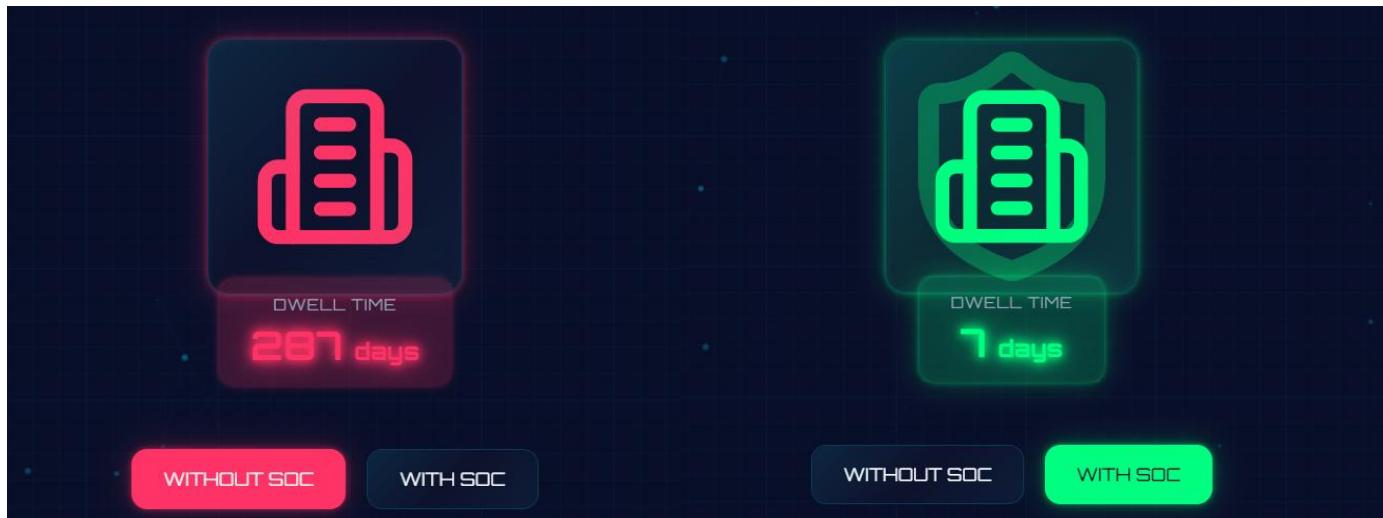


Security Operation Center Analyst L1

Why SOC Exists?

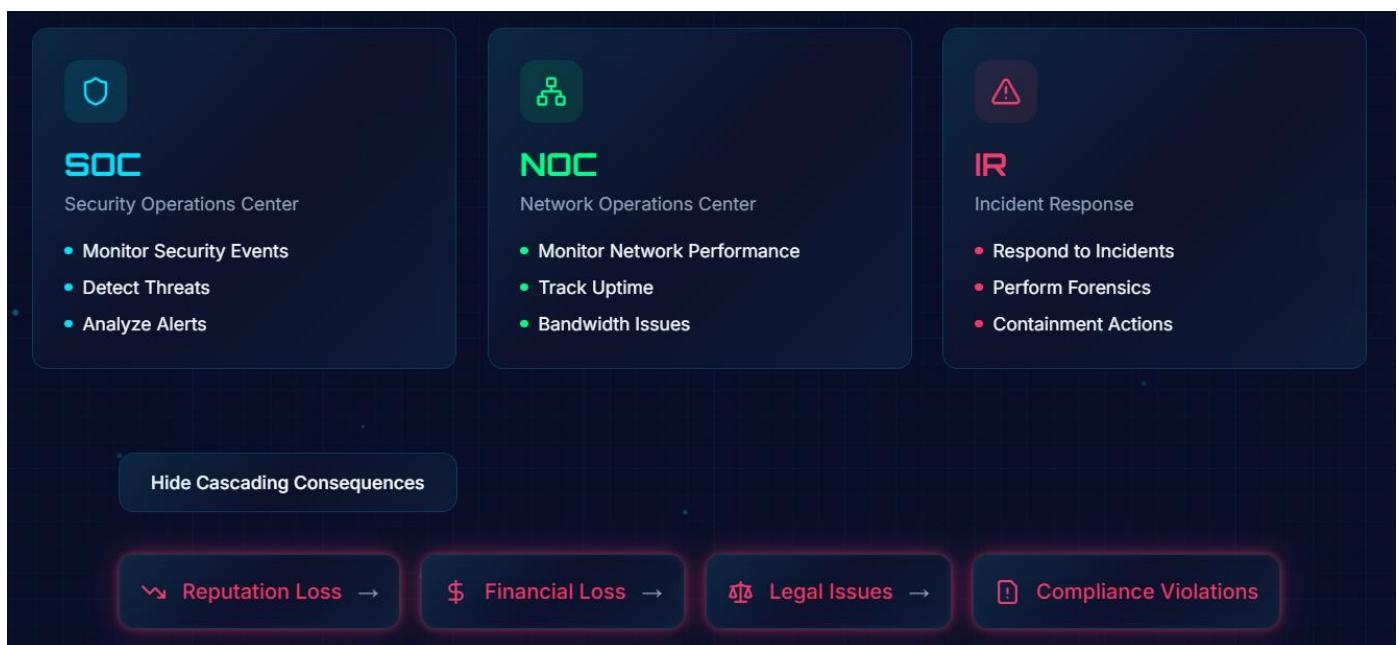
Organization bleed data and money. The SOC exists to minimize DWELL-Time (the time an attacker stay hidden). Without SOC, breacher are discovered by customers or FBI causing massive reputation and financial loss.



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)

The screenshot shows a web-based simulation tool for SOC analysts. At the top, it says "Top Attacks" and "Interactive attack simulations from a defender's perspective". There are three tabs: "Phishing" (highlighted in blue), "Brute Force", and "Ransomware".

Phishing Attack Simulation:

- Email Headers:** From: security@micr0soft.com
Subject: ⚠️ URGENT: Your account will be suspended in 24 hours!
- Email Content:** Dear Valued Customer,
We have detected unusual activity on your account. Your account will be SUSPENDED unless you verify your identity immediately.
- Attachment:** verification_form.exe
- Action Button:** Analyze Email

Threat Analysis: Risk: 95%

- [HIGH] Domain registered 2 days ago
- [HIGH] Executable attachment detected
- [MED] Urgency language patterns
- [MED] No previous communication history
- [IOC] Hash: a3f2e1d4c5b6 ...
- [IOC] Domain: micr0soft.com

Alert: ⚠️ MALICIOUS - Phishing Attack Confirmed

Quick Quiz: Try Again

As an L1 analyst, what's your FIRST action?

Options:

- A Delete the email immediately
- B Click the link to investigate
- C Check email headers and query threat intel
- D Ignore it, looks harmless

Explanation: Always analyze email headers and check sender reputation against threat intelligence before taking action. Never click suspicious links!

2. Brute Force

Log: Active Directory, Azure AD

Look For: 4625 (failed login) x 100 followed by 4624 (Success)

The screenshot shows a web-based simulation tool for security training. At the top, there are three tabs: "Phishing", "Brute Force" (which is selected and highlighted in blue), and "Ransomware". Below the tabs, the main interface is titled "Brute Force Attack Simulation". It features a "Corporate Login" section with fields for "Username" (admin@company.com) and "Password" (represented by a series of red masked dots). To the right of the login form is a "Active Directory Logs" panel. The logs show a sequence of failed logins (4625) followed by one successful login (4624):


```

23:45:13 [4625] Failed login: admin@company.com from 192.168.1.100
23:45:14 [4625] Failed login: admin@company.com from 192.168.1.100
23:45:15 [4625] Failed login: admin@company.com from 192.168.1.100
23:45:16 [4625] Failed login: admin@company.com from 192.168.1.100
23:45:17 [4625] Failed login: admin@company.com from 192.168.1.100
23:45:18 [4625] Failed login: admin@company.com from 192.168.1.100
23:45:19 [4625] Failed login: admin@company.com from 192.168.1.100
23:45:20 [4624] Successful login: admin@company.com from 192.168.1.100
    
```

 A callout box highlights a "Pattern Detected": "10 failed attempts followed by success from single IP Time window: 10 seconds". Below the logs, a "Quick Quiz" section asks: "You see 100+ failed logins followed by success. What do you do?". The options are:

- A Nothing, user probably forgot password
- B Immediately disable the account and escalate (selected)
- C Wait and monitor for more activity
- D Send an email to the user

 An explanation box states: "Explanation: This is a classic brute force success pattern. Immediate account lockout and escalation prevents further lateral movement."

3. Ransomware

Log: EDR/File server.

Look For: Mass file notification, Volume shadow copy deletion (“vssadmin delete shadows”).

The screenshot shows a dark-themed user interface for a ransomware attack simulation. At the top, there are three tabs: "Phishing", "Brute Force", and "Ransomware", with "Ransomware" being the active tab. Below the tabs, there are four horizontal sections: "Initial Access", "Encryption", "Shadow Delete", and "Ransom Note". A red progress bar is visible above the "Encryption" section. On the left, under "Encryption", there is a list of files from the directory "C:\Users\victim\" that have been encrypted, each ending with ".encrypted". On the right, under "Shadow Delete", there is an "EDR ALERT - CRITICAL" box showing a process named "vssadmin.exe" performing a "Shadow copy deletion" action, labeled as "RISK: RANSOMWARE BEHAVIOR". Below this is a "YOUR FILES ARE ENCRYPTED" box containing a skull icon, a message asking to pay 5 BTC, and a payment address starting with "bc1qxy2kgd...". At the bottom, there is a "Quick Quiz" section asking about EDR alerts on shadow copy deletion, with option A ("Isolate the endpoint immediately") selected. An explanation at the bottom states that shadow copy deletion is a strong ransomware indicator.

Ransomware Attack Simulation

Initial Access Encryption Shadow Delete Ransom Note

C:\Users\victim\

- Documents/budget_2024.xlsx .encrypted
- Documents/contracts.pdf .encrypted
- Photos/team_photo.jpg .encrypted
- Projects/roadmap.docx .encrypted
- Database/customers.db .encrypted
- Backups/full_backup.zip .encrypted

EDR ALERT - CRITICAL

Process: vssadmin.exe
Action: Shadow copy deletion
Risk: RANSOMWARE BEHAVIOR

YOUR FILES ARE ENCRYPTED

Pay 5 BTC to decrypt your files. You have 48 hours.
bc1qxy2kgd...
...

Quick Quiz

EDR alerts on shadow copy deletion. Your priority?

A Isolate the endpoint immediately

B Run a full antivirus scan

C Wait for more indicators

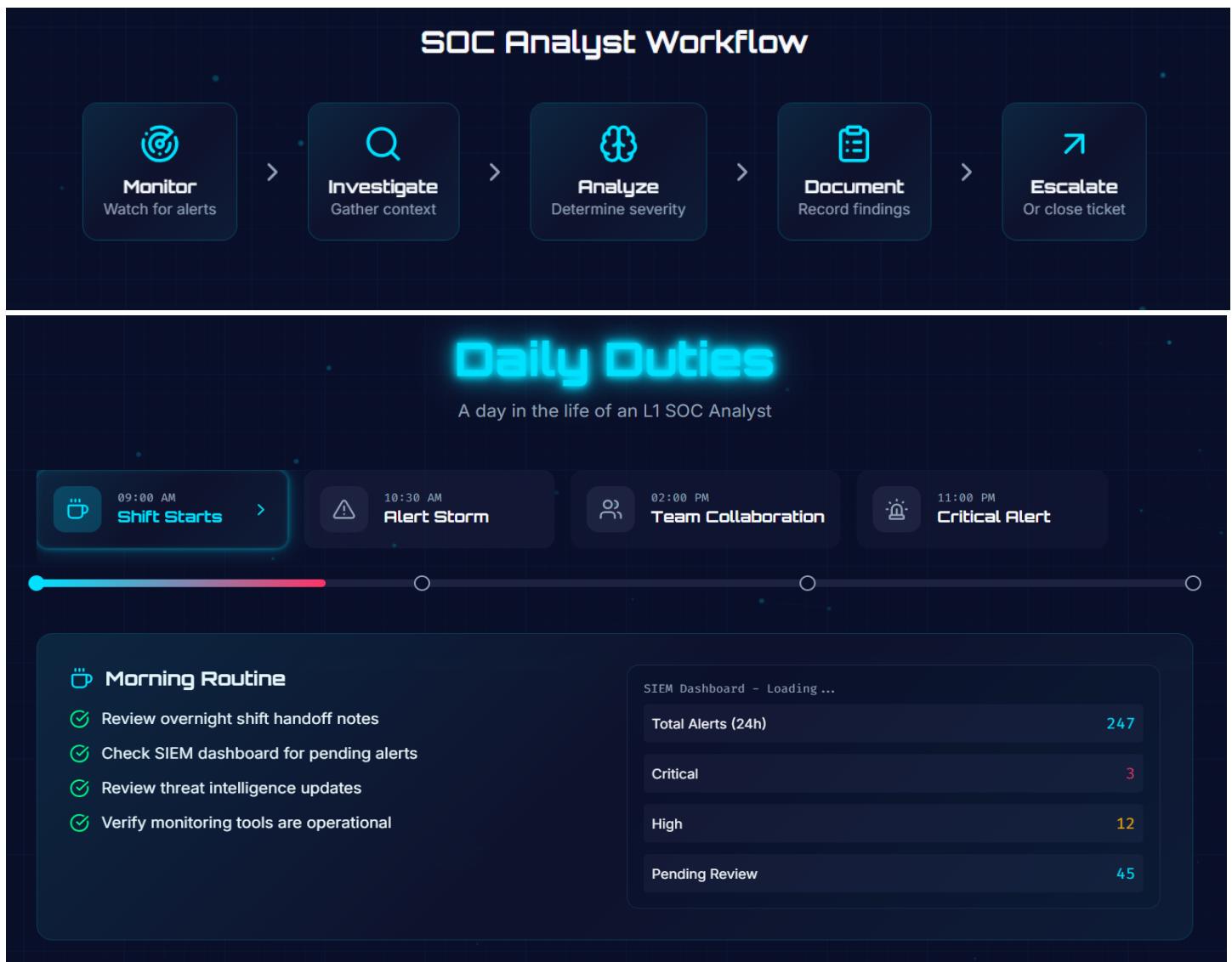
D Reboot the machine

Explanation: Shadow copy deletion is a strong ransomware indicator. Immediate isolation prevents lateral spread and gives IR time to respond.

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



The screenshot shows a digital dashboard with a timeline at the top. Four events are listed: "Shift Starts" at 09:00 AM, "Alert Storm" at 10:30 AM (highlighted with a yellow warning icon), "Team Collaboration" at 02:00 PM, and "Critical Alert" at 11:00 PM.

Alert Queue:

- Ransomware Behavior Detected (CRITICAL) - EDR • 10:31 AM
- Multiple Failed SSH Logins (HIGH) - Firewall • 10:32 AM
- Unusual Outbound Traffic (MEDIUM) - IDS • 10:33 AM
- Certificate Expiry Warning (LOW) - PKI Monitor • 10:35 AM

The screenshot shows a digital dashboard with a timeline at the top. The same four events are listed: "Shift Starts" at 09:00 AM, "Alert Storm" at 10:30 AM, "Team Collaboration" at 02:00 PM (highlighted with a green user icon), and "Critical Alert" at 11:00 PM.

Team Chat:

L2-Senior • 2:03 PM: I've got a suspicious process spawning from Word on WORKSTATION-15. Child process is powershell.exe with encoded command.

Good catch. Have you checked the command line arguments? Look for base64 encoding patterns.

L1-Analyst (You) • 2:05 PM: Yes, decoded it - it's reaching out to pastebin.com for second stage. Isolating the endpoint now.

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-Senior • 2:08 PM: Also check if any other endpoints have communicated with that pastebin URL in the last 24h.

CRITICAL ALERT RECEIVED

Alert Type: **Ransomware Detection**

Affected Systems: **15 endpoints**

Severity: **CRITICAL**

Time Detected: **11:00:32 PM**

Response Time Target: **3:00**

Isolate All Affected **Escalate to IR** **View Full Details**

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

Outbound Connection to Known C2

Source: EDR + Threat Intel

Process: outlook.exe → powershell.exe

Destination: 185.234.xx.xx (Malicious)

Beaconing pattern detected: 60s interval

Live Alert Feed

- 10:30:10 • Outbound Connection to Known C2
- 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 →

The screenshot shows a digital investigation interface with the following components:

- Threat Alerts (Top Row):**
 - 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.
- Investigation Buttons:** What SOC Sees, Investigation (highlighted), Actions, Outcome.
- Your Investigation Section:**
 - Click tools to gather evidence:
 - Check Email Headers:** Completed.
 - Query Threat Intel:** Completed.
 - Review Process Tree:** Completed.
- Investigation Notes (Right):**
 - Check Email Headers:** Spoofed sender: security@microsoft-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 →** button.

The screenshot shows a digital investigation interface with the following components:

- Threat Alerts (Top Row):**
 - 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.
- Investigation Buttons:** What SOC Sees, Investigation (highlighted), Actions, Outcome.
- L1 Action Required Section (Bottom):**
 - L1 Action Required:** Select the actions you would take as an L1 analyst:
 - Actions:**
 - Isolate the endpoint** (Completed)
 - Block C2 IP at firewall** (Completed)
 - Reset user credentials** (Completed)
 - Escalate to IR team** (Completed)
 - Document IOCs** (Completed)
 - Actions taken:** 5/5
 - See Outcome →** button.

Investigation Complete

50%
Investigation Score

Threat contained. No lateral movement detected.

Key Takeaways

- Quick isolation prevented data exfiltration
- C2 block stops attacker communication

Try Again

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

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

Suspicious Process - High Resource Usage
Source: EDR + Server Monitor

- Process: svchost.exe (unusual location)
- CPU Usage: 95% sustained
- Network: Connections to mining pool

MEDIUM

Live Alert Feed

- 10:30:10 • Suspicious Process - High Resource Usage
- 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 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

The dashboard is divided into several sections:

- Top Row:** Four cards representing different threat types:
 - 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.
- Navigation Bar:** Buttons for "What SOC Sees" (highlighted in blue), "Investigation", "Actions", and "Outcome".
- What SOC Sees:** A detailed alert for "Unusual Data Transfer Volume" (HIGH priority):
 - Source: DLP + Network Monitor
 - User: john.smith@company.com
 - Destination: mega.nz (Cloud Storage)
 - Volume: 2.3GB in 15 minutes
 To the right is a "Live Alert Feed" listing system events from 10:30:10 to 17:37:24.
- Investigation:** A button labeled "Begin Investigation →". Below it is another navigation bar with "What SOC Sees" (green), "Investigation" (highlighted in green), "Actions", and "Outcome".
- Your Investigation:** A section for gathering evidence:
 - Check User Activity (checked)
 - Review DLP Alerts (checked)
 - Check HR Status (checked)
 To the right is a "Investigation Notes" section with three entries:
 - Check User Activity:** User accessed 150+ confidential files today.
 - Review DLP Alerts:** Multiple "Confidential" labels detected in transfer.
 - Check HR Status:** User submitted resignation yesterday.
- Bottom Row:** Buttons for "Evidence gathered: 3/3" and "Take Action →".

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](#)

What SOC Sees

Pass-the-Hash Attack Detected (CRITICAL)

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 →

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 →

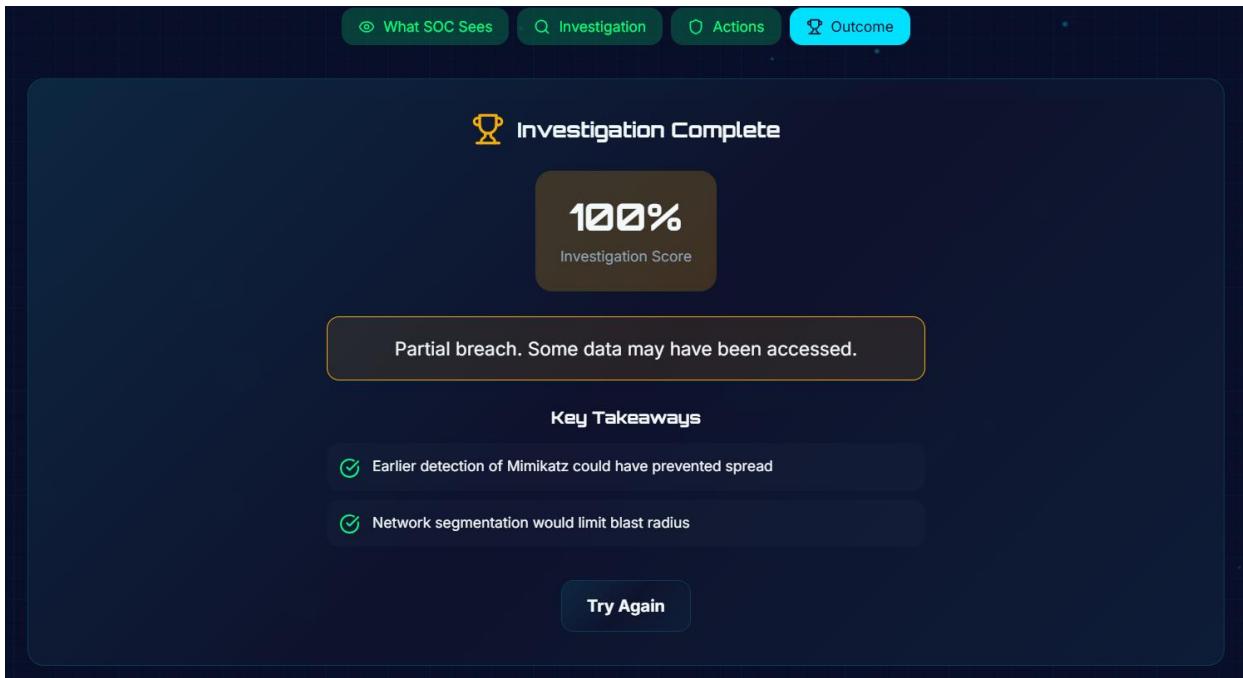
L1 Action Required

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

Time	Level	Event Description	Action
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
03:41:55	[INFO]	Email attachment downloaded	+ Evidence

[Gather Context →](#)

1. Initial Assessment 2. Log Analysis 3. Context Gathering 4. Decision

Context Gathering

Internal Checks

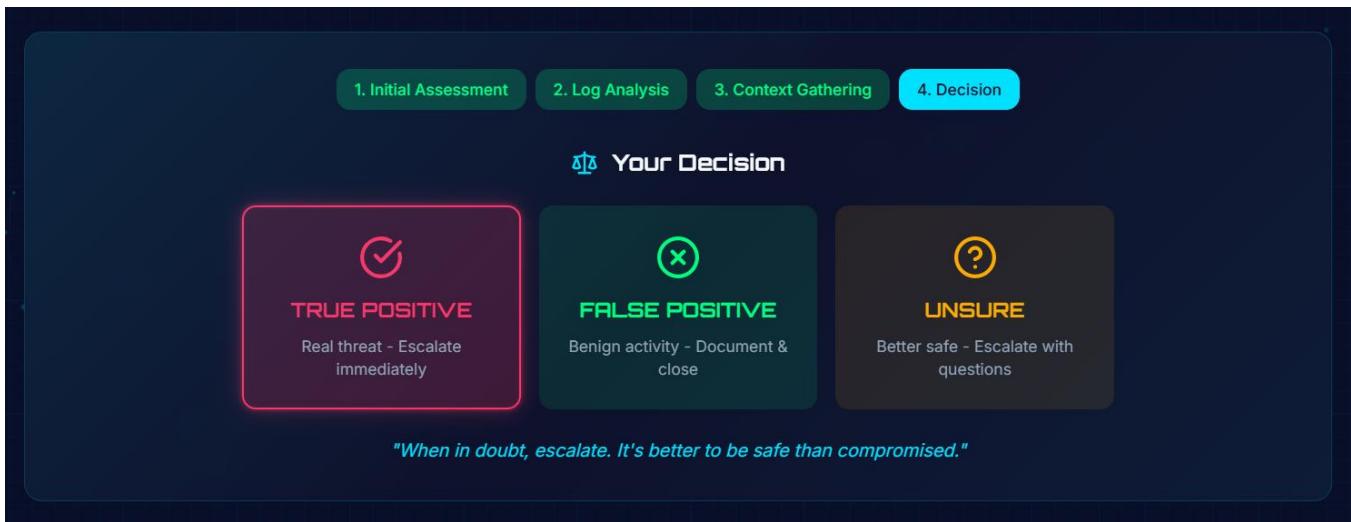
- User Account: john.smith@company.com (Marketing)
- Asset Criticality: Medium - Standard Workstation
- Historical Activity: No previous alerts for this user

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 low thresholds
- Benign Software triggering EDR heuristics
- Scheduled tasks appearing unusual process

This interface compares two lists of indicators. On the left, under "True Positive Indicators", are five items: Known malicious IP/domain, Unusual time (3 AM activity), Privilege escalation attempts, Failed logins followed by success, and Data exfiltration patterns. On the right, under "Common False Positives", are six items: Automated vulnerability scans, Legitimate admin activity with ticket, Poorly tuned detection rules, Benign software triggering rules, and Scheduled backup tasks. At the bottom is a button labeled "Try It Yourself - Practice Mode".

Practice Mode

Outbound Connection to TOR Exit Node
User workstation connecting to known TOR exit node HIGH

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

PowerShell Encoded Command Execution
Base64 encoded PowerShell command with network callback CRITICAL

Context:

- Spawns 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 →

Practice Mode Alert 5/5 Score: 4 ⚙️

Antivirus Disabled on Endpoint Windows Defender turned off MEDIUM

Context:

- IT admin account
- During software deployment
- Ticket exists

True Positive Escalate & Respond

False Positive Document & Close

Unsure Escalate with Questions

Correct! Legitimate IT activity with change ticket. Document and monitor for re-enablement.

Final Score: 5/5

Try Again

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 ×

Splunk

Industry-leading security information and event management platform

Key Use Cases

- Log aggregation
- Threat detection
- Dashboards
- Alerting

Sample Query

```
index=security sourcetype=auth action=failure |
stats count by src_ip | where count > 10
```

SIEM X

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 X

IBM QRadar

Enterprise SIEM with advanced correlation

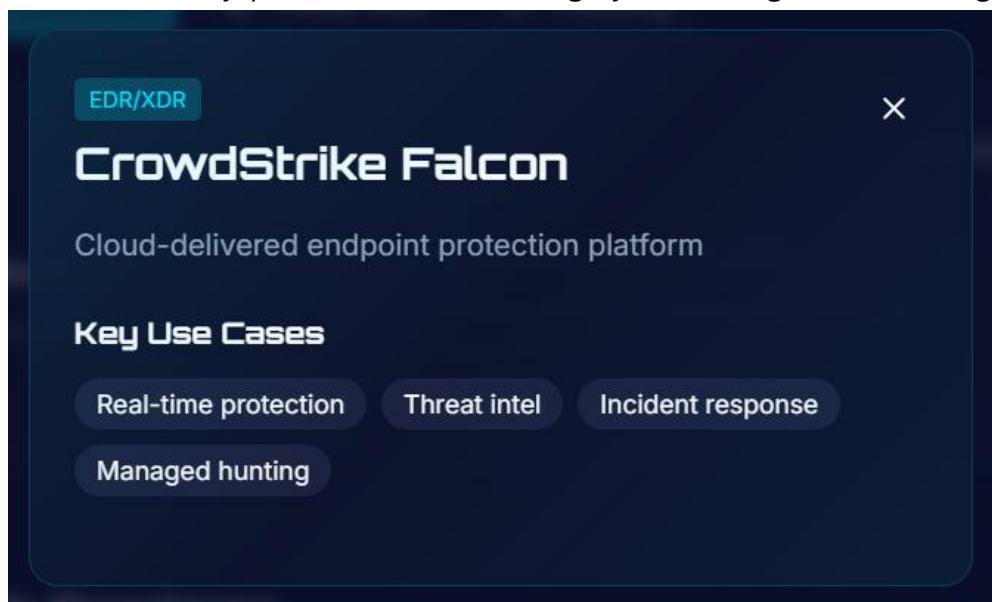
Key Use Cases

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.



EDR/XDR X

CrowdStrike Falcon

Cloud-delivered endpoint protection platform

Key Use Cases

- Real-time protection
- Threat intel
- Incident response

Managed hunting



EDR/XDR X

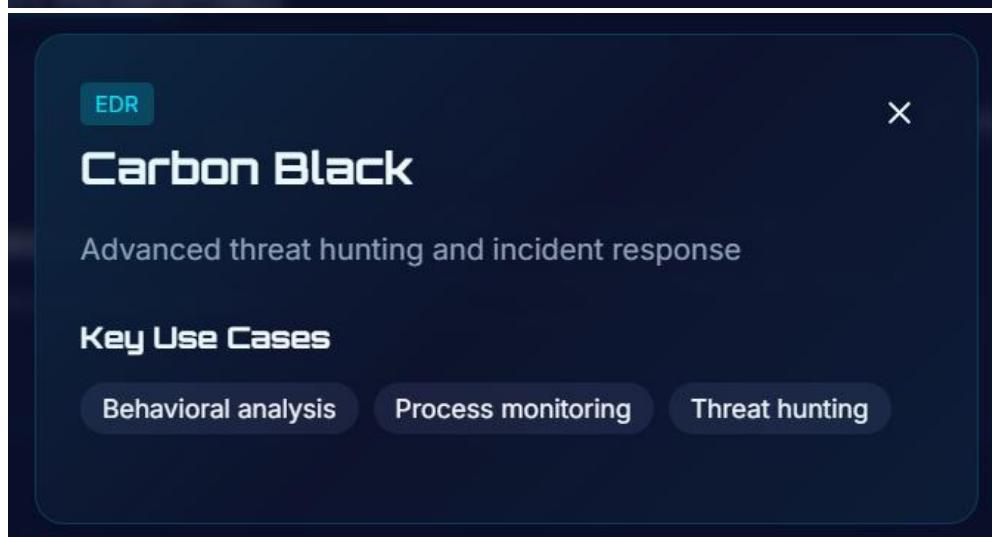
Microsoft Defender

Unified endpoint security for Microsoft ecosystem

Key Use Cases

- Microsoft 365 integration
- Attack surface reduction

Auto remediation



EDR X

Carbon Black

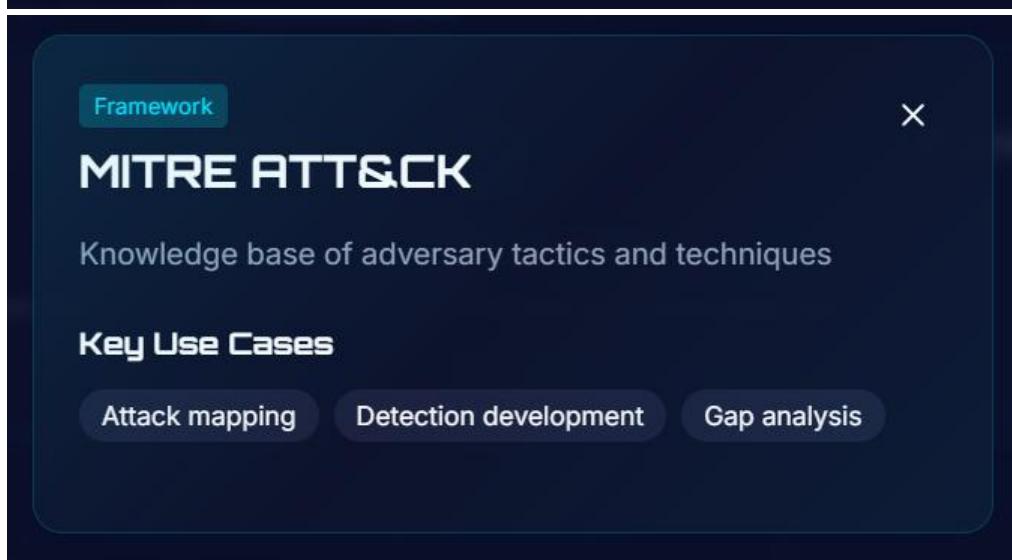
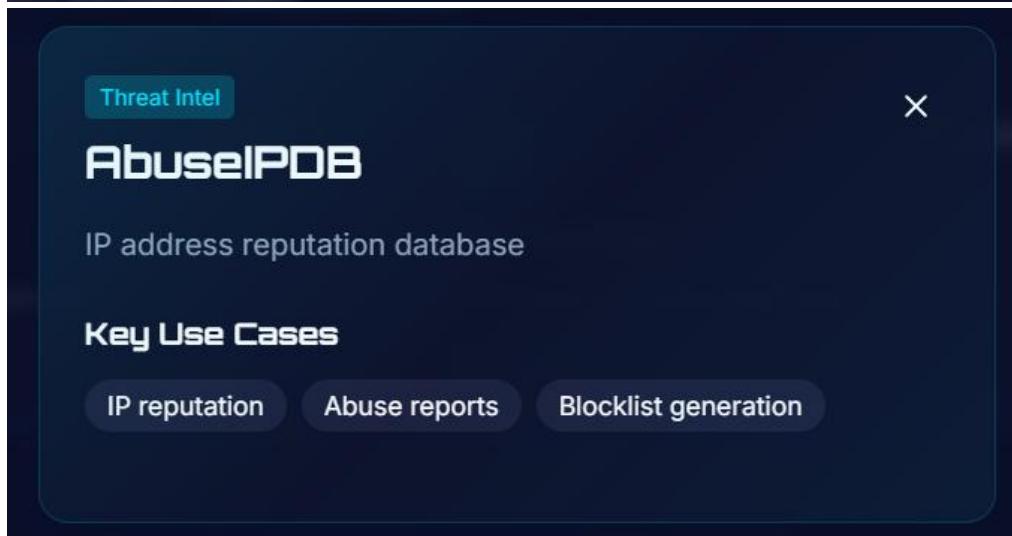
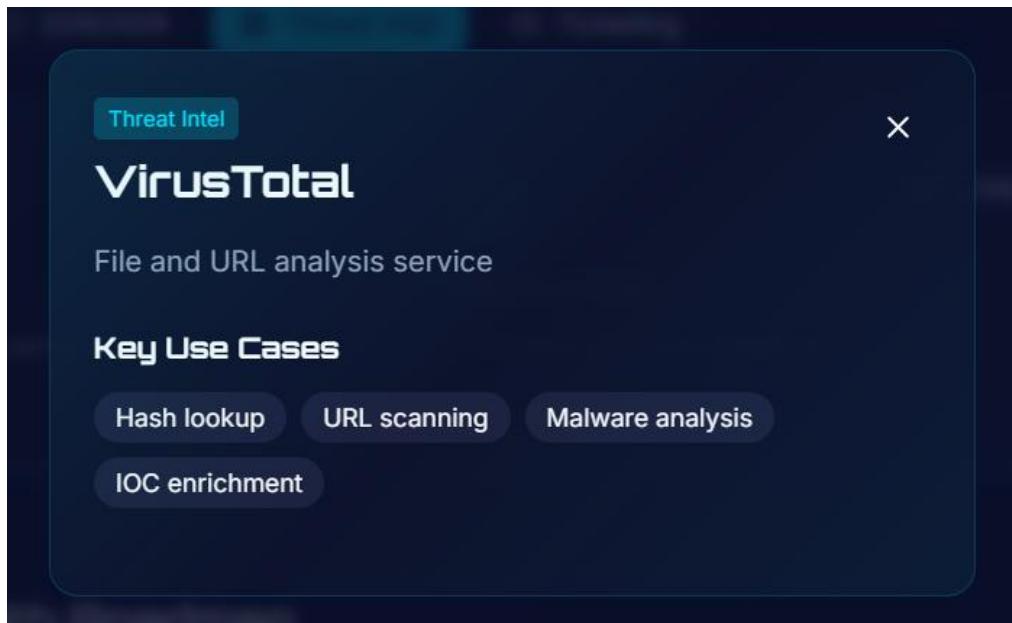
Advanced threat hunting and incident response

Key Use Cases

- Behavioral analysis
- Process monitoring
- Threat hunting

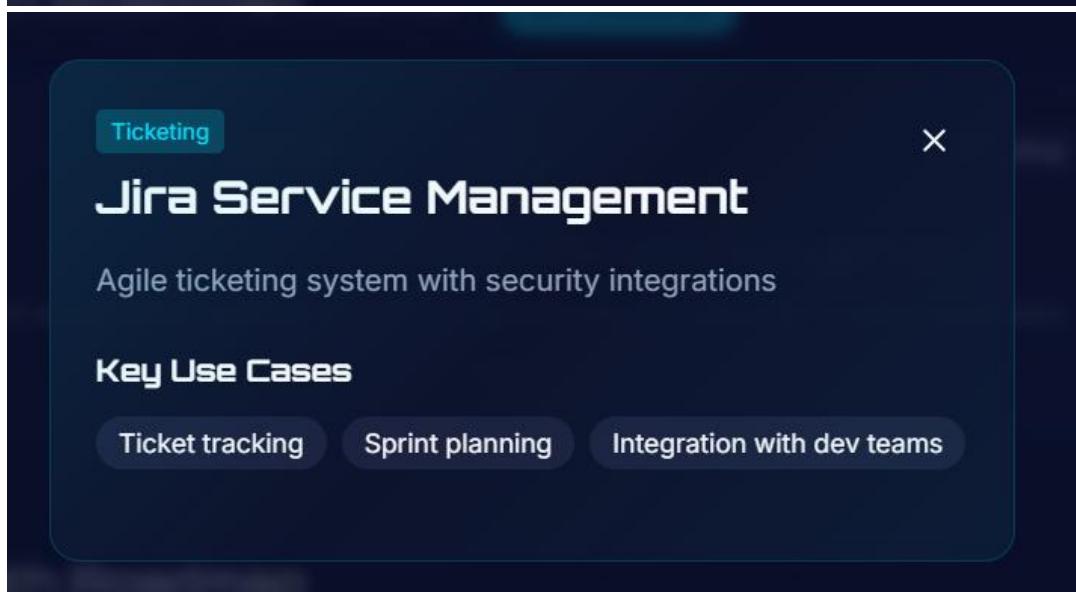
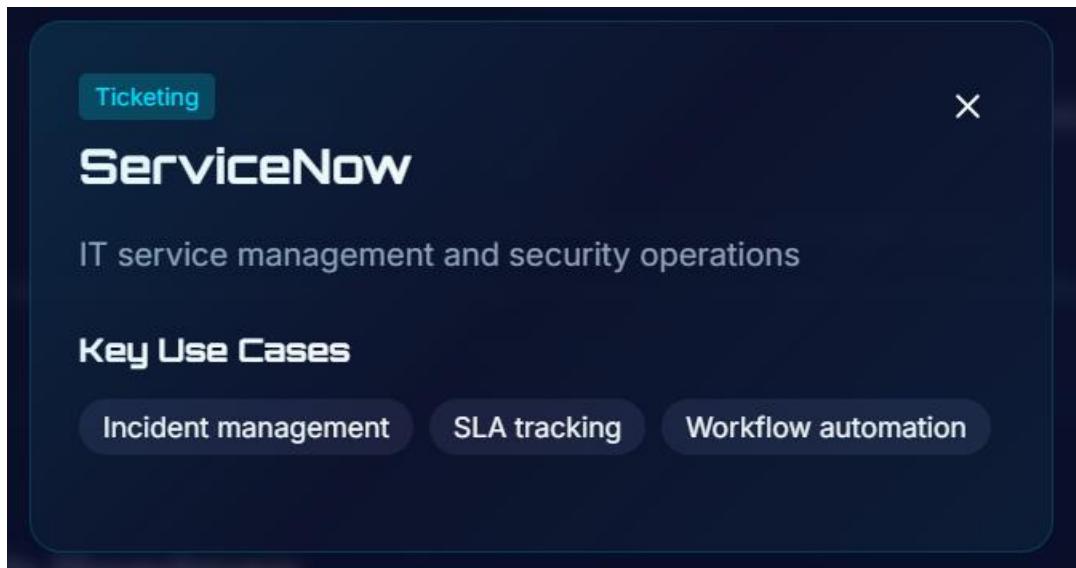
3. Threat Intelligence

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

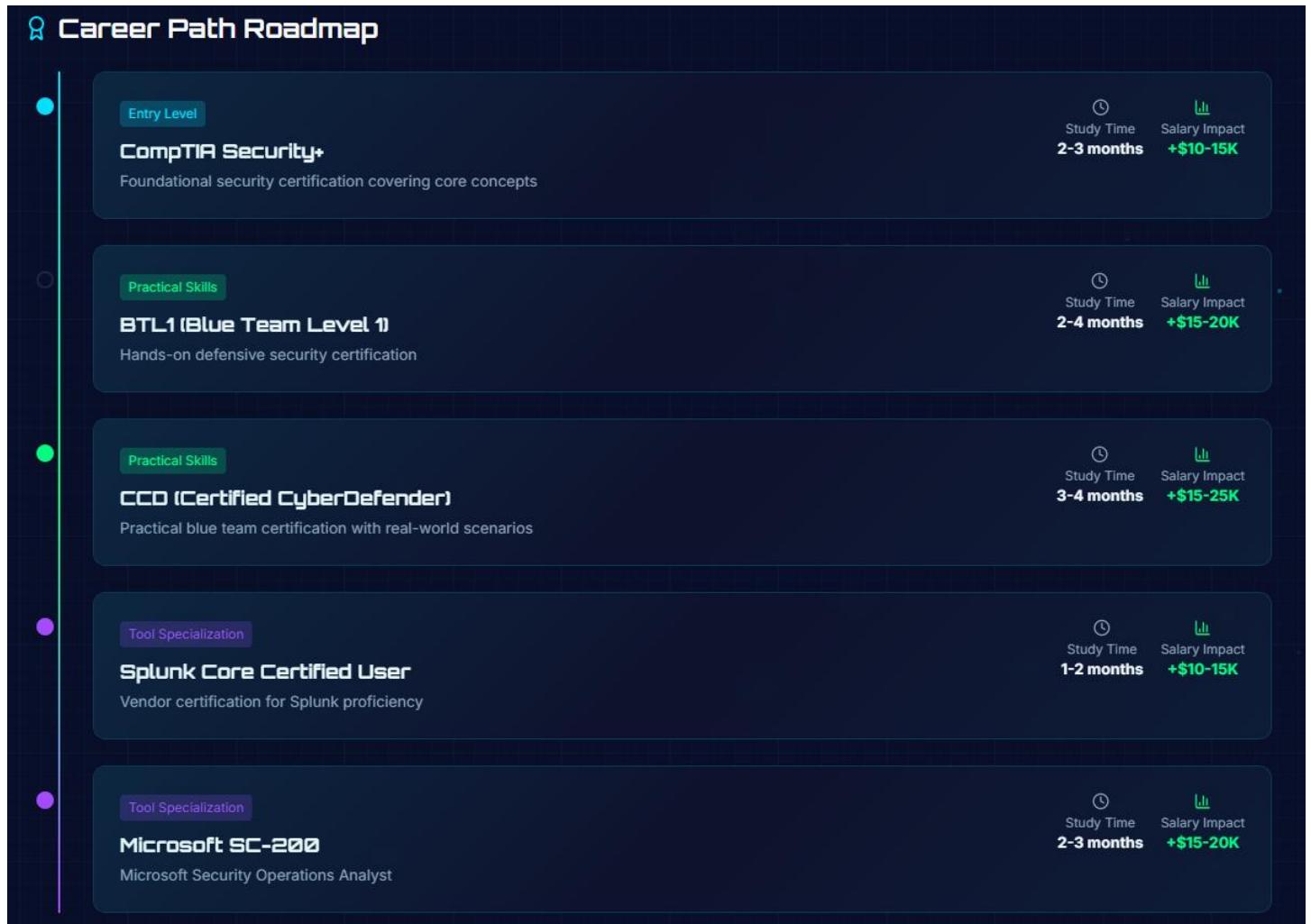
CompTIA Security+: Industry standard baseline. Many SOC roles require this as minimum qualification. Covers fundamental security concepts interviewers expect you to know.

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

Path Forward

Your roadmap to becoming a successful SOC Analyst

[!\[\]\(60efbc215ff2708f9788850749718588_img.jpg\) Build Your Home Lab](#) [!\[\]\(3d5ca619ec1486b0901e27890459ac27_img.jpg\) Document Everything](#) [!\[\]\(ccfb1d9af827ff643454fe9e67dae0ec_img.jpg\) Think Like a Defender](#)

Build Your Home Lab

A home lab is essential for hands-on practice. Here's what you need to build a functional security lab environment.

 **Virtual Machines**
Windows 10/11 workstation, Windows Server, Kali Linux for testing

 **Network Topology**
Isolated lab network with firewall, switch simulation

 **SIEM Installation**
Splunk Free or Security Onion for log aggregation

 **Attack Scenarios**
Atomic Red Team, DVWA for safe attack simulation

Free Resources

 **Splunk Free**
Full SIEM with 500MB/day limit

 **Security Onion**
All-in-one IDS/SIEM platform

 **PCAP Files**
Malware Traffic Analysis samples

[!\[\]\(84fa512fea35528b504a1ad29cb8d780_img.jpg\) Build Your Home Lab](#) [!\[\]\(9a1d751aff68d6527928a3e6ab6ba393_img.jpg\) Document Everything](#) [!\[\]\(e718490f646f7c4264a7af8d8a04980c_img.jpg\) Think Like a Defender](#)

Document Everything

Building a portfolio demonstrates your skills to employers. Document your investigations, lab setups, and learning journey.

[Your View](#) [Recruiter View](#)

 [github.com/yourname/security-portfolio](#)

Your Portfolio Structure

```
investigations/
├── phishing-analysis-01.md
└── malware-triage-02.md
home-lab/
└── splunk-setup.md
detection-rules/
└── README.md
```

Your View Recruiter View

github.com/yourusername/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

The image displays three vertically stacked screenshots of a web-based cybersecurity news quiz platform. Each screenshot shows a dark-themed interface with a grid background. At the top of each screen is a header: "Practice: Security News Quiz". Below the header, there are three news items, each with a title, source, and a category tag.

- Screenshot 1:** Shows news from CyberNews about a "Major Healthcare Provider Hit by Ransomware" (category: Ransomware). A question below asks, "How would a SOC detect this attack?", with a correct answer highlighted in green: "Network monitoring for unusual C2 traffic from trusted applications".
- Screenshot 2:** Shows news from ThreatPost about a "Supply Chain Attack Compromises Software Update" (category: Supply Chain). A question below asks, "How would a SOC detect this attack?", with a correct answer highlighted in green: "Email gateway alerts + endpoint detection of macro-enabled documents".
- Screenshot 3:** Shows news from KrebsOnSecurity about a "Phishing Campaign Targets Financial Sector" (category: Phishing). This screen is partially visible at the bottom of the image.

At the bottom of the third screenshot, there is a large call-to-action button with a blue gradient background, white text, and a small circular icon: "Ready to Start Your SOC Journey?". Below this button, a message reads: "You've learned the fundamentals. Now it's time to put them into practice. Build your lab, earn your certifications, and start defending." At the very bottom of the image is another button: "Review Material".

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!