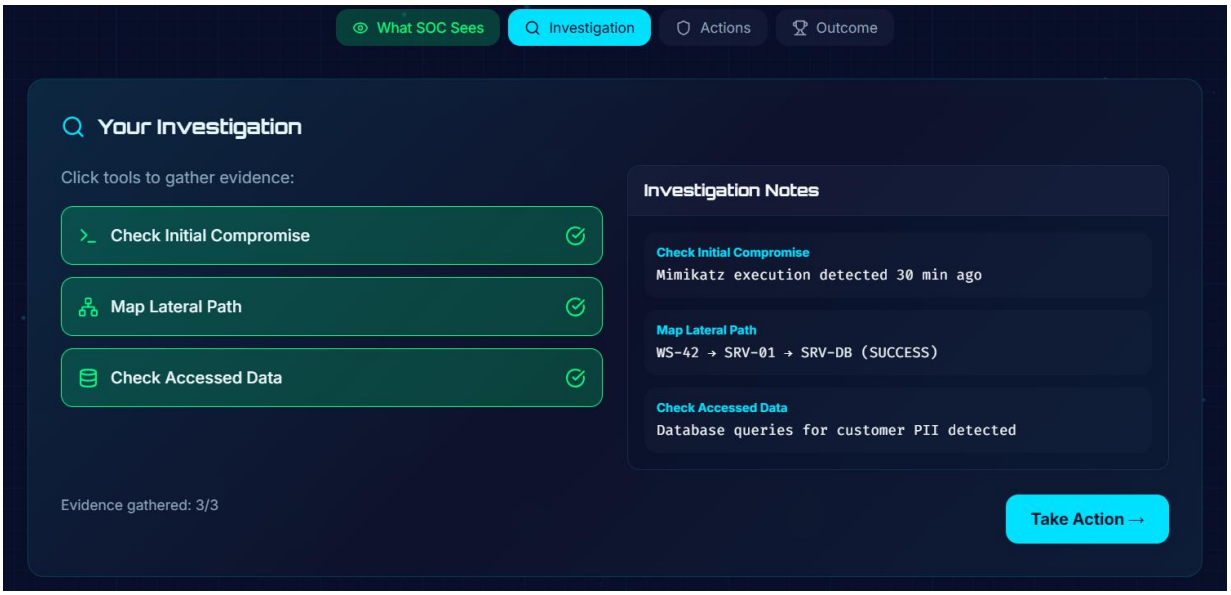


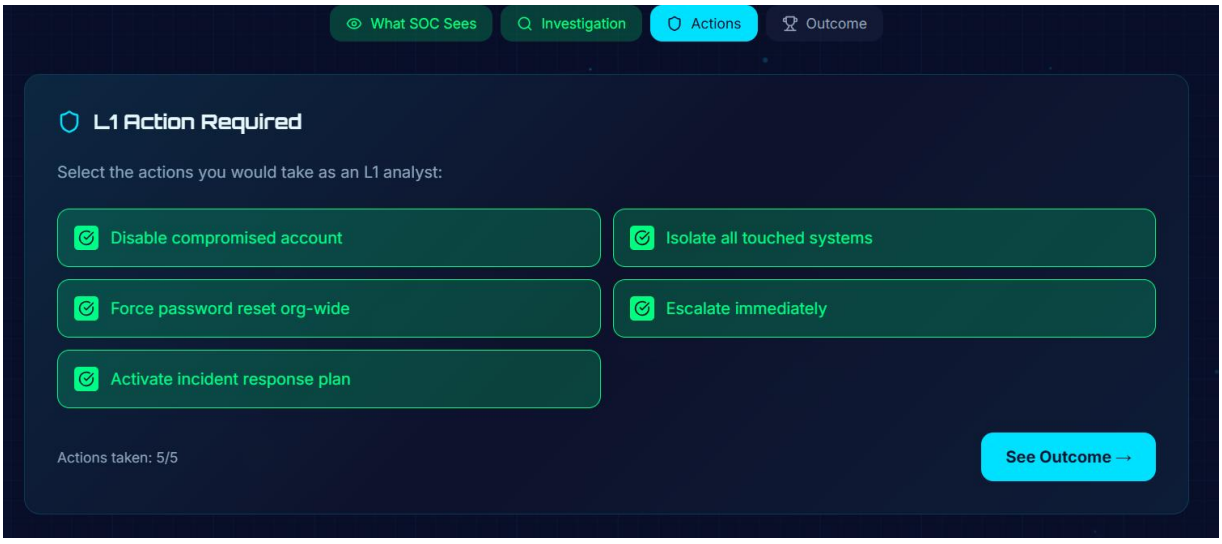


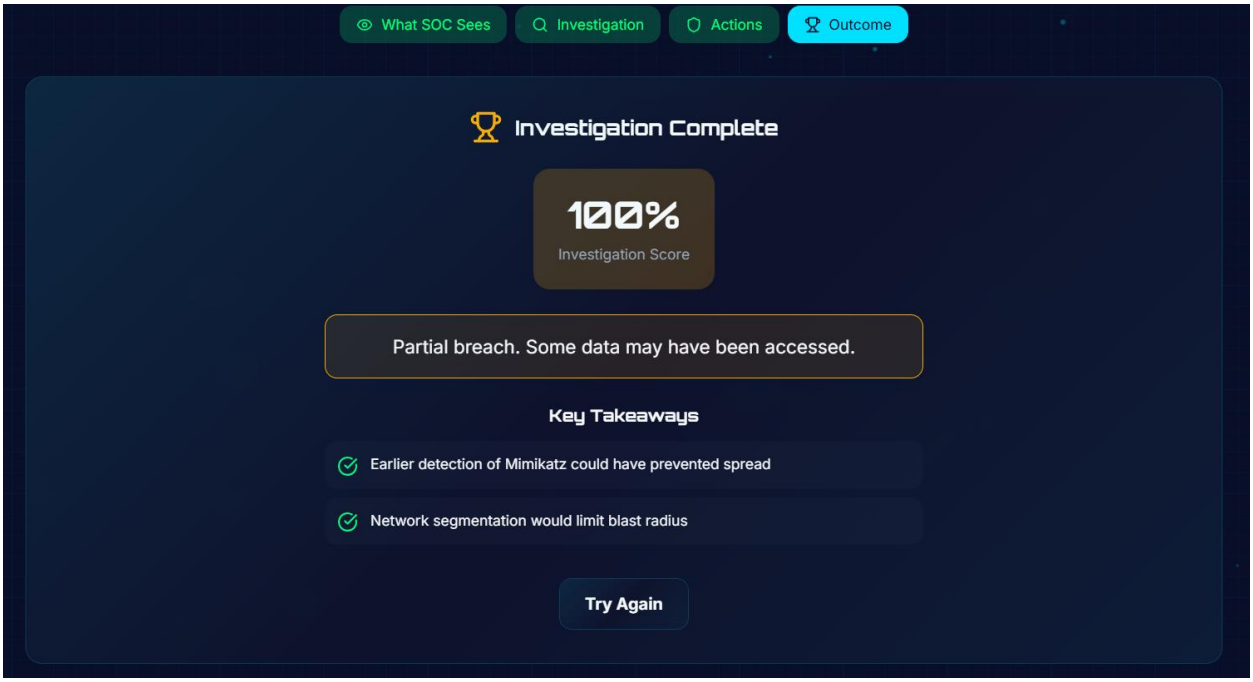

What SOC Sees
Investigation
Actions
Outcome
L1 Action Required
Select the actions you would take as an L1 analyst:
Block cloud storage access
Preserve user mailbox
Contact HR and Legal
Escalate to IR for forensics
Document timeline
Actions taken: 5/5
See Outcome →


What SOC Sees
Investigation
Actions
Outcome
Investigation Complete
100%
Investigation Score
Insider threat confirmed. Legal action initiated.
Key Takeaways
DLP policies caught the exfiltration
HR context was crucial for investigation
Try Again


Phishing with C2 Callback
User clicked phishing link, malware establishing command & control
Data Exfiltration Attempt
Large volume of data being uploaded to external cloud storage
Lateral Movement Detection
Compromised account attempting to access multiple systems
Cryptomining Malware
Server showing high CPU usage from unknown process
What SOC Sees
Investigation
Actions
Outcome
What SOC Sees
CRITICAL
Pass-the-Hash Attack Detected
Source: EDR + AD Monitor
Source: WORKSTATION-42
Target attempts: 15 servers in 5 minutes
NTLM auth with admin hash
Live Alert Feed
10:30:10 Pass-the-Hash Attack Detected
11:31:12 Alert 1: System event logged
12:32:14 Alert 2: System event logged
13:33:16 Alert 3: System event logged
14:34:18 Alert 4: System event logged
15:35:20 Alert 5: System event logged
16:36:22 Alert 6: System event logged
17:37:24 Alert 7: System event logged
Begin Investigation →


What SOC Sees
Investigation
Actions
Outcome
Your Investigation
Click tools to gather evidence:
Check Initial Compromise
Map Lateral Path
Check Accessed Data
Investigation Notes
Check Initial Compromise
Mimikatz execution detected 30 min ago
Map Lateral Path
WS-42 → SRV-01 → SRV-DB (SUCCESS)
Check Accessed Data
Database queries for customer PII detected
Evidence gathered: 3/3
Take Action →

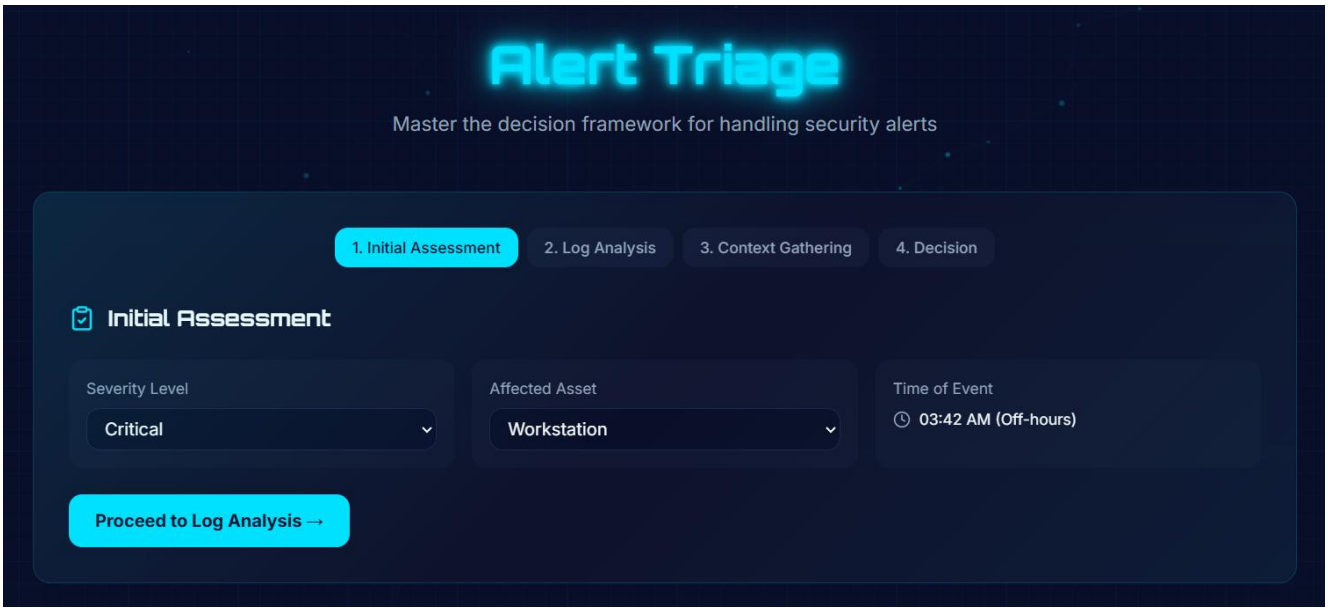

What SOC Sees
Investigation
Actions
Outcome
L1 Action Required
Select the actions you would take as an L1 analyst:
Disable compromised account
Isolate all touched systems
Force password reset org-wide
Escalate immediately
Activate incident response plan
Actions taken: 5/5
See Outcome →

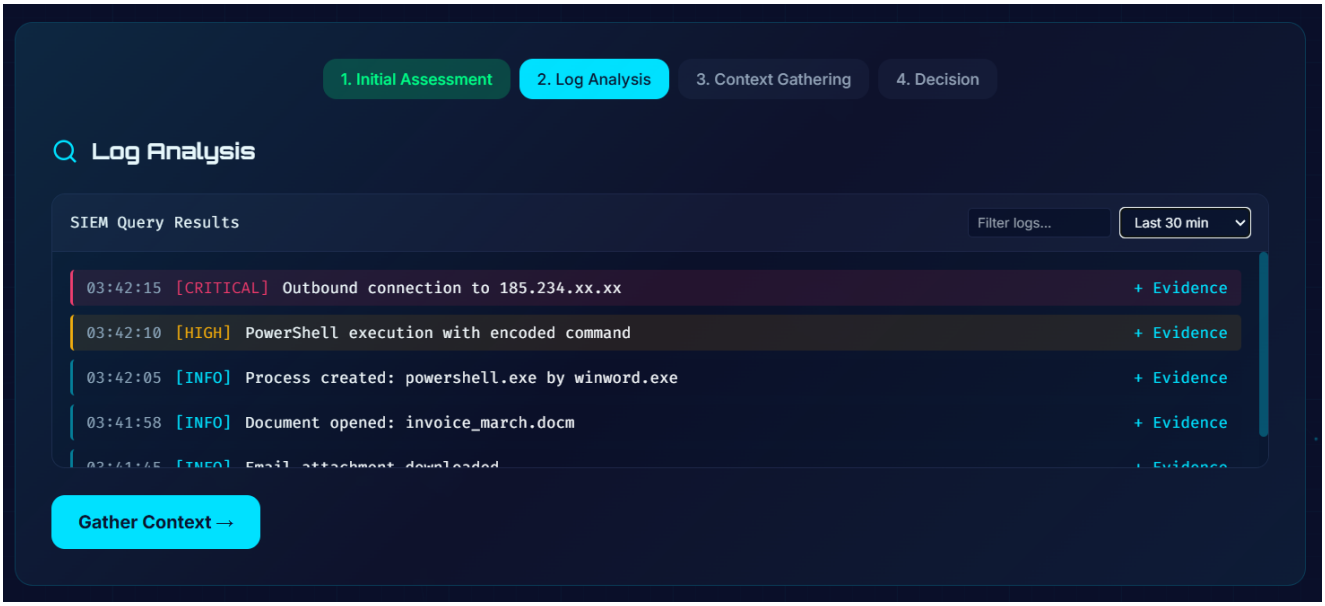


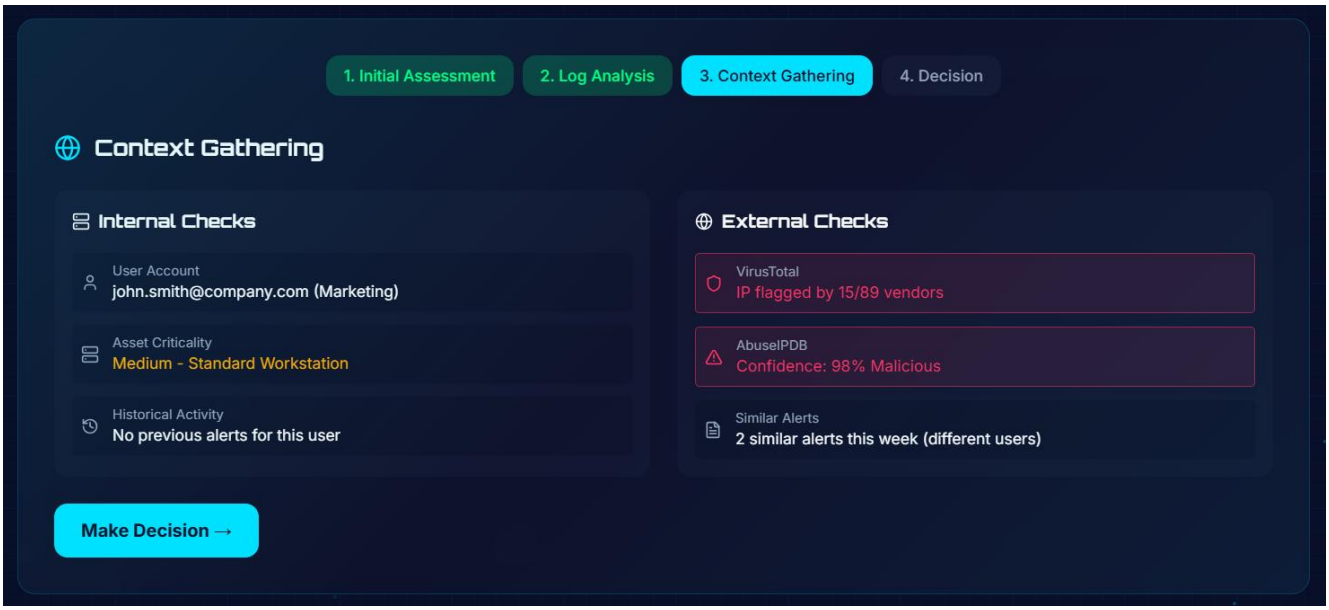
Alert Triage: Your Decision-making Framework

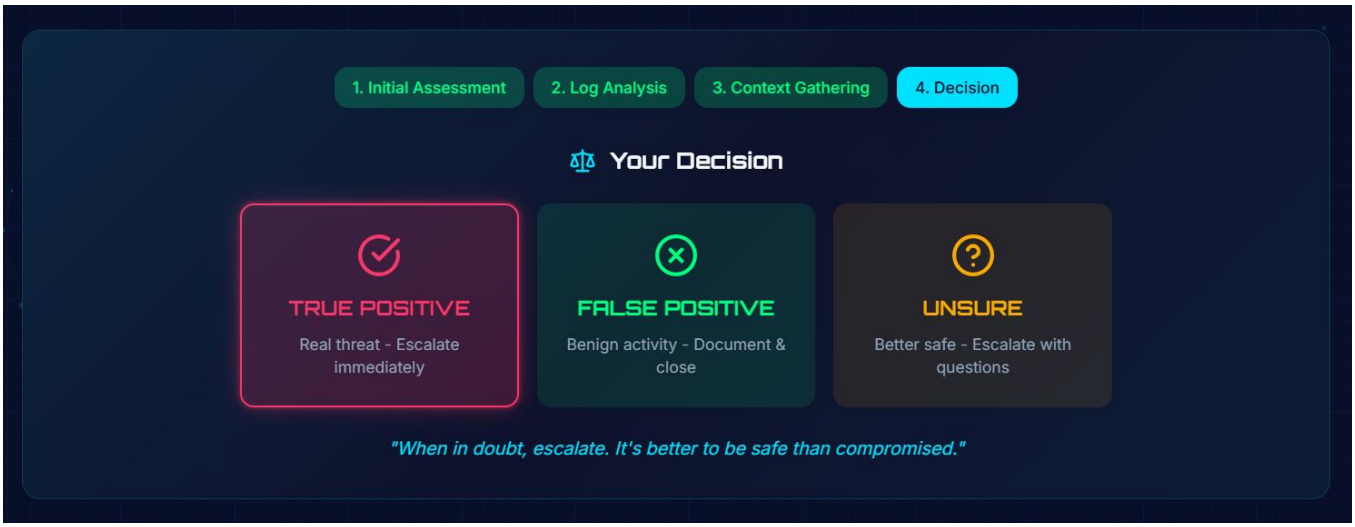
Every soc shift presents dozens or hundreds of alerts. Soc skills lies in rapidly determining which require escalation and which are false positives. This systemic approach ensures you never miss real threats whilst avoiding alert fatigue. Follow this framework for every single alert.

1. **Initial assessment**
   Read alert description, check severity rating, note affected asset. Quick context: Is this a critical server or user workstation? Business hour or 3AM?
2. **Log analysis**
   Query SIEM for related logs, check 30 minutes before and after alert look for: source IP, destination, user account, process details, frequency.
3. **Context Gathering**
   Is source IP internal or external? Is user account legitimate? Check threat intelligence, Known malicious domain/IP? Any similar alerts recently?
4. **Decision**
   True positive? Escalate with documentation. False positive? Close with clear justification. Unsure? Escalate, better safe than compromised.


Alert Triage
Master the decision framework for handling security alerts
1. Initial Assessment
2. Log Analysis
3. Context Gathering
4. Decision
Initial Assessment
Severity Level
Critical
Affected Asset
Workstation
Time of Event
03:42 AM (Off-hours)
Proceed to Log Analysis →


1. Initial Assessment
2. Log Analysis
3. Context Gathering
4. Decision
Log Analysis
SIEM Query Results
Filter logs...
Last 30 min
03:42:15 [CRITICAL] Outbound connection to 185.234.xx.xx + Evidence
03:42:10 [HIGH] PowerShell execution with encoded command + Evidence
03:42:05 [INFO] Process created: powershell.exe by winword.exe + Evidence
03:41:58 [INFO] Document opened: invoice_march.docm + Evidence
Gather Context →


1. Initial Assessment
2. Log Analysis
3. Context Gathering
4. Decision
Context Gathering
Internal Checks
User Account
john.smith@company.com (Marketing)
Asset Criticality
Medium - Standard Workstation
Historical Activity
No previous alerts for this user
External Checks
VirusTotal
IP flagged by 15/89 vendors
AbuseIPDB
Confidence: 98% Malicious
Similar Alerts
2 similar alerts this week (different users)
Make Decision →

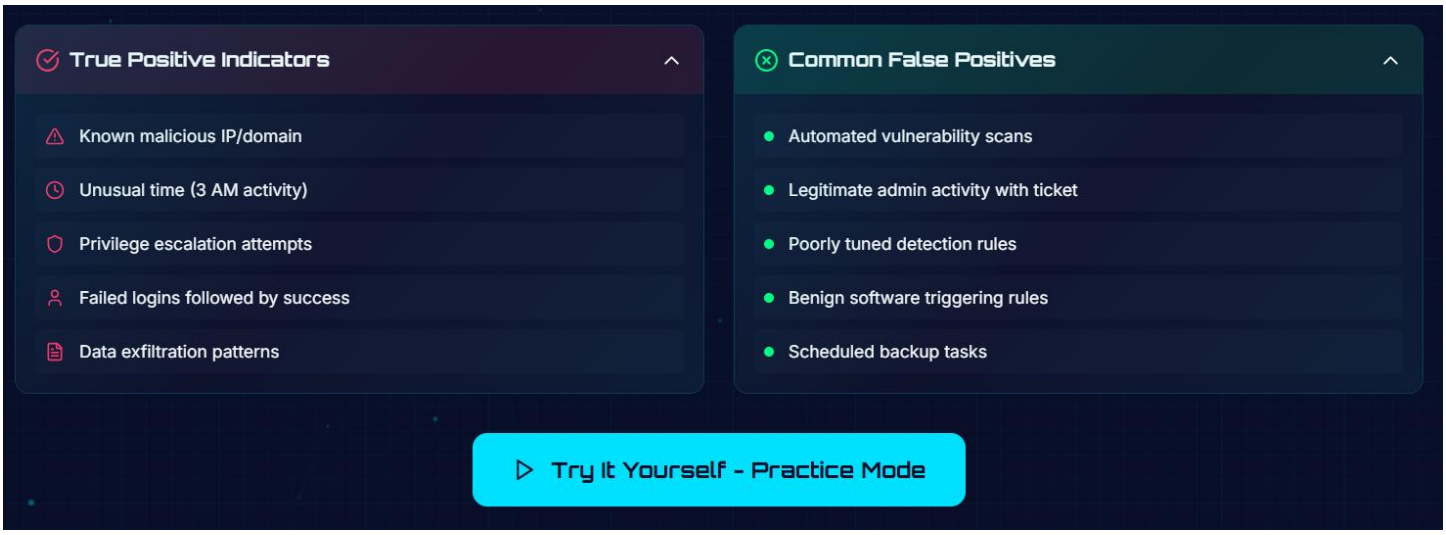


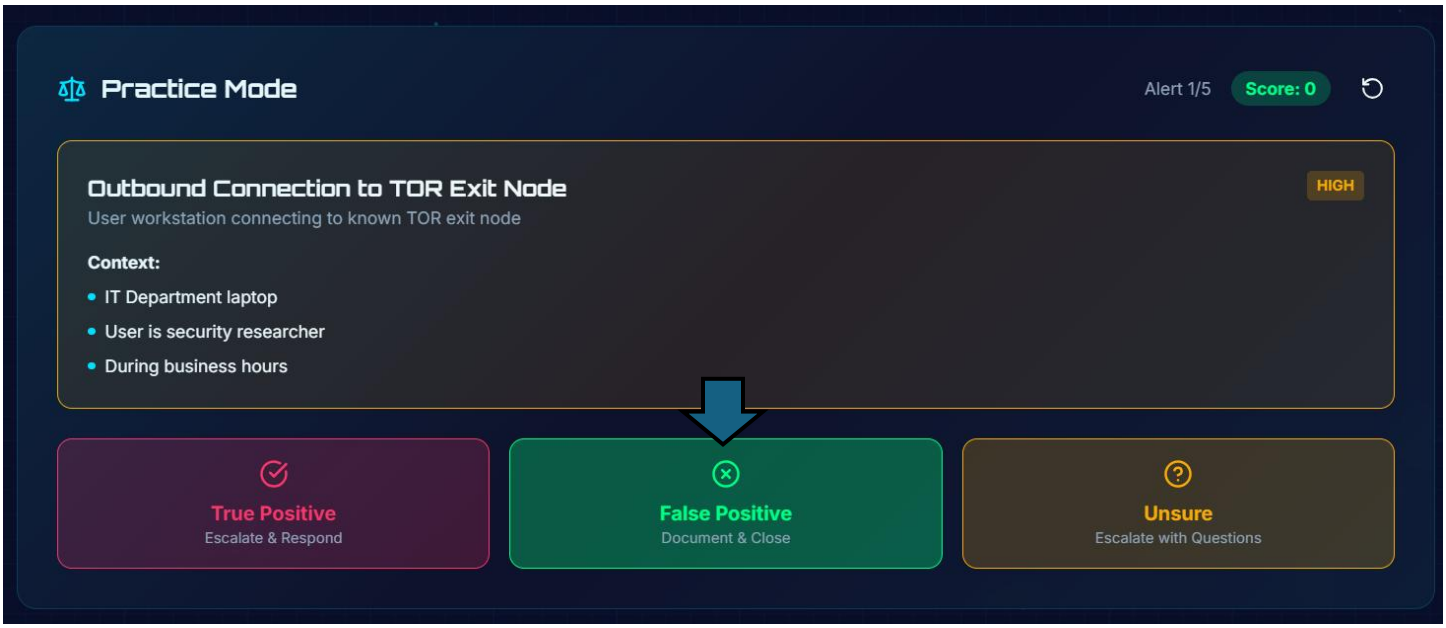
True positive Indicators

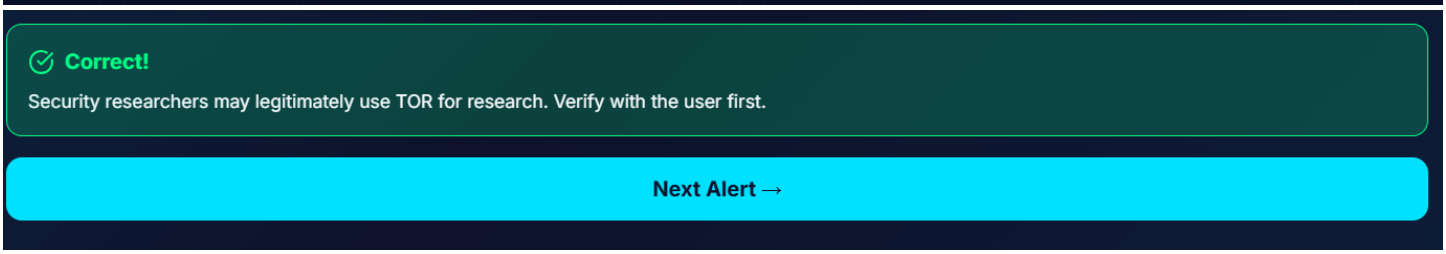
- Connection to known malicious IP/domain
- Unusual time of activity (3am access to finance data)
- Privilege escalation patterns (large uploads to cloud storage)
- Multiple failed logins followed by success

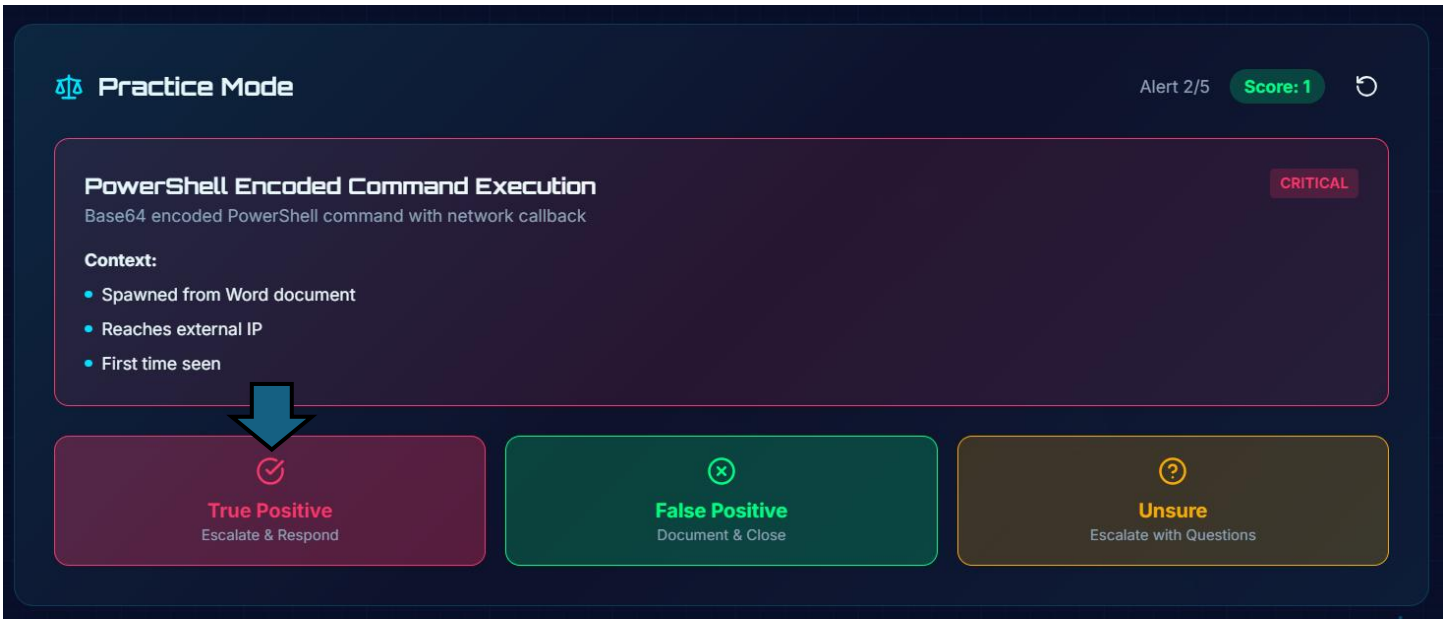
Common False Positives

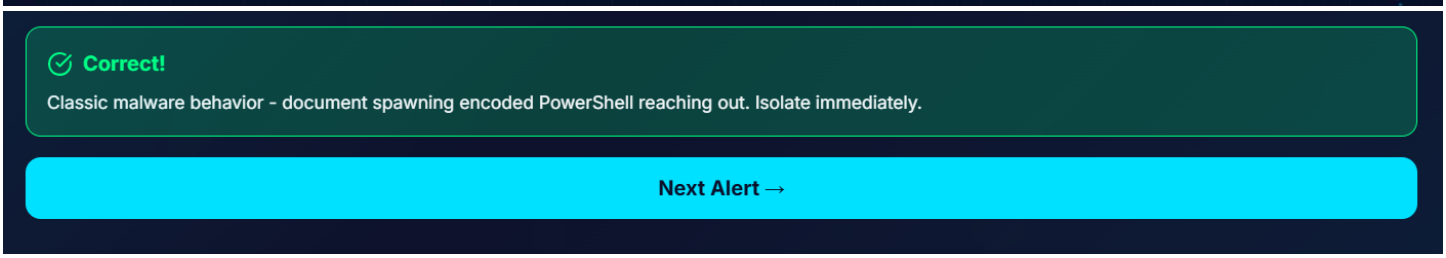
- Automated system scans triggering port scan alerts
- Legitimate admin activity flagged as suspicious
- Poorly tuned SIEM rules with how thresholds
- Benign Software triggering EDR heuristics
- Scheduled tasks appearing unusual process

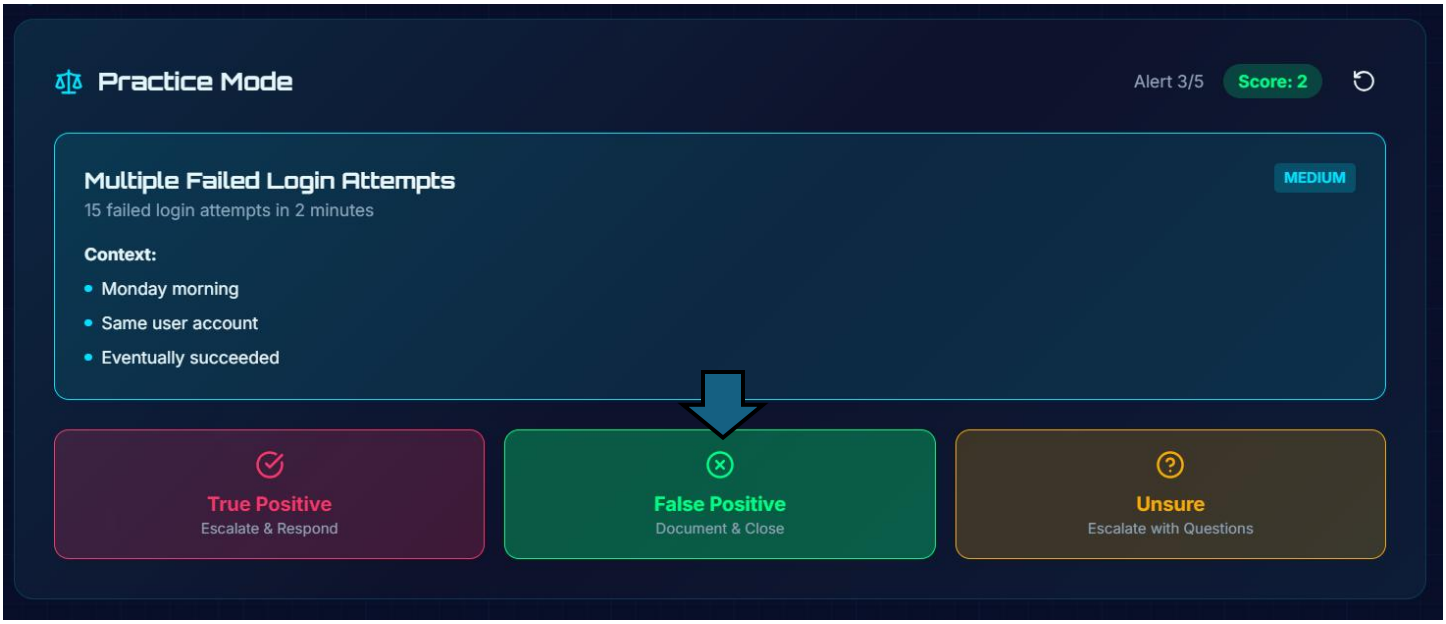


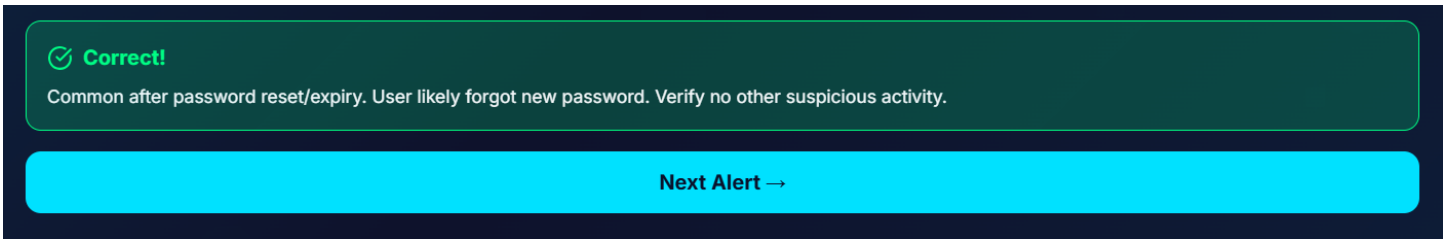

Practice Mode
Alert 1/5
Score: 0
Outbound Connection to TOR Exit Node
HIGH
User workstation connecting to known TOR exit node
Context:
IT Department laptop
User is security researcher
During business hours
True Positive
Escalate & Respond
False Positive
Document & Close
Unsure
Escalate with Questions

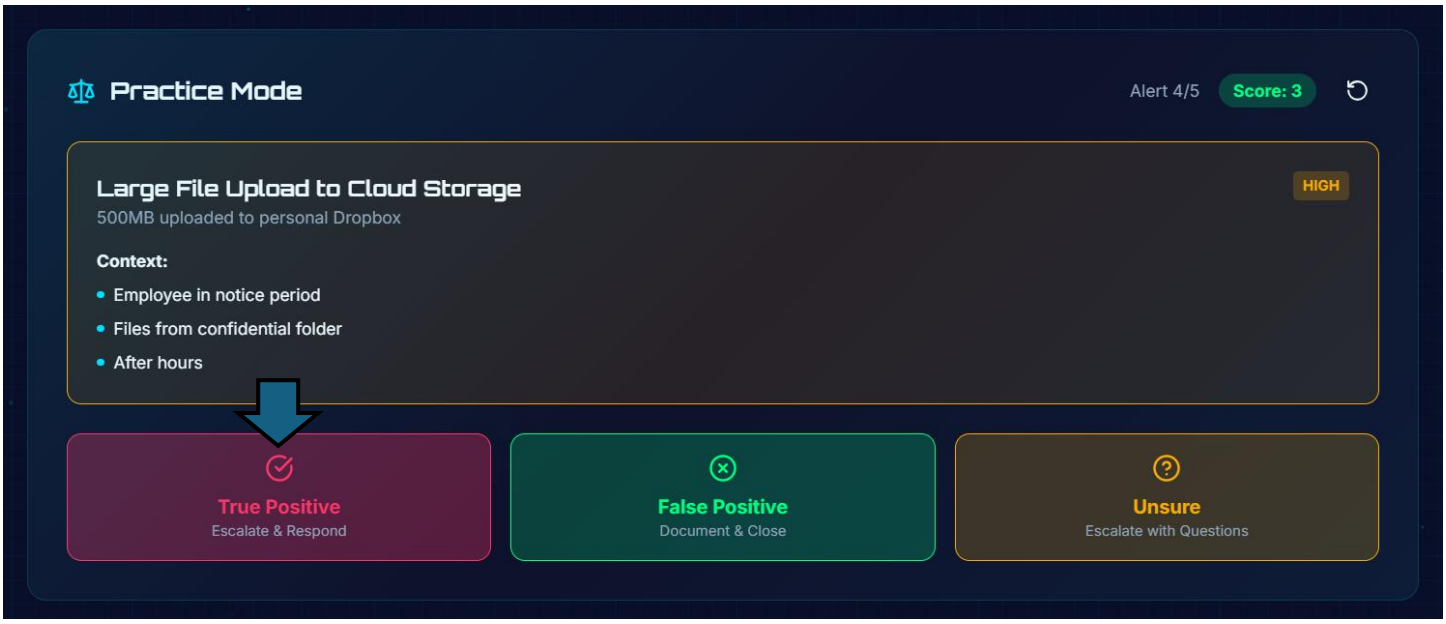

Correct!
Security researchers may legitimately use TOR for research. Verify with the user first.
Next Alert →

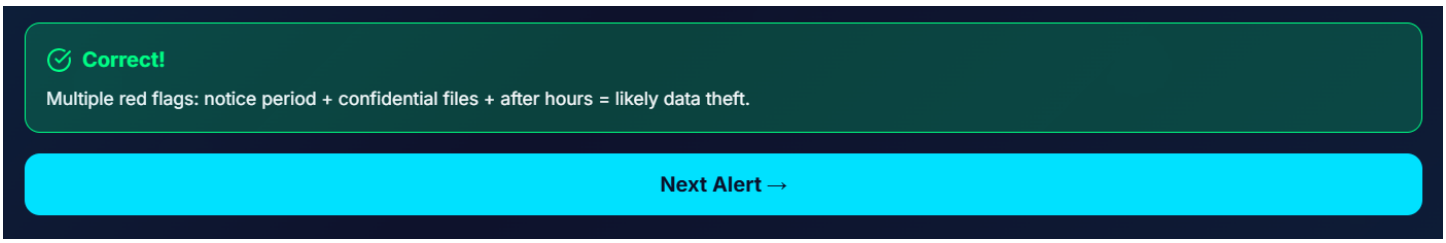

Practice Mode
Alert 2/5
Score: 1
PowerShell Encoded Command Execution
CRITICAL
Base64 encoded PowerShell command with network callback
Context:
Spawned from Word document
Reaches external IP
First time seen
True Positive
Escalate & Respond
False Positive
Document & Close
Unsure
Escalate with Questions

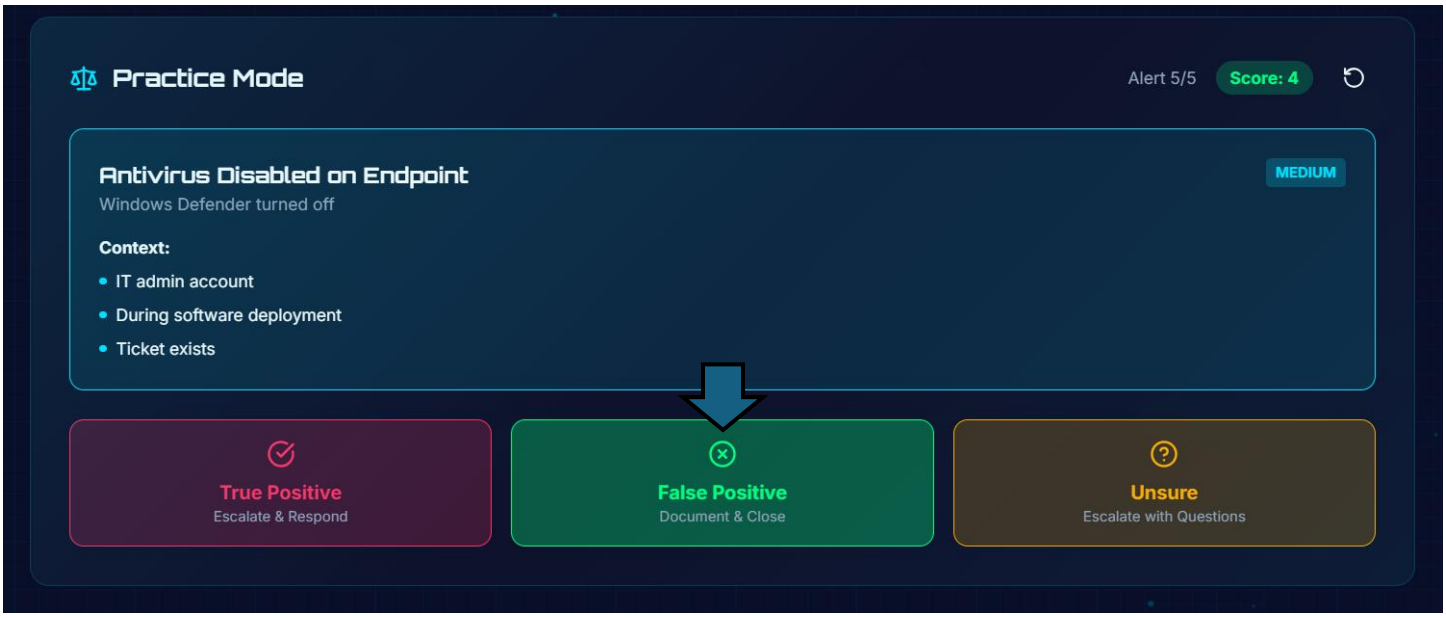

Correct!
Classic malware behavior - document spawning encoded PowerShell reaching out. Isolate immediately.
Next Alert →

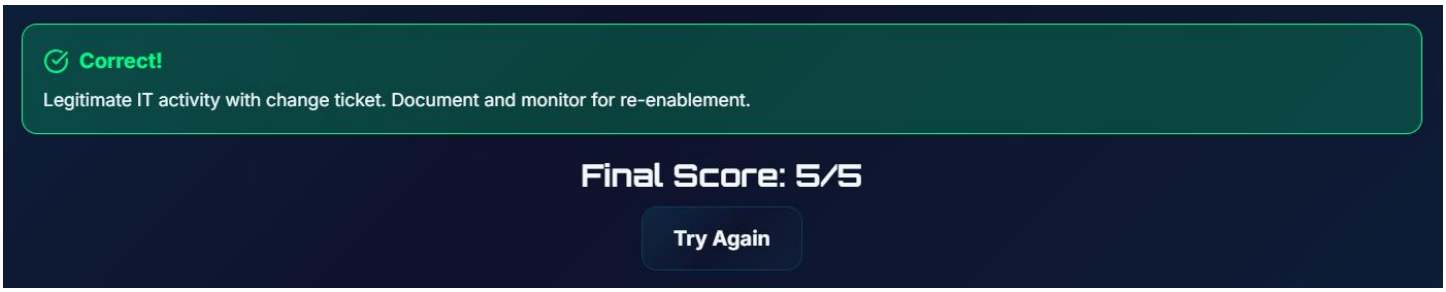

Practice Mode
Alert 3/5
Score: 2
Multiple Failed Login Attempts
MEDIUM
15 failed login attempts in 2 minutes
Context:
Monday morning
Same user account
Eventually succeeded
True Positive
Escalate & Respond
False Positive
Document & Close
Unsure
Escalate with Questions


Correct!
Common after password reset/expiry. User likely forgot new password. Verify no other suspicious activity.
Next Alert →


Practice Mode
Alert 4/5
Score: 3
Large File Upload to Cloud Storage
HIGH
500MB uploaded to personal Dropbox
Context:
Employee in notice period
Files from confidential folder
After hours
True Positive
Escalate & Respond
False Positive
Document & Close
Unsure
Escalate with Questions


Correct!
Multiple red flags: notice period + confidential files + after hours = likely data theft.
Next Alert →

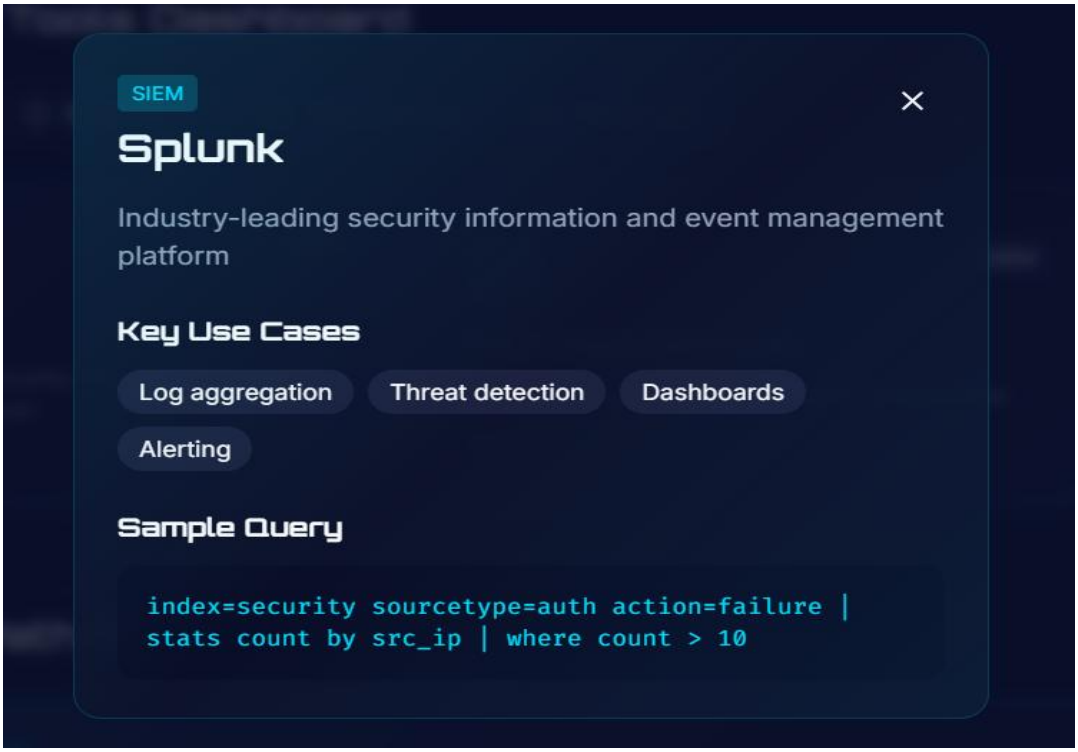


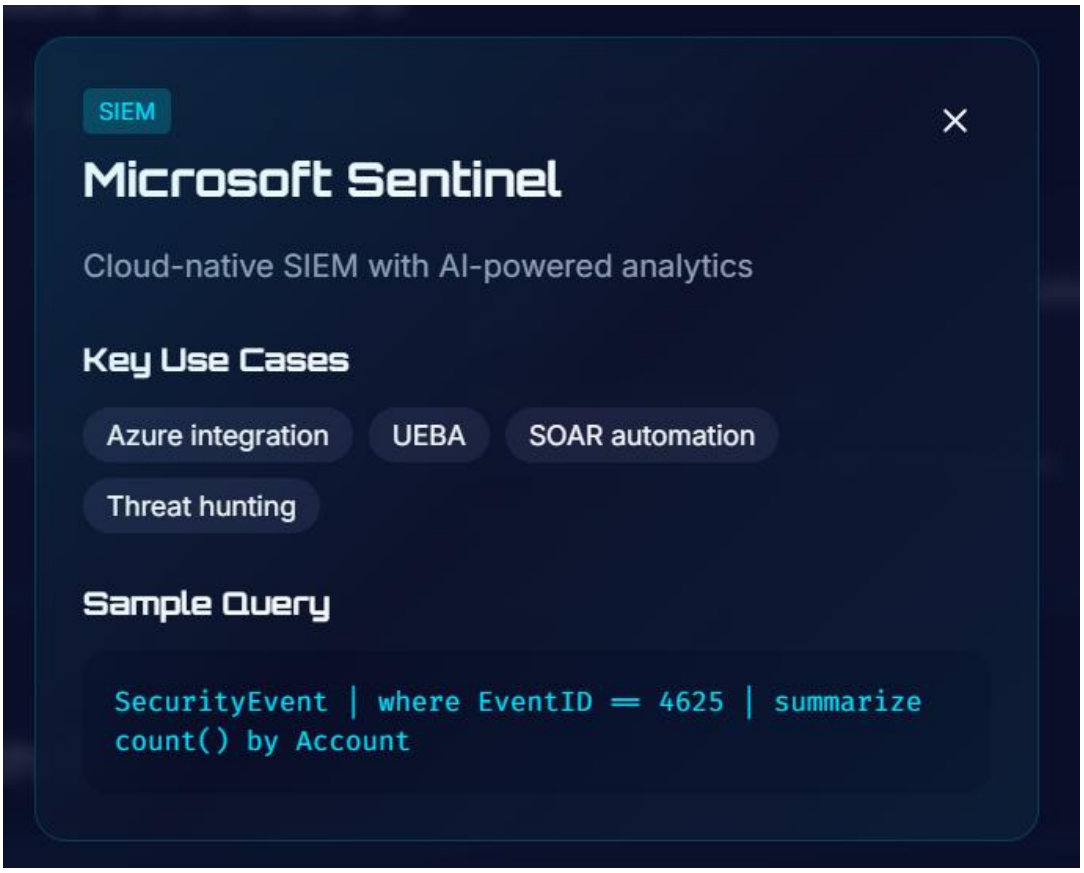


Essential Tools & Certifications

Tools

1. **SIEM**
   Splunk (most common), Microsoft Sentinel (Azure), IBM QRadar. Learn one deeply, Concepts transfer between platforms. Focus on: creating queries, building dashboards, correlating events

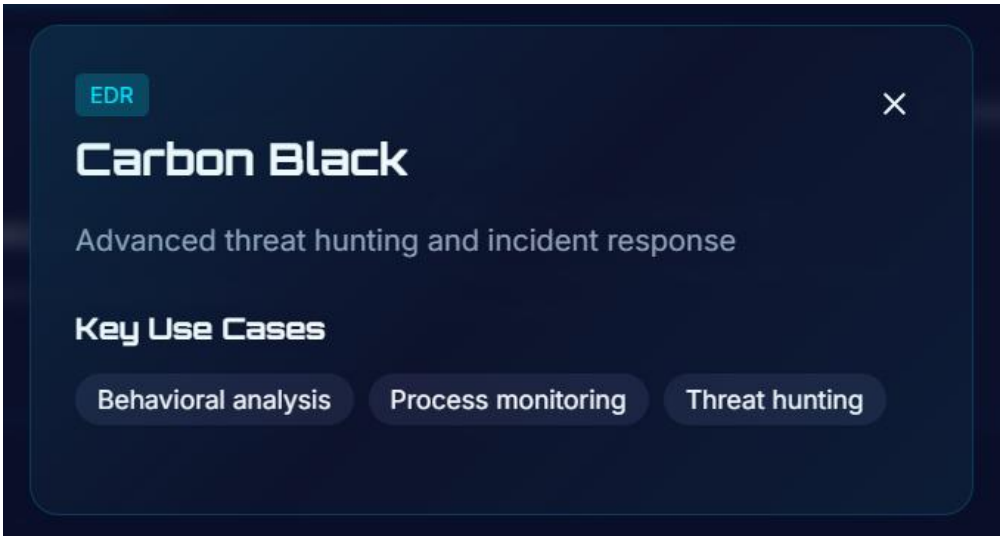



SIEM
Microsoft Sentinel
Cloud-native SIEM with AI-powered analytics
Key Use Cases
Azure integration
UEBA
SOAR automation
Threat hunting
Sample Query
SecurityEvent | where EventID == 4625 | summarize count() by Account

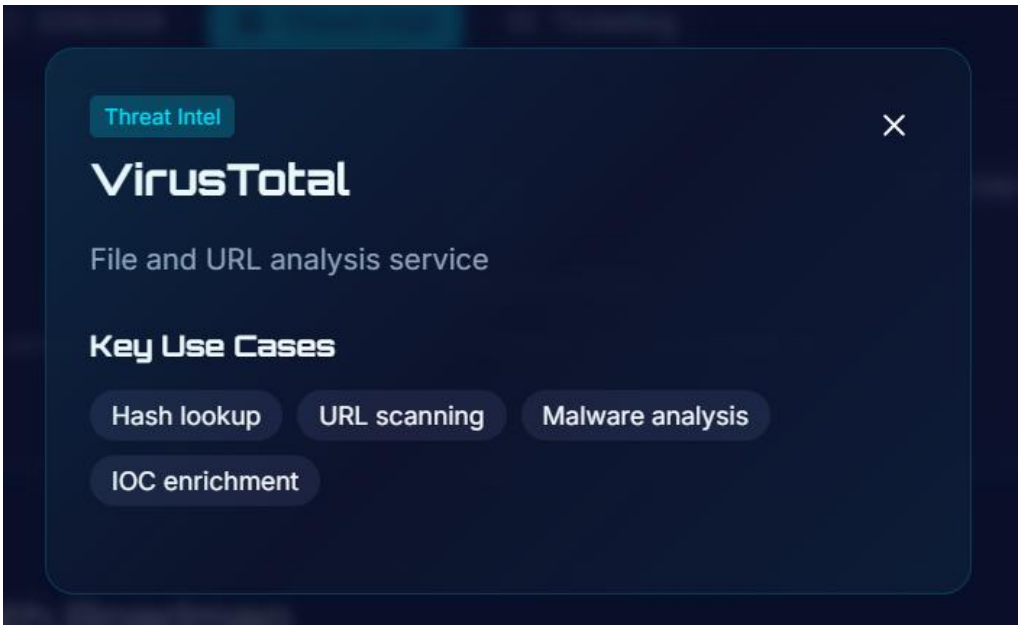

SIEM
IBM QRadar
Enterprise SIEM with advanced correlation
Key Use Cases
Offense management
Network insights
Risk scoring
Compliance

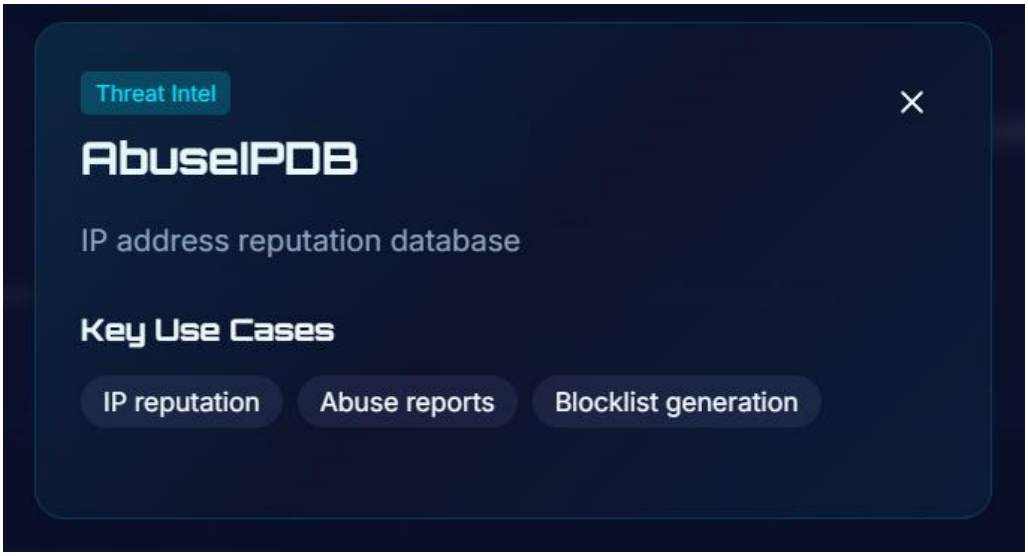
2. **EDR/XDR Solutions**

   CrowdStrike Falcon, Microsoft Defender for endpoint, carbon black. Understand: endpoint telemetry, process trees, files integrity monitoring, threat hunting capabilities.

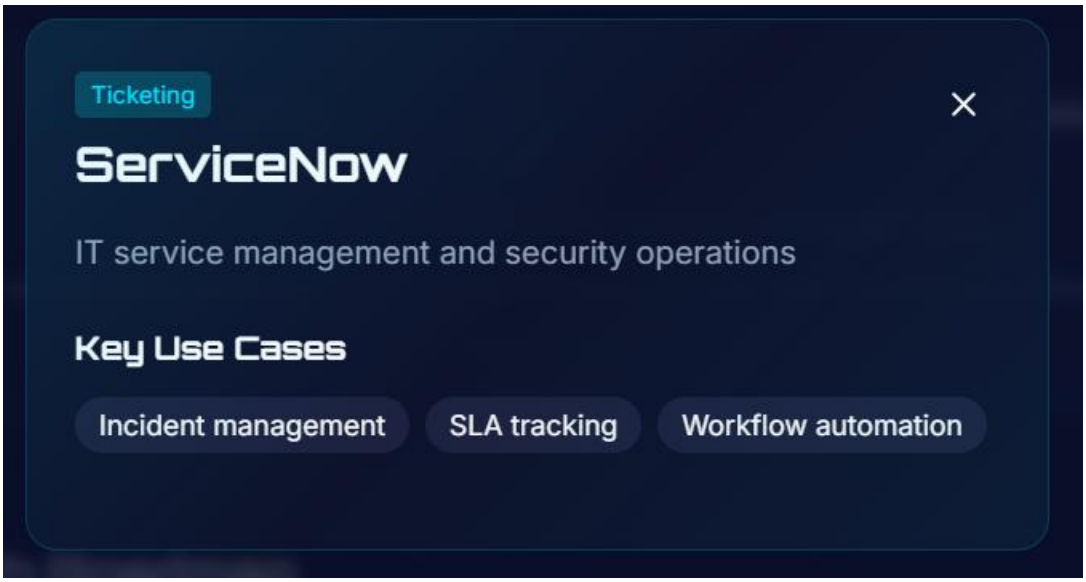


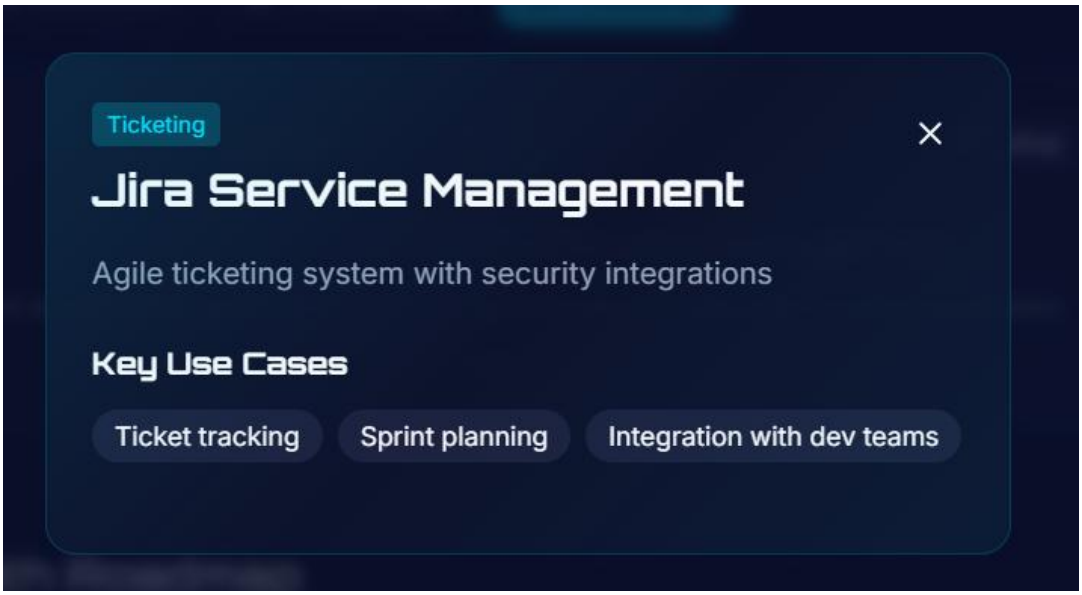
3. **Threat Intelligence**
   VirusTotal, AbuselPDB, MTRE ATT&CK Navigator. Use for : IOC enrichment, reputation checks, mapping adversary techniques to detections.





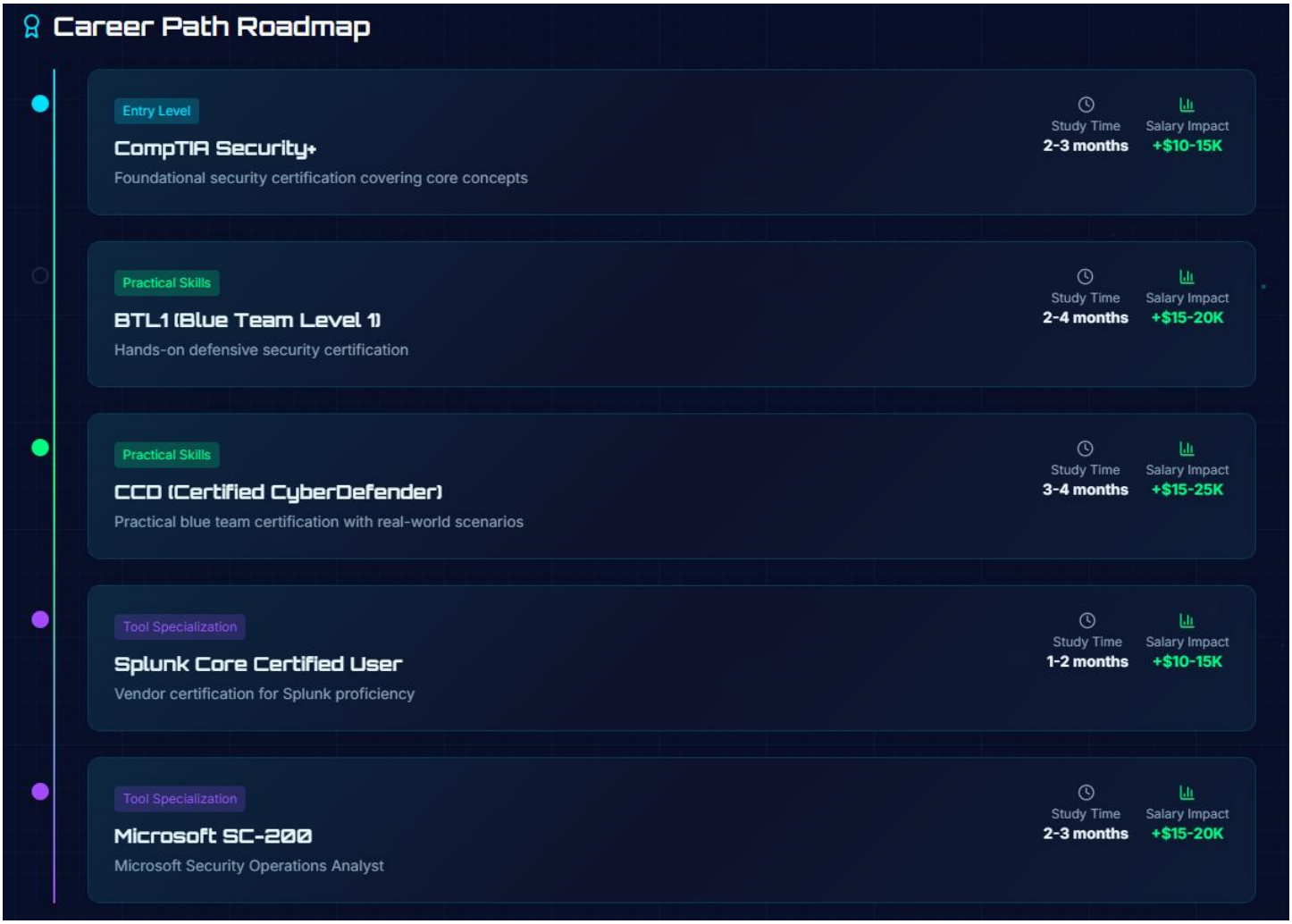
4. **Ticketing Systems**
   ServiceNow, Jira Critical for: documenting investigations, tracking escalations,maintaining audit trails, measuring KPIs.





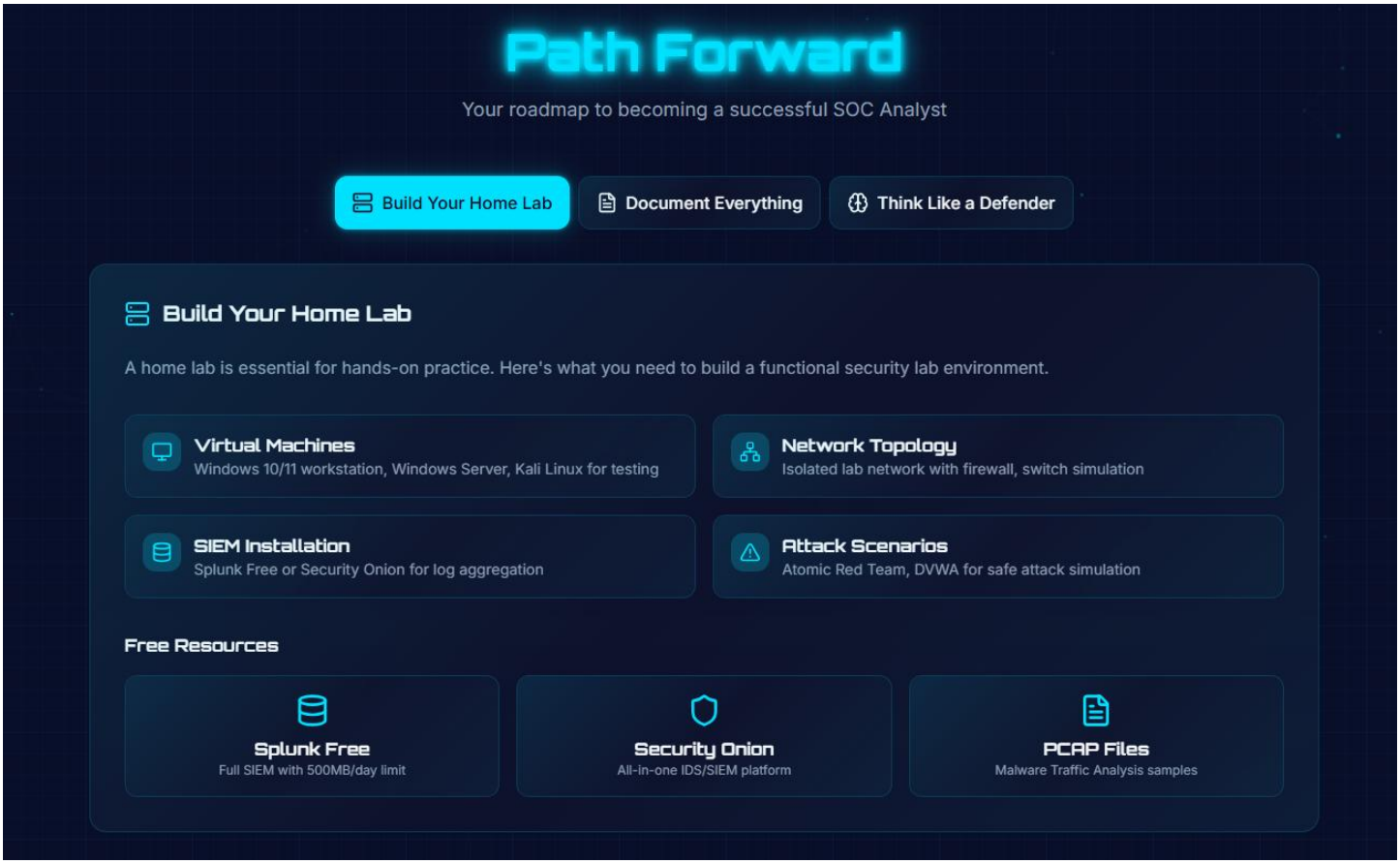
Certifications

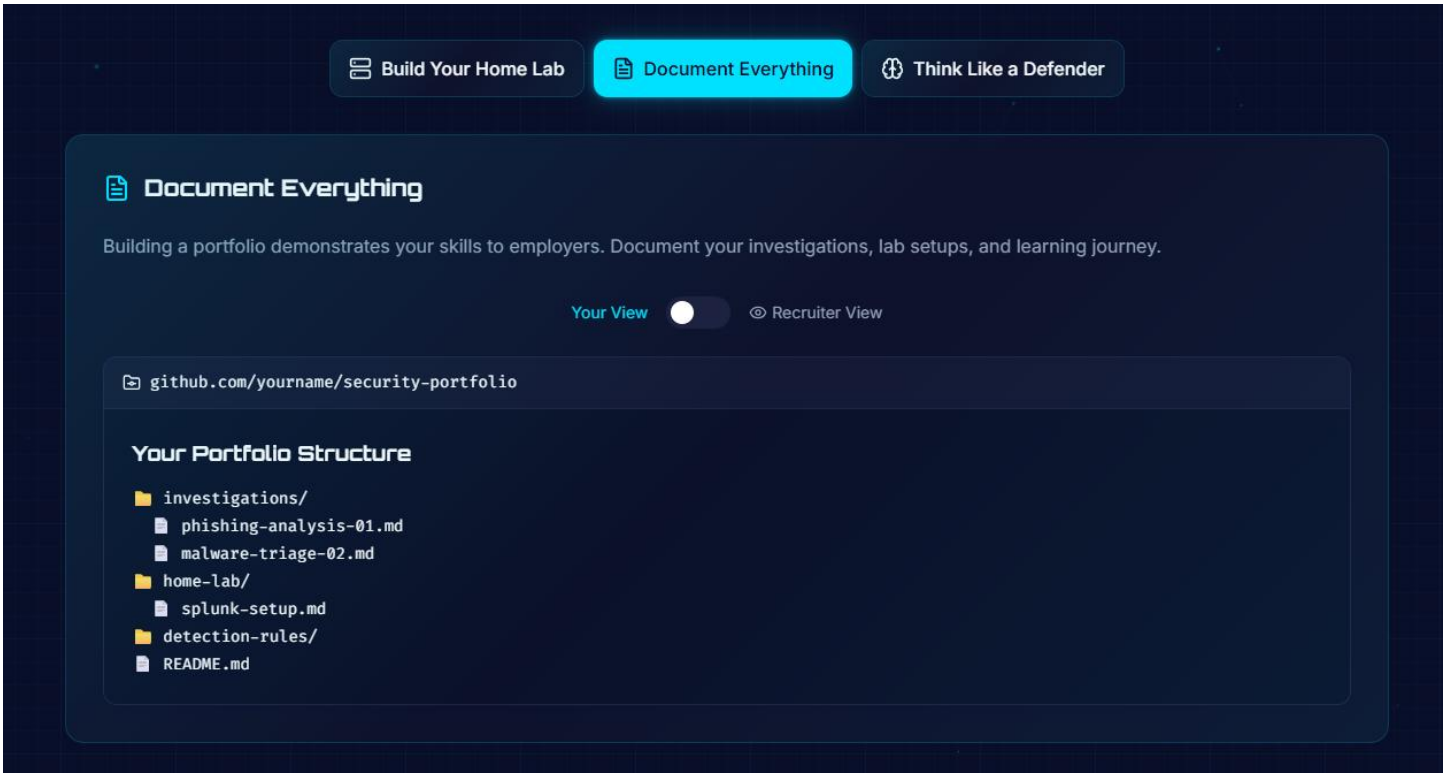
1. **Entry Level**
   CompTIA Security+: Industry standard baseline. Many SOC roles require this as minimum qualification. Covers fundamental security concepts interviewers expect you to know.
2. **Practical Skills**
   BTL1(Blue Team Level1) or CCD (Certified Cybersecurity Defender), Hands on defender Security. These prove you can actually analyze logs and detect threats, not just memorize theory
3. **Tool Specific**
   Splunk core certified user or Microsoft sc-200- vendor certification, practical tool expertise. Valuable when applying for organizations

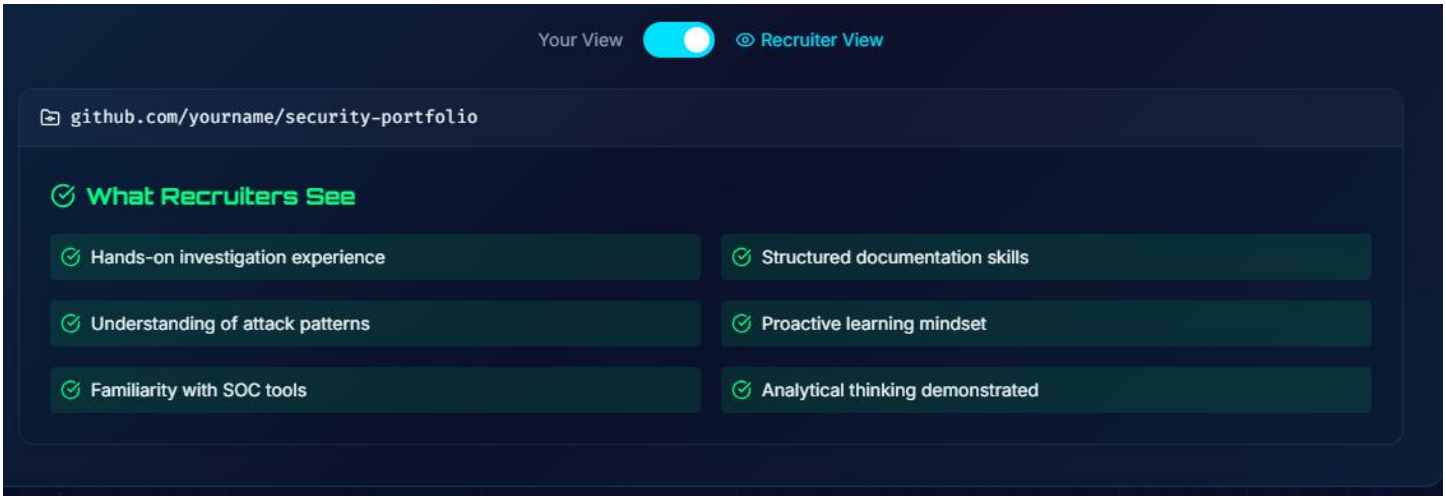


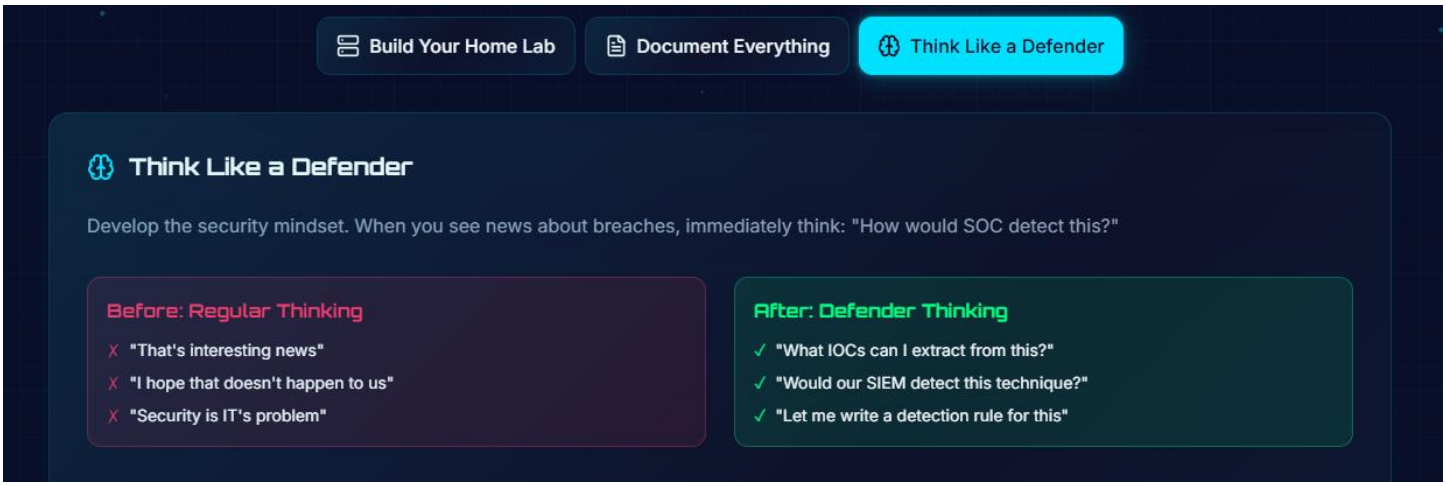
Path forward to from training to Employment

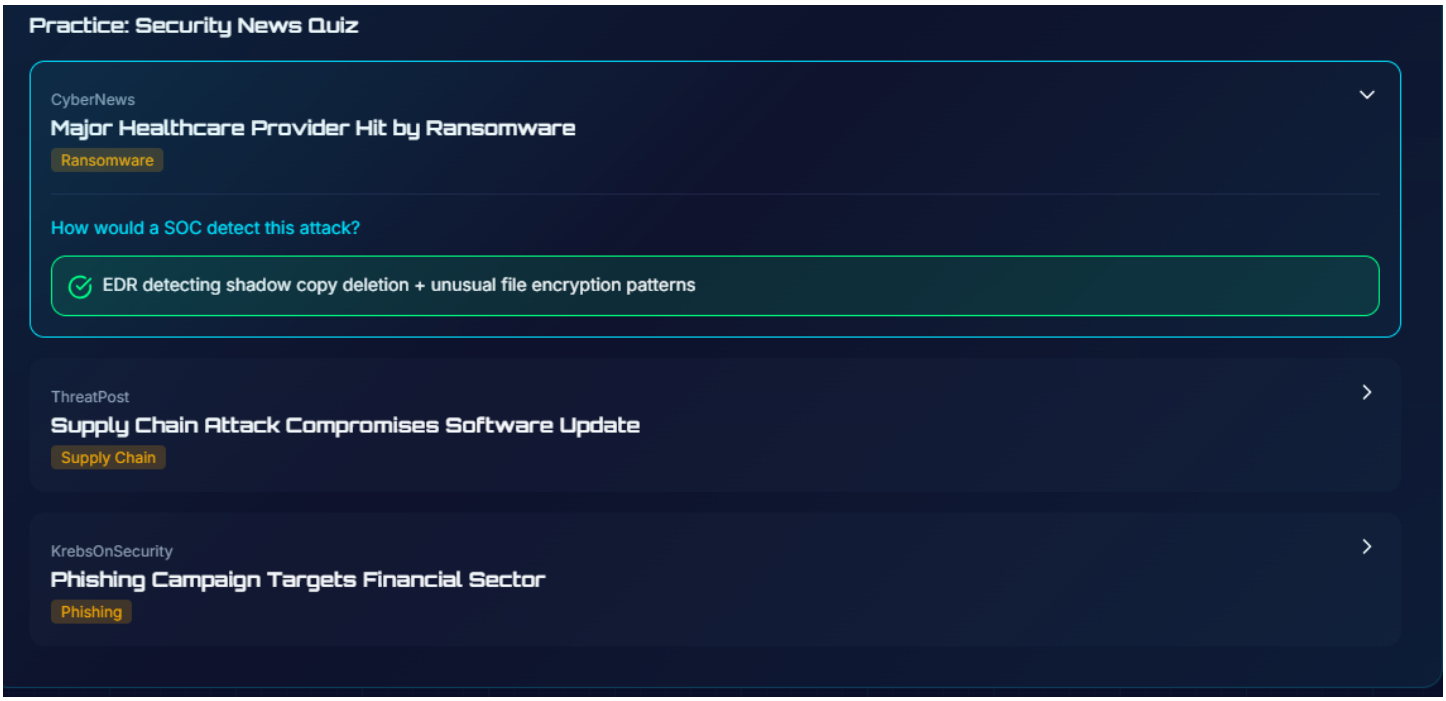
1. Build your home lab
2. Document everything
3. Think like a defender

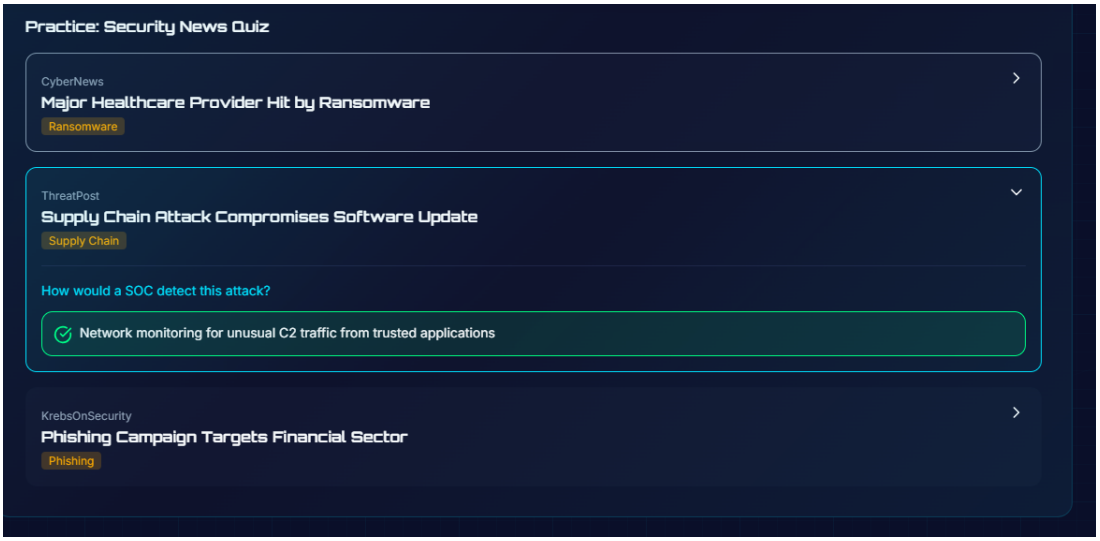


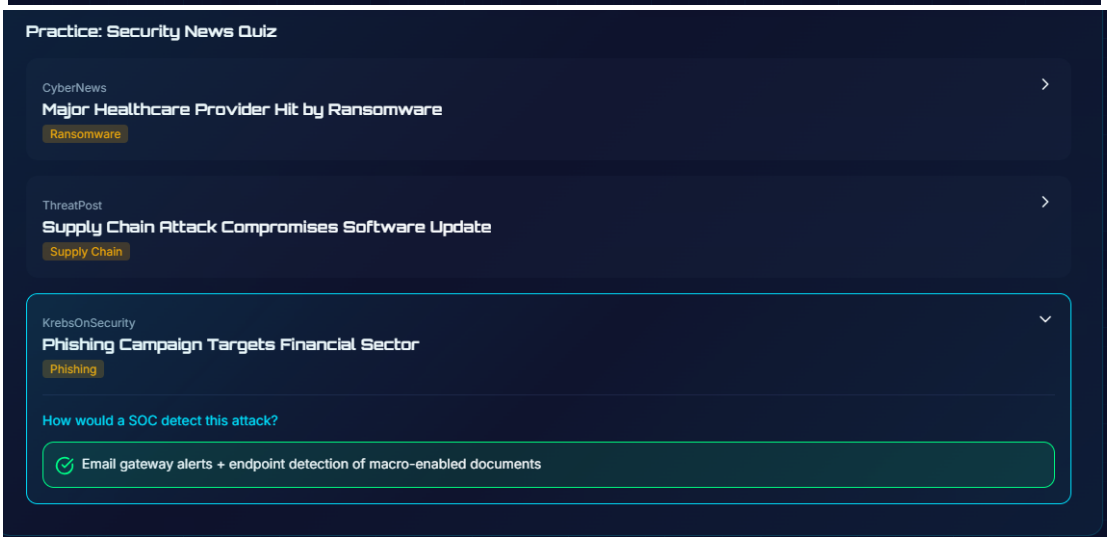


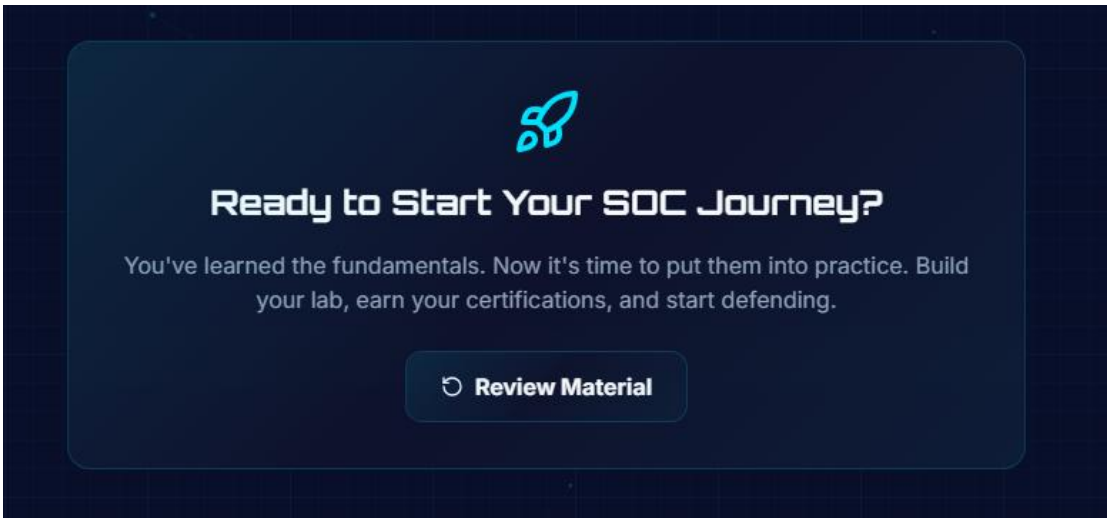

Your View
Recruiter View
github.com/yourname/security-portfolio
What Recruiters See
Hands-on investigation experience
Structured documentation skills
Understanding of attack patterns
Proactive learning mindset
Familiarity with SOC tools
Analytical thinking demonstrated


Build Your Home Lab
Document Everything
Think Like a Defender
Think Like a Defender
Develop the security mindset. When you see news about breaches, immediately think: "How would SOC detect this?"
Before: Regular Thinking
"That's interesting news"
"I hope that doesn't happen to us"
"Security is IT's problem"
After: Defender Thinking
"What IOCs can I extract from this?"
"Would our SIEM detect this technique?"
"Let me write a detection rule for this"


Practice: Security News Quiz
CyberNews
Major Healthcare Provider Hit by Ransomware
Ransomware
How would a SOC detect this attack?
EDR detecting shadow copy deletion + unusual file encryption patterns
ThreatPost
Supply Chain Attack Compromises Software Update
Supply Chain
KrebsOnSecurity
Phishing Campaign Targets Financial Sector
Phishing







Note on the Screenshots: The examples shown throughout this guide are taken from an **interactive cybersecurity learning platform** I'm currently developing. This hands-on project combines my security knowledge with web development skills (MERN Stack) to create an engaging learning experience. Once completed, I'll be making it publicly available.

About Me

I'm an aspiring **SOC Analyst** and **Web Application Penetration Tester**, actively building my expertise in both defensive and offensive security. My journey involves hands-on learning with SIEM platforms (Splunk, Wazuh), EDR solutions (CrowdStrike, SentinelOne), and pentesting tools like Burp Suite, Nmap, and Nessus.

I'm passionate about transforming security alerts into actionable insights and uncovering vulnerabilities through structured methodologies like the OWASP Top 10. My goal is to contribute meaningfully to organizations by bridging the gap between threat detection and secure application development.

Let's Connect:

I regularly share insights, projects, and learning experiences on my professional platforms. Follow my journey and feel free to connect:

- **LinkedIn:** Usama Sani Khanzada | LinkedIn
- **GitHub:** Usama Sani

Your feedback, collaboration ideas, and questions are always welcome. Let's learn and grow together in the ever-evolving field of cybersecurity!