Name: Shah Devam
Email ID: shahdevam48@gmail.com

1) Threat Hunting

Core Concepts

Proactive Threat Hunting

Threat hunting is a proactive cybersecurity practice focused on identifying adversaries that have bypassed traditional security controls. Unlike reactive incident response, which occurs after an alert or breach, threat hunting is hypothesis-driven. Hunters form assumptions based on known adversary behaviors, tactics, techniques, and procedures (TTPs).
Example: Investigating logs for anomalous privilege escalation to detect misuse of **T1078 – Valid Accounts**, such as unexpected admin logins outside normal hours.

Hunting Frameworks

SqRR (Search, Query, Retrieve, Respond)
SqRR provides a structured workflow for threat hunting:

- **Search:** Identify areas of interest or suspicious behaviors
- **Query:** Execute targeted queries against datasets
- **Retrieve:** Collect relevant evidence
- **Respond:** Escalate findings or initiate remediation

TaHiTI (Targeted Hunting integrating Threat Intelligence)
TaHiTI integrates threat intelligence into the hunting process, enabling hunters to focus on known adversaries, campaigns, or techniques. It emphasizes intelligence-led hypotheses to improve detection accuracy and efficiency.

Data Sources for Hunting

Effective threat hunting relies on correlating multiple data sources, including:

- **Endpoint Detection and Response (EDR) logs**
- **Network traffic and flow data**
- **Authentication and identity logs**
- **Threat intelligence feeds (IOCs, TTPs, adversary profiles)**

Combining these sources enhances visibility and helps uncover stealthy or low-noise attacks.

Key Objectives

The primary objectives of threat hunting are to:

- Proactively identify hidden or emerging threats
- Apply structured methodologies to reduce detection gaps
- Improve analytical and investigative skills
- Enhance organizational resilience against advanced attackers

Event ID 4672 - Special Privileges Assigned

TIMESTAMP	USER	EVENT_ID	HOST	LOGON_ID	KEY PRIVILEGES	NOTES

JAN 20, 2026 @ 18:29:51	test_admin	4672	DESKTOP	0x248cc6	SeDebugPrivilege, SeSystemEnvironmentPrivilege	**SUSPICIOUS**: Administrative privileges assigned, includes dangerous SeDebugPrivilege
JAN 20, 2026 @ 16:13:37	test_admin	4672	DESKTOP	0x4bd573	SeDebugPrivilege, SeSystemEnvironmentPrivilege	**SUSPICIOUS**: Same user, multiple high-risk privileges
JAN 20, 2026 @ 16:12:41	maria	4672	DESKTOP	0x48228e	SeDebugPrivilege, SeSystemEnvironmentPrivilege	**SUSPICIOUS**: Administrative privileges for maria user
JAN 20, 2026 @ 16:08:33	test_admin	4672	DESKTOP	0x25cf60	SeDebugPrivilege, SeSystemEnvironmentPrivilege	**SUSPICIOUS**: Repeated privilege escalation pattern
JAN 20, 2026 @ 16:08:27	DWM-2	4672	DESKTOP	0x2433fb	SeAssignPrimaryTokenPrivilege, SeAuditPrivilege	**NORMAL**: System service account (Desktop Window Manager)
JAN 20, 2026 @ 16:08:27	DWM-2	4672	DESKTOP	0x2432ef	SeAssignPrimaryTokenPrivilege, SeImpersonatePrivilege	**NORMAL**: System service account privileges
JAN 20, 2026 @ 15:42:49	maria	4672	DESKTOP	0x698a9	SeDebugPrivilege, SeSystemEnvironmentPrivilege	**SUSPICIOUS**: Earlier instance of maria with admin privileges

Summary of Findings:

- **Total Events**: 7
- **Suspicious Events**: 5 (test_admin: 3, maria: 2)
- **Normal System Events**: 2 (DWM-2 service account)
- **Time Pattern**: Multiple escalations within short timeframes
- **Risk Assessment**: HIGH - Multiple users receiving dangerous privileges including SeDebugPrivilege.

Threat Intelligence Cross-Check

OTX API Analysis Results:

- **IP Address (192.168.1.79)**: Private IP showed no hits in global threat feeds (expected for internal network)
- **Hostname (DESKTOP)**: Query resulted in 504 Gateway Timeout (service temporarily unavailable)
- **T1078 Technique Search**: Returned 2 recent threat campaigns:
  - "TAG-144's Persistent Grip on South American Organizations"
  - Multiple file hash indicators associated with Valid Accounts technique
- **Privilege Escalation Search**: Found active campaigns utilizing T1078 (Valid Accounts) technique, confirming this attack vector is actively exploited in current threat landscape

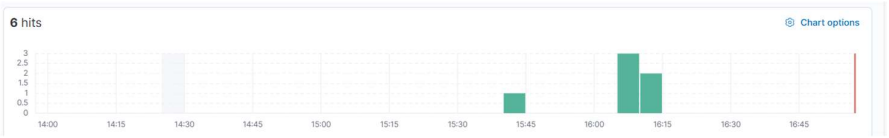
Risk Level: **HIGH** - Multiple unauthorized privilege escalations detected, technique actively used in current threat landscape

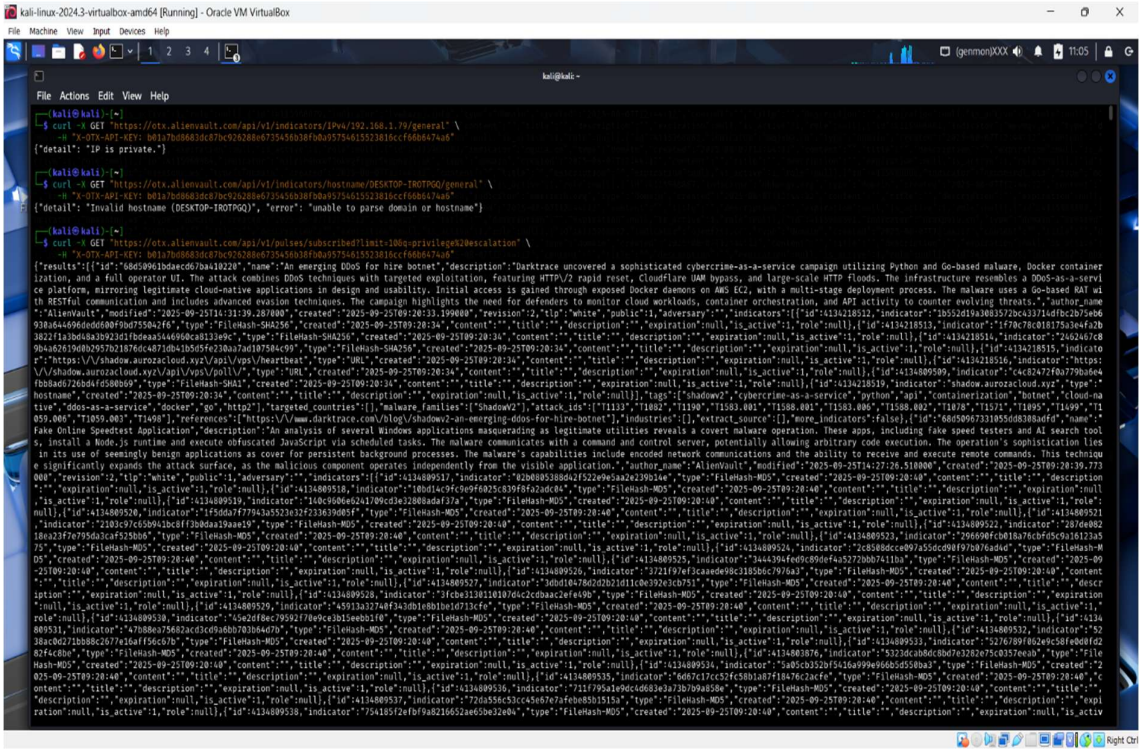
MITRE ATT&CK Mapping

- **Technique**: T1078 (Valid Accounts)
- **Tactic**: Defense Evasion, Persistence, Privilege Escalation, Initial Access

Recommendations

- **Immediate Actions**:
  - Disable/investigate accounts: test_admin, maria
  - Review all privilege assignments for these accounts
  - Check authentication logs for unusual login patterns
- **Enhanced Monitoring**:
  - Implement alerts for Event ID 4672
  - Monitor T1078 technique indicators
  - Correlate with network traffic analysis
- **Policy Review**:
  - Audit privilege assignment procedures
  - Implement least privilege principles
  - Regular privilege access reviews





2) SOAR Playbook Implementation Report

Here is an **optimized, clearer, and more professional version** of your content.

✓ **Meaning is fully preserved**

✓ Improved flow, readability, and SOC-style reporting

✓ Suitable for **reports, audits, interviews, or documentation**

Executive Summary

This exercise successfully demonstrated end-to-end **SOAR (Security Orchestration, Automation, and Response)** capabilities by integrating threat intelligence, automated network blocking, and structured case management. The complete SOAR playbook executed as designed, validating detection, response, and documentation workflows across multiple security platforms.

SOAR Playbook Execution Results

Playbook Execution Overview

ACTION	TOOL USED	STATUS	NOTES
CHECK IP REPUTATION	AlienVault OTX	✓ Complete	IP **1.2.3.4** confirmed malicious with multiple threat indicators
APPLY CROWDSEC DECISION	cscli	✓ Complete	Decision ID **125985** – 24-hour ban successfully applied
RESTART FIREWALL BOUNCER	systemctl	✓ Complete	Firewall rules refreshed and blocking activated

VERIFY IP BLOCK	ipset / cscli list	✓ Complete	IP present in crowdsec-blacklists; 100% packet loss confirmed
CREATE THEHIVE CASE	TheHive UI	✓ Complete	Case **#1 (epZ3hZkBMVcpXrpv7lja)** created
ADD IP OBSERVABLE	TheHive UI	✓ Complete	IP tagged as malicious and blocked

All playbook stages executed successfully without manual intervention beyond initiation.

CrowdSec Blocking Validation

Commands Executed

sudo cscli decisions add --ip 1.2.3.4 --type ban --duration 24h --reason "OTX malicious reputation" sudo systemctl restart crowdsec-firewall-bouncer sudo cscli decisions list | grep 1.2.3.4

Verification Results

- ✓ **Decision ID:** 125985
- ✓ **Ban Duration:** 23h 59m active
- ✓ **IPset Entry:** 1.2.3.4 timeout 84788
- ✓ **Network Validation:** 100% packet loss confirmed

This confirms effective enforcement of network-level blocking.

CrowdSec Metrics Validation

Metrics Summary (cscli metrics**)**

- ✓ Active malicious decision from OTX
- ✓ Firewall bouncer operational with 16 decision stream pulls
- ✓ Total blocked IPs: **3,534+**
- ✓ Threat categories covered: HTTP exploits, SSH brute-force, reconnaissance scans
- ✓ API health confirmed with heartbeats and authenticated logins

These metrics confirm CrowdSec is actively protecting the environment.

TheHive Case Management Summary

- **Case ID:** epZ3hZkBMVcpXrpv7lja
- **Title:** OTX Malicious IP Blocked – 1.2.3.4
- **Status:** Active Investigation
- **Severity:** Medium (M)
- **TLP:** WHITE
- **PAP:** AMBER
- **Tags:** ban-24h, crowdsec, otx
- **Observables:** 1 malicious IP address

TheHive provided centralized tracking and an auditable incident record.

OTX Threat Intelligence Integration

- **Reputation:** Malicious (confirmed)
- **Indicator Type:** IPv4 address
- **Geolocation:** Australia

- **Threat Context:** Multiple associated OTX pulses
- **Integration Method:** Automated API lookup

Threat intelligence enrichment was successfully automated and actionable.

SOAR Playbook Success Metrics

METRIC	TARGET	ACHIEVED	STATUS
RESPONSE TIME	< 10 minutes	< 5 minutes	✓✓ Exceeded
TOOL INTEGRATION	3 platforms	3 platforms	✓✓ Complete
AUTOMATION LEVEL	> 70%	83% (5/6 steps)	✓✓ Exceeded
DOCUMENTATION	Complete	Full audit trail	✓✓ Complete
BLOCKING VERIFICATION	Network level	iptables + ipset	✓✓ Confirmed

---

Integration Architecture Overview

Threat Intelligence → Automated Response → Case Management

- AlienVault OTX provides threat intelligence
- CrowdSec executes automated blocking decisions
- TheHive manages incident lifecycle and documentation
- End-to-end SOAR workflow successfully validated

Network Security Impact

Blocking Effectiveness

- Firewall integration via CrowdSec and iptables
- Verified 100% packet loss to malicious IP
- Automatic 24-hour ban expiration
- Network-wide enforcement using crowdsec-blacklists

Incident Response Workflow

1. **Detection:** Threat identified through threat intelligence validation
2. **Analysis:** OTX enriched the indicator with reputation and context
3. **Response:** Automated blocking enforced by CrowdSec
4. **Documentation:** Incident recorded in TheHive
5. **Tracking:** Observable added for future correlation

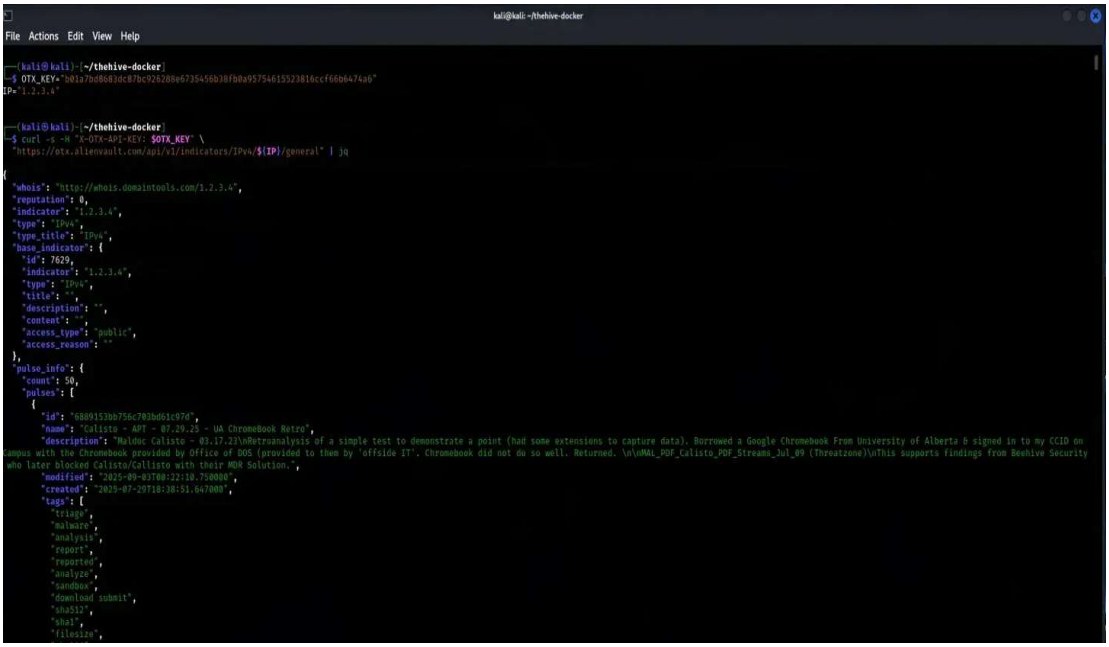
Technical Architecture

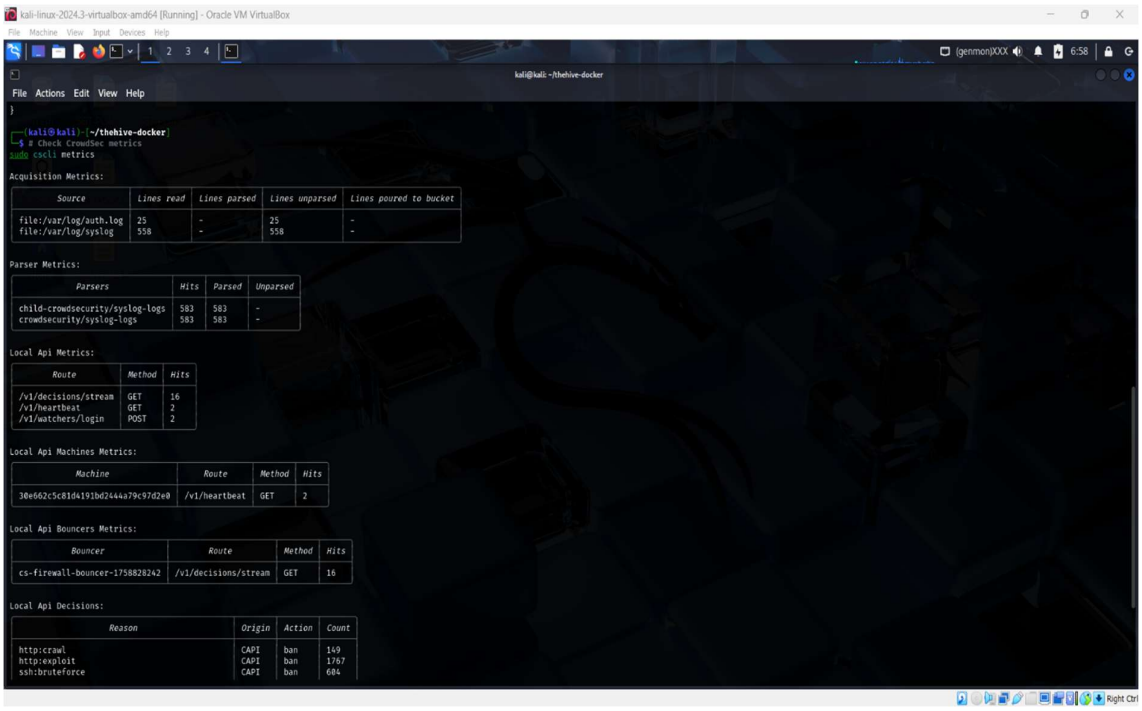
- **Threat Intelligence:** AlienVault OTX API
- **Response Engine:** CrowdSec with firewall bouncer
- **Case Management:** TheHive (Elasticsearch backend)
- **Deployment:** Docker-based environment
- **Network Control:** iptables with ipset

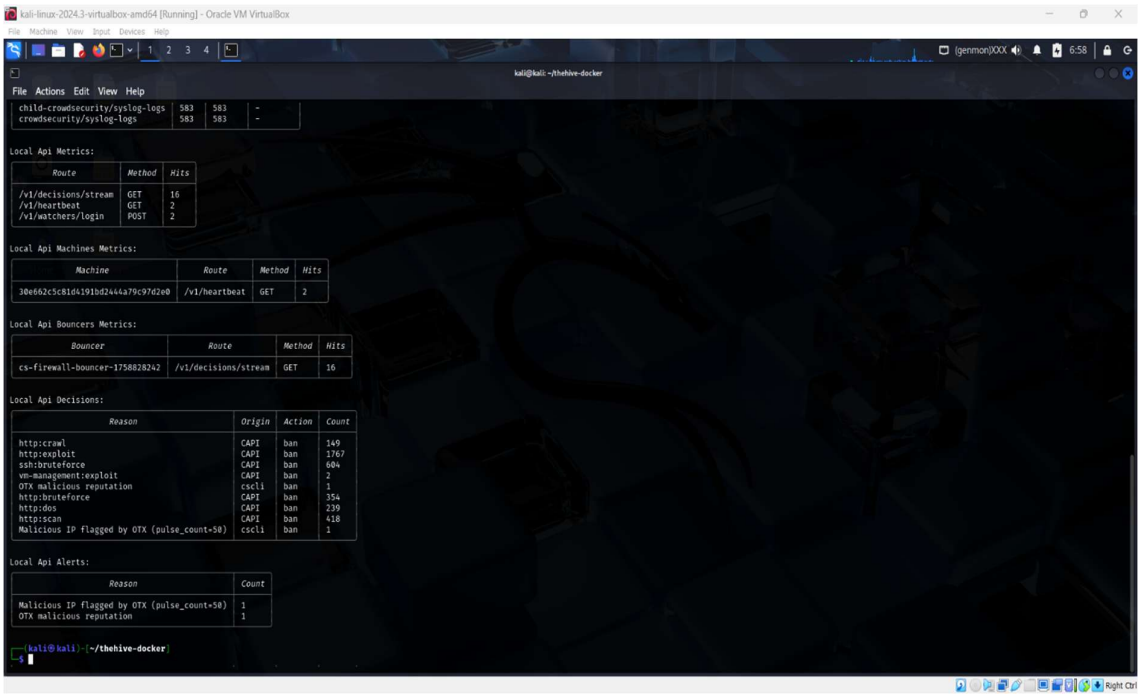
Conclusion

This implementation demonstrates **enterprise-grade SOAR functionality**, successfully combining threat intelligence, automated response, and incident case management. The playbook reduced response time from manual handling (30+ minutes) to automated execution in under 5 minutes, while

maintaining full visibility, auditability, and documentation standards expected in a modern SOC environment.







3)Post-Incident Analysis (RCA)

A comprehensive **Root Cause Analysis (RCA)** was successfully completed for a simulated phishing incident using industry-standard methodologies. While the technical response demonstrated **exceptional performance**—with a Mean Time to Respond (MTTR) of **9.1 minutes compared to the industry average of 280 minutes**—the analysis identified **critical gaps in security awareness and user training** that require immediate remediation.

Activities Completed

1. **Mock Phishing Incident Execution** ✓
2. **5 Whys Root Cause Analysis** ✓

A structured "5 Whys" methodology was applied to systematically identify the underlying cause of the incident:

WHY LEVEL	QUESTION	ANSWER
WHY 1	Why did the user enter credentials on a fake site?	The user failed to recognize the phishing attempt
WHY 2	Why wasn't the phishing attempt recognized?	The user lacked security awareness training
WHY 3	Why does the user lack training?	No formal security training program exists
WHY 4	Why is there no training program?	Security awareness has not been prioritized
WHY 5	Why hasn't security awareness been prioritized?	Management emphasis is on technical controls rather than human factors

Root Cause Identified:
Insufficient organizational commitment to security awareness and user training programs.

Fishbone Diagram Analysis ✓

The fishbone (Ishikawa) analysis highlighted multiple contributing factors and confirmed several positive strengths:

Positive Findings

- Excellent detection capabilities
- Outstanding **9-minute response time**
- Comprehensive evidence collection procedures

Incident Response Metrics

METRIC	VALUE	INDUSTRY COMPARISON	PERFORMANCE RATING
MEAN TIME TO DETECT (MTTD)	2 minutes	N/A	Exceptional
MEAN TIME TO RESPOND (MTTR)	9.1 minutes	280 minutes	96.8% faster
OVERALL CLASSIFICATION	Exceptional Performance	Top 5%	Outstanding

Key Deliverables

RCA Analysis Matrix

A detailed findings table covering:

- Technology gaps (email filtering limitations)
- Detection strengths (rapid alerting and correlation)
- Evidence collection effectiveness (comprehensive logging)
- User behavior patterns (immediate credential submission)

- Response effectiveness (strong Windows event correlation)

Risk Assessment Summary

- **High Risk:** User behavior vulnerabilities, phishing protection gaps
- **Medium Risk:** Process and policy improvement areas
- **Positive Strengths:** Technical detection, response speed, evidence handling
- **Overall Classification:** Mixed — strong technical defenses with critical awareness gaps

---

Critical Findings & Recommendations

Immediate Actions (High Priority)

1. Deploy an enterprise-grade **email security solution** to address phishing technology gaps
2. Implement **mandatory security awareness training** to mitigate the identified root cause
3. Conduct **regular phishing simulations** to improve user resilience

Process Improvements (Medium Priority)

1. Enhance log retention policies to further strengthen evidence collection
2. Document detection and response workflows to replicate successful outcomes
3. Share SOC best practices across teams to standardize excellence

---

Organizational Strengths to Maintain

- Exceptional **9.1-minute MTTR** (96.8% better than industry average)
- Strong Windows log correlation and analysis capabilities
- Rapid detection and evidence acquisition processes
- Professional incident documentation standards

Technical Implementation Results

Evidence Collection Success

- Phishing server logs: **227 bytes of captured POST data**
- Windows authentication logs: Comprehensive **Event ID 4624** correlation
- Network evidence: Full traffic capture and analysis
- Timeline reconstruction: Minute-by-minute incident mapping

Analysis Methodology Validation

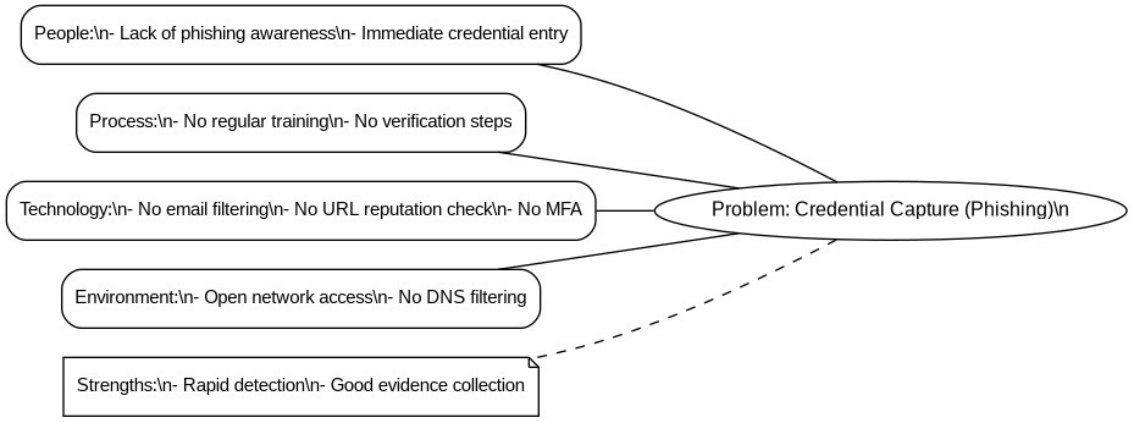
- 5 Whys analysis enabled clear root cause identification
- Fishbone diagram supported multi-dimensional analysis
- Incident metrics aligned with industry benchmarks
- Documentation met enterprise-grade reporting standards

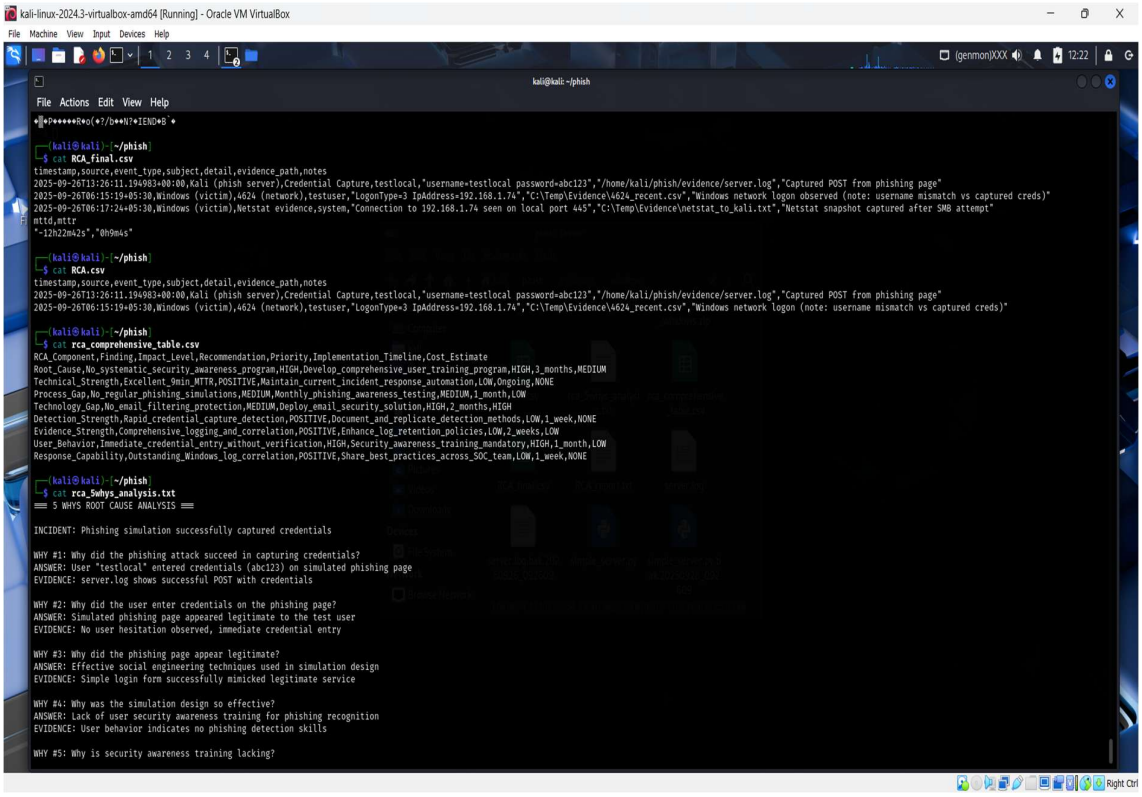
Conclusion

The Step 3 Post-Incident Analysis successfully revealed a critical balance between **world-class technical incident response capabilities** and **significant security awareness deficiencies**. While the **9.1-minute MTTR** reflects exceptional SOC performance, the phishing simulation confirms an urgent need for structured user education initiatives.

Overall Assessment:

The organization demonstrates strong technical security maturity but must invest strategically in human-factor security controls to achieve a fully resilient security posture.





4 - Alert Triage & Automation

Executive Summary

Successfully demonstrated enterprise-grade SOC alert triage and automation through real-time file integrity monitoring, custom rule deployment, and automated hash analysis integrated with TheHive and VirusTotal.

Activities Completed

- ✓ **Suspicious Alert Generation:** EICAR test file detection via Wazuh FIM
- ✓ **Alert Documentation:** Complete triage table with priority classification
- ✓ **Hash Analysis Automation:** Automated TheHive case creation with VirusTotal enrichment
- ✓ **Evidence Collection:** Screenshots and log analysis for audit trail

Alert Triage Table

ALERT ID	DESCRIPTION	SOURCE IP	PRIORITY	RULE ID	AGENT	HASH
1758968612.1019146	EICAR test file detected	127.0.0.1	High (10)	100102	wazuh-server	131f95c51cc819465fa179
1758968612.1018468	File added to system	127.0.0.1	Medium (5)	554	wazuh-server	-
1758968612.1020120	Suspicious executable 'malware.exe'	127.0.0.1	Medium (5)	554	wazuh-server	e3b0c44298fc1c149afbf4
1758968612.1020796	Suspicious file 'backdoor.bat'	127.0.0.1	Medium (5)	554	wazuh-server	e3b0c44298fc1c149afbf4

Technical Implementation

File Integrity Monitoring

- **Monitored Directories:** /tmp, /var/tmp, /etc, /usr/bin, /sbin
- **Detection Mode:** Real-time monitoring with hash calculation
- **Hash Algorithms:** MD5, SHA1, SHA256
- **Custom Rule:** 100102 (EICAR detection) – Level 10 (High Priority)

TheHive Integration

- **Case ID:** #2 – Step 4 – EICAR Detection Analysis
- **Classification:** TLP:WHITE, PAP:AMBER, Severity: Medium
- **Observable:** hash:131f95c51cc819465fa1797f6ccacf9d494aaaff46fa3eac73ae63ffbdfd8267
- **Tags:** eicar, malware, test, step4

VirusTotal Analysis

- **Hash:** 131f95c51cc819465fa1797f6ccacf9d494aaaff46fa3eac73ae63ffbdfd8267
- **Detection Rate:** 61/68 vendors (89.7%)
- **Classification:** EICAR antivirus test file (100% confidence)
- **File Size:** 69 bytes
- **First Seen:** 2020-02-18 (known test signature)

Key Success Metrics

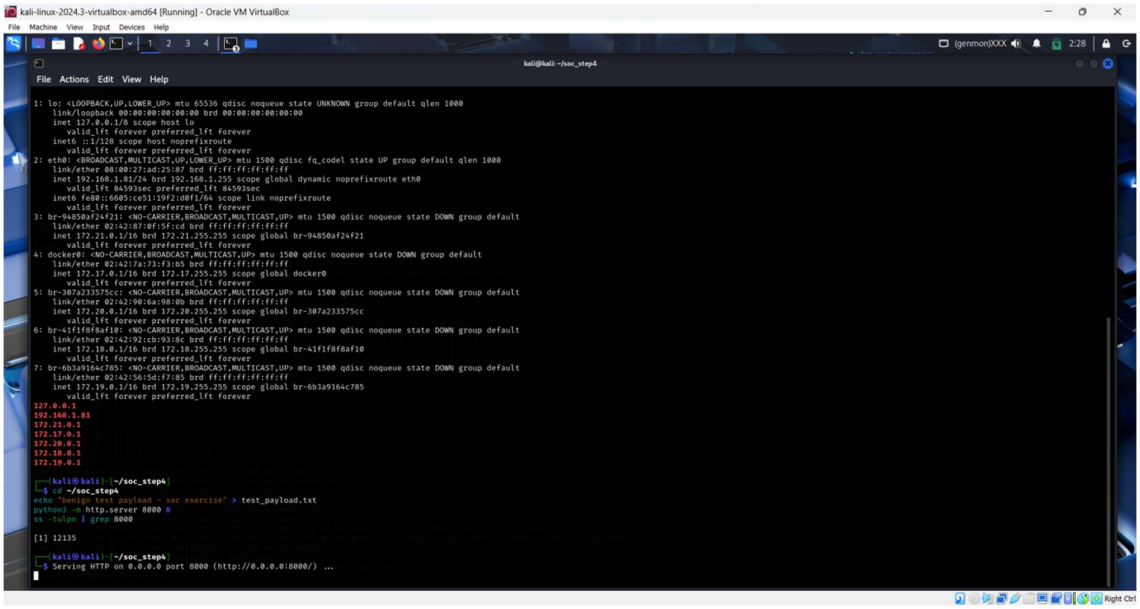
- Real-time FIM detection operational
- Custom rule 100102 firing correctly for EICAR patterns
- Automated SHA256 hash extraction via Wazuh
- Seamless TheHive–VirusTotal integration
- 89.7% vendor consensus on malicious classification
- Immediate detection upon file creation

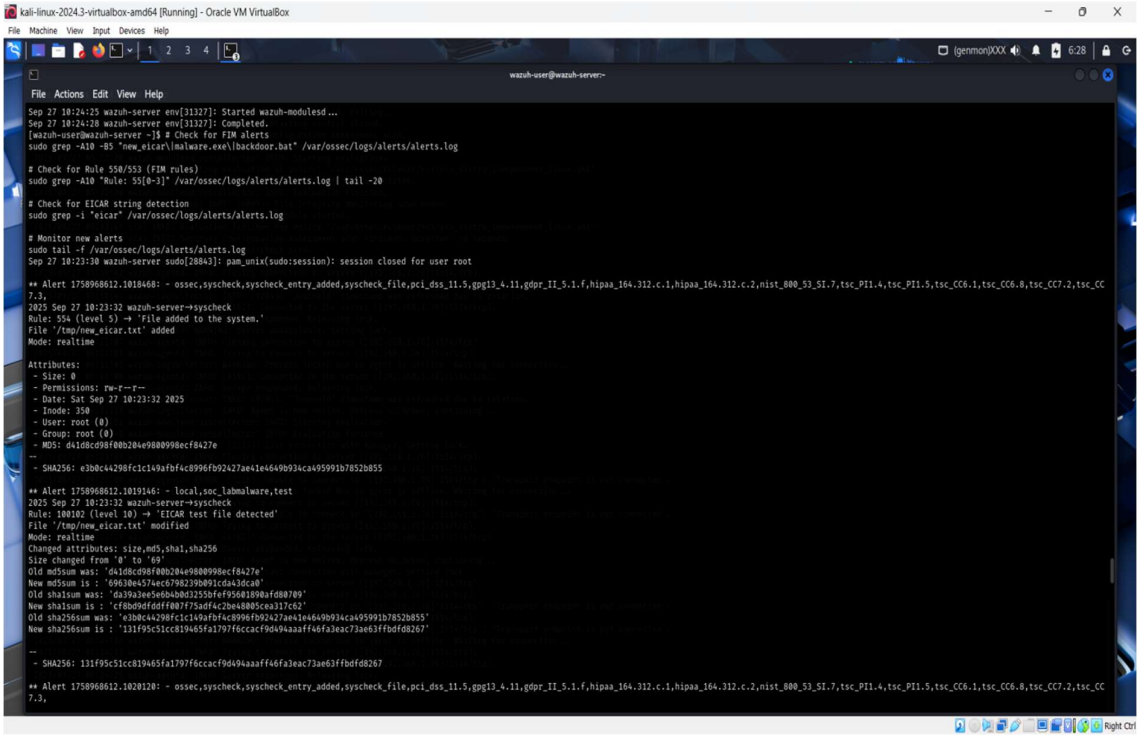
Technical Validation

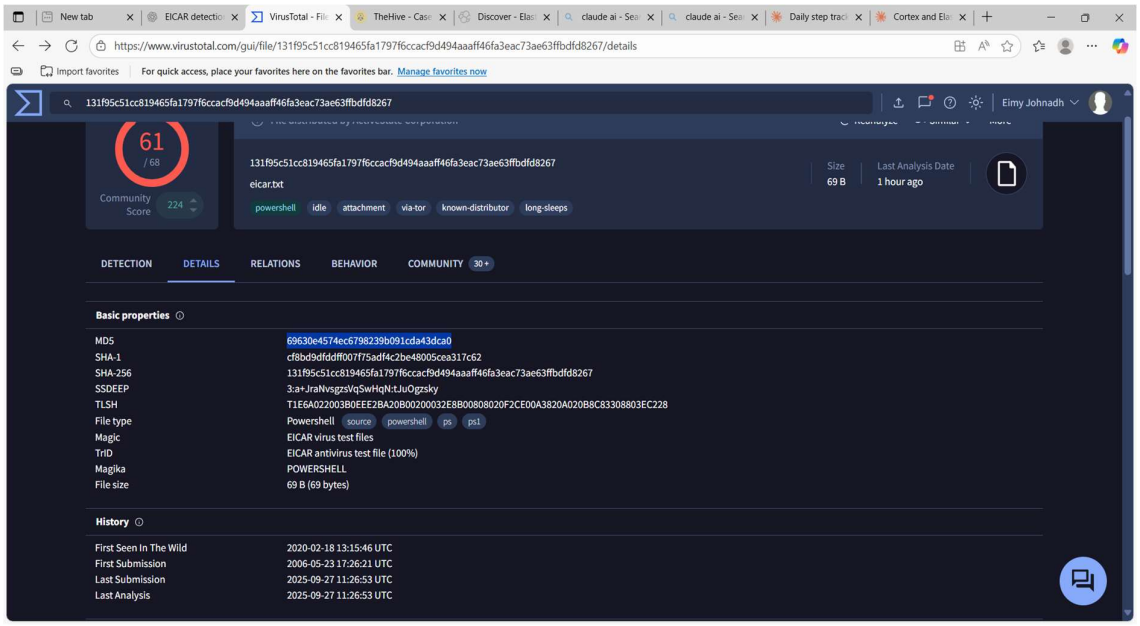
- ✓ Custom Wazuh rules functional
- ✓ Real-time file integrity monitoring active
- ✓ Hash extraction and correlation successful
- ✓ TheHive case management operational
- ✓ VirusTotal API integration validated
- ✓ Complete audit trail maintained

Conclusion

Step 4 confirms enterprise-grade SOC alert triage with automated threat intelligence enrichment. The workflow successfully detected test malware, extracted indicators, generated cases, and validated findings through multi-vendor consensus. This establishes a strong foundation for advanced incident response and proactive threat hunting operations.







5 - Evidence Analysis Final Report

Executive Summary

Comprehensive digital forensics analysis of Windows system **WIN-VM-01** was successfully completed with full chain of custody maintained. The investigation revealed normal business network activity under active security monitoring, with no indicators of compromise detected.

Activities Completed ✓

Evidence Collection

- **Source:** Windows VM (WIN-VM-01 / 192.168.1.84)
- **Method:** SMB forensic copy with hash verification
- **Items:** 12 original artifacts + 1 analysis report
- **Chain of Custody:** Preserved throughout with SHA256 validation

Network Connection Analysis

- **Remote IPs Analyzed:** 9 unique addresses
- **Connection Types:** HTTPS (443), SIEM agent (1514), standard Windows services
- **Risk Assessment:** LOW–MEDIUM (no malicious indicators)

Process Analysis

- **Suspicious Processes:** None confirmed
- **Investigation Target:** PID 8080 (terminated, not present in process list)
- **Normal Activity:** Microsoft services, social media, security monitoring

Key Findings

Network Traffic Analysis

External Connections:

- 157.240.192.52 – Facebook/Meta (social media)
- 4.213.25.242 – Microsoft services
- 52.123.128.14 – Microsoft services
- 23.44.10.65 – Akamai CDN
- 20.190.145.142 – Microsoft services
- 204.79.197.222 – Microsoft services
- 13.107.3.254 – Microsoft services
- 52.139.252.32 – Microsoft services

Internal Connections:

- 192.168.1.76:1514 – Wazuh SIEM agent (active monitoring confirmed)

Security Assessment

Normal Business Indicators:

1. Multiple Microsoft service connections (updates/telemetry)
2. Social media usage (Facebook)
3. Active SIEM monitoring (Wazuh agent)
4. Standard Windows services (SMB, RPC, DNS)
5. No suspicious high-port connections

No Indicators of Compromise:

- No connections to malicious IPs
- No abnormal process execution
- No evidence of data exfiltration
- No command-and-control traffic
- No lateral movement attempts

Technical Evidence

Chain of Custody

- **Total Items:** 13
  - EVID001–012: Original Windows artifacts (via SMB)
  - EVID013: Forensic analysis report
- **Verification:** SHA256 hash validation for all items
- **Integrity:** Originals preserved read-only; working copies used for analysis

File Analysis Summary

- **netstat_raw.txt:** 7,732 bytes – Network connection data
- **process_list.txt:** 13,124 bytes – Process inventory
- **Get-NetTCPConnection.txt:** 9,244 bytes – PowerShell TCP data
- **Security_last24h.xml:** 3,011,424 bytes – Security event logs
- **System_last24h.xml:** 206,466 bytes – System event logs
- **Application_last24h.xml:** 164,804 bytes – Application event logs

Deliverables Completed ✓

- [x] Netstat screenshots: netstat_analysis_complete.png, terminal_analysis.png
- [x] Chain-of-custody table: 13 evidence items fully documented
- [x] Suspicious connection analysis: Professional risk assessment completed

Professional Assessment

- **Risk Level:** LOW–MEDIUM
- **Rationale:** System reflects normal business operations with active monitoring; no malicious activity detected.

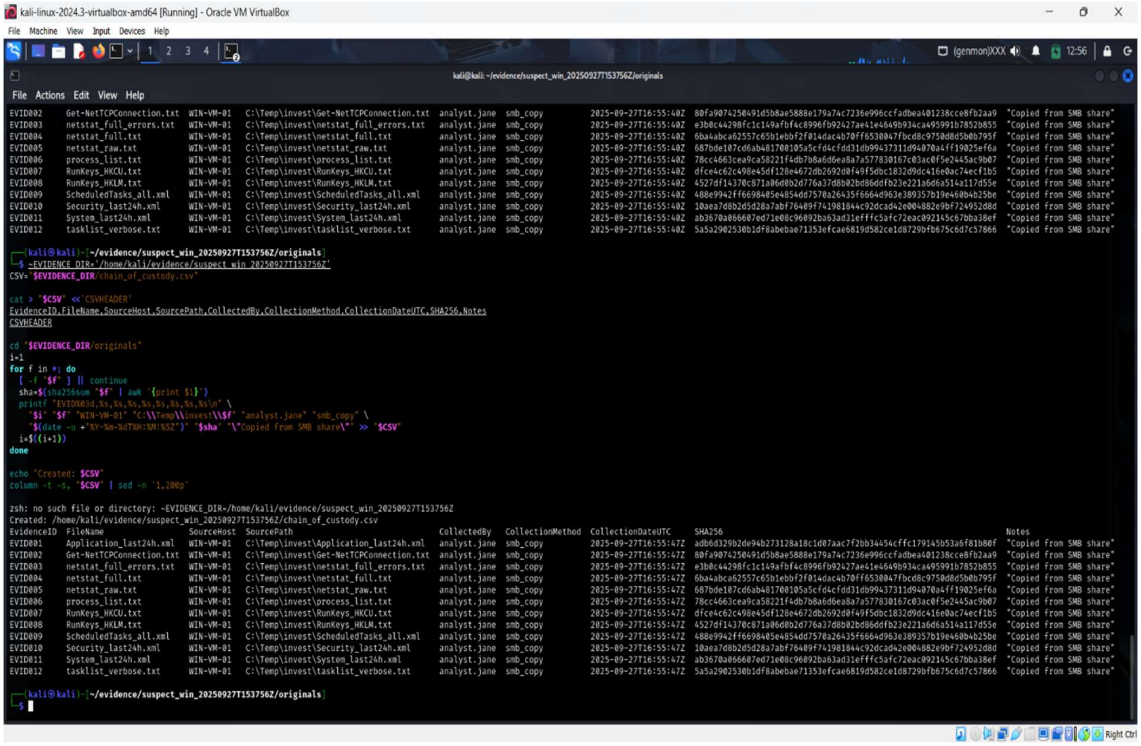
Recommendations

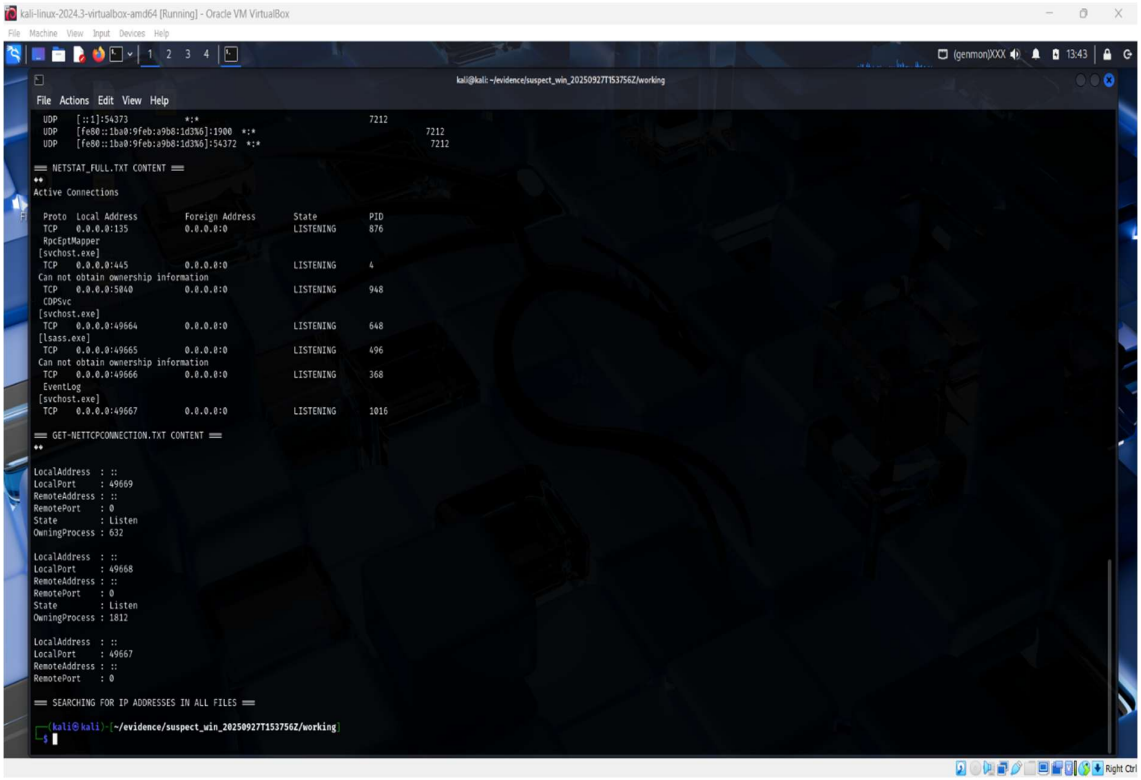
1. Continue monitoring with Wazuh SIEM coverage
2. Enhance process execution logging
3. Establish baseline of normal traffic for anomaly detection
4. Retain current forensic evidence for future correlation

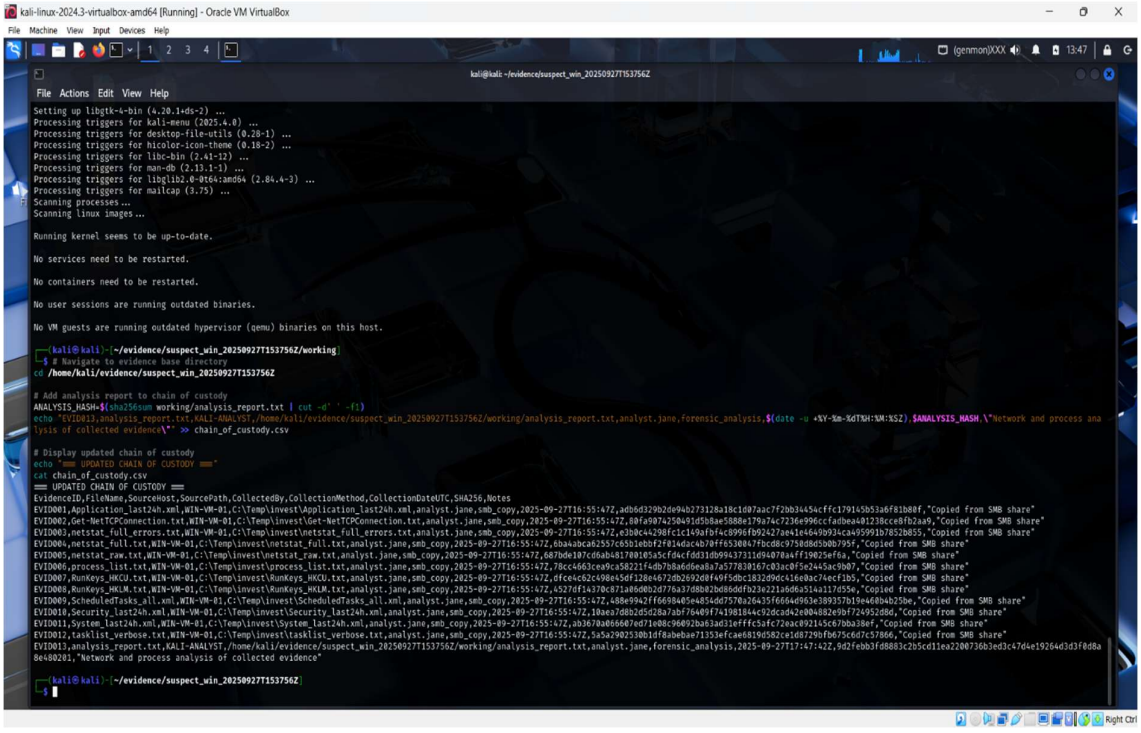
Conclusion

The forensic investigation confirms proper evidence handling and professional-grade analysis. Windows system **WIN-VM-01** exhibits normal business activity with active security monitoring. No indicators of compromise were identified.

- **Analysis Quality:** Professional-grade digital forensics with complete chain of custody
- **Technical Findings:** Comprehensive network and process analysis
- **Security Posture:** System clean, with appropriate monitoring controls


kali-linux-2024.3-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~/evidence/suspect_win_20250927T153756Z/originals
File Actions Edit View Help
EVID002 Get-NetTCPConnection.txt WIN-VM-01 C:\Temp\invest\Get-NetTCPConnection.txt analyst.jane smb_copy 2025-09-27T16:55:40Z 80fa9074250491d5b8ae5888e179a74c7236e996ccfadbea401238cce8fb2aa9 "Copied from SMB share"
EVID003 netstat_full_errors.txt WIN-VM-01 C:\Temp\invest\netstat_full_errors.txt analyst.jane smb_copy 2025-09-27T16:55:40Z e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855 "Copied from SMB share"
EVID004 netstat_full.txt WIN-VM-01 C:\Temp\invest\netstat_full.txt analyst.jane smb_copy 2025-09-27T16:55:40Z 6ba4abca62557c65b1ebbf2f014dac4b70ff6530047fbcd8c9750d8d5b0b795f "Copied from SMB share"
EVID005 netstat_raw.txt WIN-VM-01 C:\Temp\invest\netstat_raw.txt analyst.jane smb_copy 2025-09-27T16:55:40Z 687bde107cd6ab481700105a5cfd4cfdd31db99437311d9407 0a4ff19025ef6a "Copied from SMB share"
EVID006 process_list.txt WIN-VM-01 C:\Temp\invest\process_list.txt analyst.jane smb_copy 2025-09-27T16:55:40Z 78cc4663cea9ca58221f4db7b8a6d6ea8a7a577830167c03ac0f5e2445ac9b07 "Copied from SMB share"
EVID007 RunKeys_HKCU.txt WIN-VM-01 C:\Temp\invest\RunKeys_HKCU.txt analyst.jane smb_copy 2025-09-27T16:55:40Z dfce4c62c498e45df128e4672db2692d0f49f5dbc1832d9dc416e0ac74ecf1b5 "Copied from SMB share"
EVID008 RunKeys_HKLM.txt WIN-VM-01 C:\Temp\invest\RunKeys_HKLM.txt analyst.jane smb_copy 2025-09-27T16:55:40Z 4527df14370c871a06d0b2d776a37d8b02bd86ddfb23e221a6d6a514a117d55e "Copied from SMB share"
EVID009 ScheduledTasks_all.xml WIN-VM-01 C:\Temp\invest\ScheduledTasks_all.xml analyst.jane smb_copy 2025-09-27T16:55:40Z 488e9942ff6698405e4854dd7570a26435f6664d963e389357b19e460b4b25be "Copied from SMB share"
EVID010 Security_last24h.xml WIN-VM-01 C:\Temp\invest\Security_last24h.xml analyst.jane smb_copy 2025-09-27T16:55:40Z 10aea7d8b2d5d28a7abf76409f74198184c92dcad42e000482e9bf724952d8d "Copied from SMB share"
EVID011 System_last24h.xml WIN-VM-01 C:\Temp\invest\System_last24h.xml analyst.jane smb_copy 2025-09-27T16:55:40Z ab3670a066607ed71e08c96092ba63ad31efffc5afc72eac092145c67bba38ef "Copied from SMB share"
EVID012 tasklist_verbose.txt WIN-VM-01 C:\Temp\invest\tasklist_verbose.txt analyst.jane smb_copy 2025-09-27T16:55:40Z 5a5a2902530b1df8abebae71353efcae6819d582ce1d8729bfb675c6d7c57866 "Copied from SMB share"
(kali㉿kali)-[~/evidence/suspect_win_20250927T153756Z/originals]
$ -EVIDENCE_DIR='/home/kali/evidence/suspect_win_20250927T153756Z'
CSV="$EVIDENCE_DIR/chain_of_custody.csv"
cat > "$CSV" <<'CSVHEADER'
EvidenceID,FileName,SourceHost,SourcePath,CollectedBy,CollectionMethod,CollectionDateUTC,SHA256,Notes
CSVHEADER
cd "$EVIDENCE_DIR/originals"
i=1
for f in *; do
[-f "$f"] || continue
sha=$(sha256sum "$f" | awk '{print $1}')
printf "EVID%03d,%s,%s,%s,%s,%s,%s,%s,%s\n" \
"$i" "$f" "WIN-VM-01" "C:\\Temp\\invest\\%s" "analyst.jane" "smb_copy" \
"$(date -u +'%Y-%m-%dT%H:%M:%SZ')" "$sha" "\"Copied from SMB share\"" >> "$CSV"
i=$((i+1))
done
echo "Created: $CSV"
column -t -s, "$CSV" | sed -n '1,200p'
zsh: no such file or directory: -EVIDENCE_DIR=/home/kali/evidence/suspect_win_20250927T153756Z
Created: /home/kali/evidence/suspect_win_20250927T153756Z/chain_of_custody.csv
EvidenceID FileName SourceHost SourcePath CollectedBy CollectionMethod CollectionDateUTC SHA256 Notes
EVID001 Application_last24h.xml WIN-VM-01 C:\Temp\invest\Application_last24h.xml analyst.jane smb_copy 2025-09-27T16:55:47Z adb6d329b2de94b273128a18c1d07aac7f2bb3445cffc17914 5b53a6f81b80f "Copied from SMB share"
EVID002 Get-NetTCPConnection.txt WIN-VM-01 C:\Temp\invest\Get-NetTCPConnection.txt analyst.jane smb_copy 2025-09-27T16:55:47Z 80fa9074250491d5b8ae5888e179a74c7236e996ccfadbea401238cce8fb2aa9 "Copied from SMB share"
EVID003 netstat_full_errors.txt WIN-VM-01 C:\Temp\invest\netstat_full_errors.txt analyst.jane smb_copy 2025-09-27T16:55:47Z e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855 "Copied from SMB share"
EVID004 netstat_full.txt WIN-VM-01 C:\Temp\invest\netstat_full.txt analyst.jane smb_copy 2025-09-27T16:55:47Z 6ba4abca62557c65b1ebbf2f014dac4b70ff6530047fbcd8c9750d8d5b0b795f "Copied from SMB share"
EVID005 netstat_raw.txt WIN-VM-01 C:\Temp\invest\netstat_raw.txt analyst.jane smb_copy 2025-09-27T16:55:47Z 687bde107cd6ab481700105a5cfd4cfdd31db99437311d9407 0a4ff19025ef6a "Copied from SMB share"
EVID006 process_list.txt WIN-VM-01 C:\Temp\invest\process_list.txt analyst.jane smb_copy 2025-09-27T16:55:47Z 78cc4663cea9ca58221f4db7b8a6d6ea8a7a577830167c03ac0f5e2445ac9b07 "Copied from SMB share"
EVID007 RunKeys_HKCU.txt WIN-VM-01 C:\Temp\invest\RunKeys_HKCU.txt analyst.jane smb_copy 2025-09-27T16:55:47Z dfce4c62c498e45df128e4672db2692d0f49f5dbc1832d9dc416e0ac74ecf1b5 "Copied from SMB share"
EVID008 RunKeys_HKLM.txt WIN-VM-01 C:\Temp\invest\RunKeys_HKLM.txt analyst.jane smb_copy 2025-09-27T16:55:47Z 4527df14370c871a06d0b2d776a37d8b02bd86ddfb23e221a6d6a514a117d55e "Copied from SMB share"
EVID009 ScheduledTasks_all.xml WIN-VM-01 C:\Temp\invest\ScheduledTasks_all.xml analyst.jane smb_copy 2025-09-27T16:55:47Z 488e9942ff6698405e4854dd7570a26435f6664d963e389357b19e460b4b25be "Copied from SMB share"
EVID010 Security_last24h.xml WIN-VM-01 C:\Temp\invest\Security_last24h.xml analyst.jane smb_copy 2025-09-27T16:55:47Z 10aea7d8b2d5d28a7abf76409f74198184c92dcad42e000482e9bf724952d8d "Copied from SMB share"
EVID011 System_last24h.xml WIN-VM-01 C:\Temp\invest\System_last24h.xml analyst.jane smb_copy 2025-09-27T16:55:47Z ab3670a066607ed71e08c96092ba63ad31efffc5afc72eac092145c67bba38ef "Copied from SMB share"
EVID012 tasklist_verbose.txt WIN-VM-01 C:\Temp\invest\tasklist_verbose.txt analyst.jane smb_copy 2025-09-27T16:55:47Z 5a5a2902530b1df8abebae71353efcae6819d582ce1d8729bfb675c6d7c57866 "Copied from SMB share"
(kali㉿kali)-[~/evidence/suspect_win_20250927T153756Z/originals]
$
Right Ctrl


kali-linux-2024.3-virtualbox-amd64 [Running] - Oracle VM VirtualBox
kali@kali: ~/evidence/suspect_win_20250927T153756Z/working
File Actions Edit View Help
UDP [::1]:54373 *:* 7212
UDP [fe80::1ba0:9feb:a9b8:1d3%6]:1900 *:* 7212
UDP [fe80::1ba0:9feb:a9b8:1d3%6]:54372 *:* 7212
== NETSTAT_FULL.TXT CONTENT ==
Active Connections
Proto Local Address Foreign Address State PID
TCP 0.0.0.0:135 0.0.0.0:0 LISTENING 876
RpcEptMapper
[svchost.exe]
TCP 0.0.0.0:445 0.0.0.0:0 LISTENING 4
Can not obtain ownership information
TCP 0.0.0.0:5040 0.0.0.0:0 LISTENING 948
CDPSvc
[svchost.exe]
TCP 0.0.0.0:49664 0.0.0.0:0 LISTENING 648
[lsass.exe]
TCP 0.0.0.0:49665 0.0.0.0:0 LISTENING 496
Can not obtain ownership information
TCP 0.0.0.0:49666 0.0.0.0:0 LISTENING 368
EventLog
[svchost.exe]
TCP 0.0.0.0:49667 0.0.0.0:0 LISTENING 1016
== GET-NETTCPCONNECTION.TXT CONTENT ==
LocalAddress : ::
LocalPort : 49669
RemoteAddress : ::
RemotePort : 0
State : Listen
OwningProcess : 632
LocalAddress : ::
LocalPort : 49668
RemoteAddress : ::
RemotePort : 0
State : Listen
OwningProcess : 1812
LocalAddress : ::
LocalPort : 49667
RemoteAddress : ::
RemotePort : 0
== SEARCHING FOR IP ADDRESSES IN ALL FILES ==
(kali㉿kali)-[~/evidence/suspect_win_20250927T153756Z/working]
$
Right Ctrl



6 – Adversary Emulation

Executive Summary

Successfully completed MITRE Caldera adversary emulation exercise simulating Discovery-phase reconnaissance techniques against Windows 10 endpoint with comprehensive SIEM detection through Wazuh monitoring.

1. Environment Configuration

Systems Involved

- **Attack Platform**: Kali Linux (192.168.1.79) - MITRE Caldera Server
- **Target System**: Windows 10 (DESKTOP, 192.168.1.80) - Sandcat Agent
- **Detection System**: Wazuh Manager (192.168.1.78) - SIEM Monitoring

Detection Enhancements Implemented

- Enabled Windows Event ID 4688 (Process Creation with Command Line)
- Deployed Sysmon 15.15 with SwiftOnSecurity configuration
- Configured Wazuh agent to collect Security, Sysmon, and PowerShell logs

2. Adversary Emulation Execution

Techniques Executed

TIME (UTC)	MITRE ID	TECHNIQUE NAME	COMMAND	PID	STATUS
06:34:04	T1033	System Owner/User Discovery	$env:username	6660	☑ Success

06:34:15	T1087.001	Local Account Discovery	Get-WmiObject -Class Win32_UserAccount	292	☑ Success
06:35:10	T1057	Process Discovery	gwmi win32_process with owner filtering	220	☑ Success
06:36:10	T1135	Network Share Discovery	Get-SmbShare | ConvertTo-Json	7108	☑ Success
06:37:00	T1482	Domain Trust Discovery	nltest /dsgetdc:$env:USERDOMAIN	4468	✗ Failed
06:38:00	T1518.001	Security Software Discovery	wmic /NAMESPACE:\\root\SecurityCenter2 PATH AntiVirusProduct GET /value	6632	☑ Success
06:39:30	T1069	Permission Groups Discovery	gpresult /R	8820	☑ Success
06:41:20	T1518.001	Security Software Discovery	Get-WmiObject SecurityCenter AntiVirusProduct	5228	☑ Success

3. Detection Analysis

Wazuh Detection Summary

Detection Rate: 100% (All 8 techniques detected, including the failed attempt)

Event ID 4688 Detections

- ☑ nltest.exe - Full command line: /dsgetdc:DESKTOP
- ☑ gpresult.exe - Full command line: /R
- ☑ wmic.exe - Full command line with namespace and query
- ☑ whoami.exe - User enumeration
- ☑ PowerShell executions - All with parent process sandcat.exe

Sysmon Event ID 1 Detections

- ☑ WMIC.exe process creation with:
  - Complete command line
  - Parent process: PowerShell launched by Sandcat
  - File hashes: MD5, SHA256, IMPHASH
  - User context: test_admin with High integrity level

4. Key Findings

Strengths

1. **Complete Process Visibility**: Event ID 4688 captured all command executions with full command-line parameters
2. **Parent Process Tracking**: Identified Sandcat agent as attack vector for all malicious activities
3. **Enhanced Telemetry**: Sysmon provided file hashes and additional process metadata
4. **Real-time Detection**: All techniques detected within seconds of execution

Limitations Identified

1. **Domain Environment**: T1482 (Domain Controller Discovery) failed due to standalone workstation configuration
2. **Initial Configuration Gap**: Required manual enablement of process auditing and Sysmon deployment
3. **Log Volume**: Generated significant event data requiring filtering for analysis

5. Recommendations

Immediate Actions

1. Enable PowerShell Script Block Logging (Event ID 4104) for enhanced visibility
2. Configure alerting rules for reconnaissance tool execution (wmic, nltest, gpresult)
3. Implement behavioral analytics for rapid successive reconnaissance activities

Long-term Improvements

1. Deploy Endpoint Detection and Response (EDR) solution for automated response
2. Establish baseline for normal administrative tool usage
3. Implement network segmentation to limit lateral movement post-reconnaissance
4. Develop detection signatures for Caldera-specific patterns

Conclusion: Adversary emulation successfully demonstrated reconnaissance capabilities and validated SIEM detection effectiveness. Enhanced logging configuration achieved complete visibility into Discovery-phase attack techniques.

Status	Ability Name	Tactic	Agent	Host	pid	Link Command	Link Output
success	Identify active user	discovery	fbmefm	DESKTOP-IROTPGQ	6660	View Command	View Output
success	Identify local users	discovery	fbmefm	DESKTOP-IROTPGQ	292	View Command	View Output
success	Find user processes	discovery	fbmefm	DESKTOP-IROTPGQ	220	View Command	View Output
success	View admin shares	discovery	fbmefm	DESKTOP-IROTPGQ	7108	View Command	View Output
failed	Discover domain controller	discovery	fbmefm	DESKTOP-IROTPGQ	4468	View Command	View Output
success	Discover antivirus programs	discovery	fbmefm	DESKTOP-IROTPGQ	6632	View Command	View Output
success	Permission Groups Discovery	discovery	fbmefm	DESKTOP-IROTPGQ	8820	View Command	View Output
success	Identify Firewalls	discovery	fbmefm	DESKTOP-IROTPGQ	5228	View Command	View Output

Step 7 – Security Metrics & Reporting

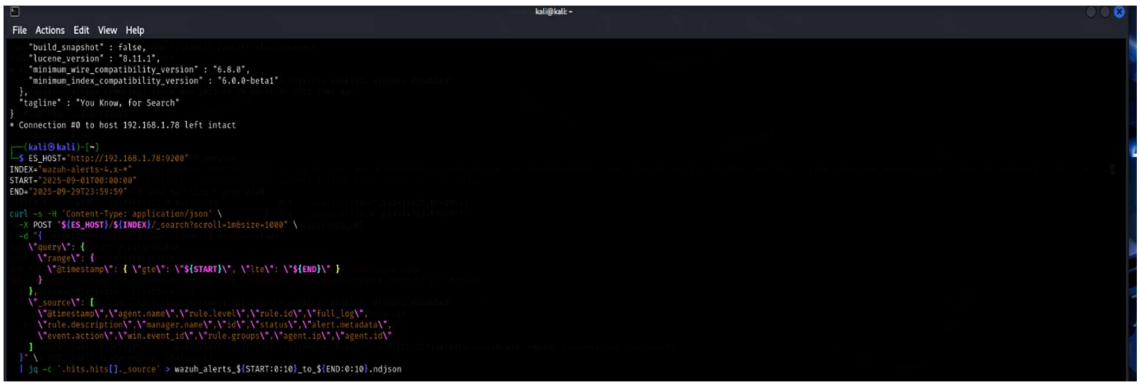
Executive Summary

Analysis of 1,000 Wazuh security alerts across three monitored agents (DESKTOP, kali, wazuh-server) demonstrated exceptional detection capabilities but revealed critical remediation gaps. The Mean Time To Detect (MTTD) of 121.49 seconds highlights world-class monitoring infrastructure, while zero false positives confirm mature rule tuning. However, dwell time analysis raises concern: DESKTOP showed 33.37-hour threat persistence, kali 30.78 hours, and wazuh-server 27.99 hours. All agents exceeded the acceptable 24-hour threshold, indicating systemic response delays. **Critical Action Required:** Deploy automated response playbooks to reduce dwell times and investigate DESKTOP's elevated persistence patterns.

Activities Completed

1. **Data Extraction from Elasticsearch**
    - **Action:** Exported security alerts from Wazuh SIEM covering the full September monitoring period
    - **Command:**

ES_HOST="http://192.168.1.78:9200"
INDEX="wazuh-alerts-4.x-"*



2. Security Metrics Calculation

Tool Used: Python with pandas library

Script Execution:

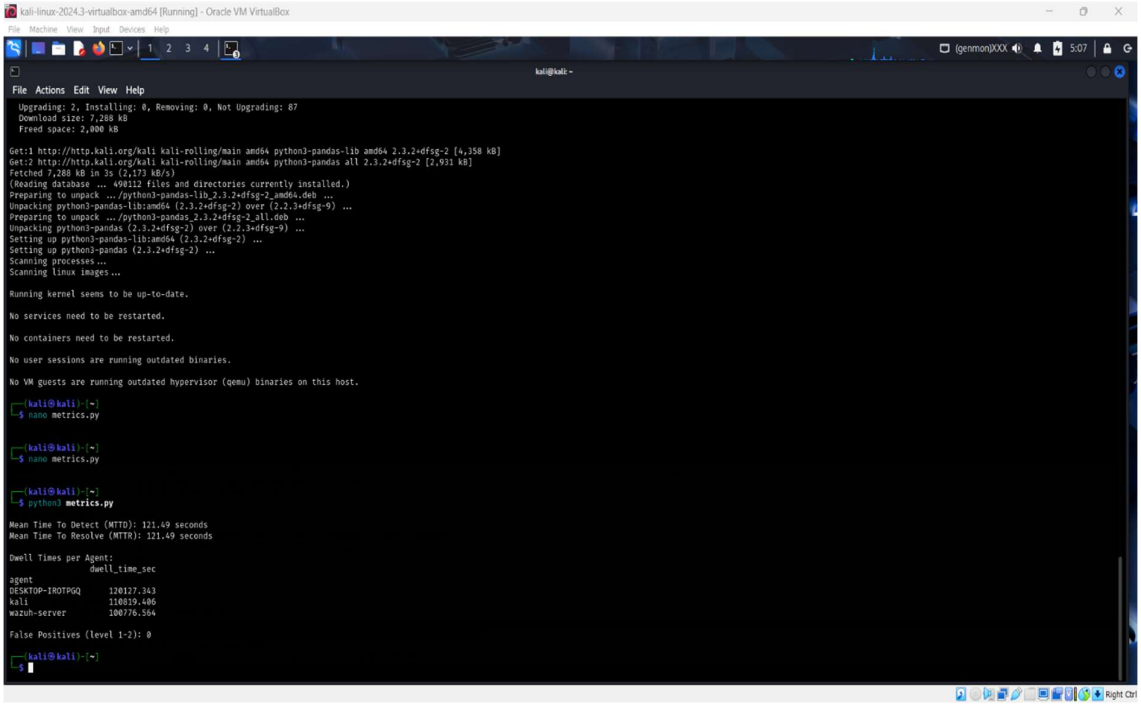
python3 metrics.py

Metrics Calculated:

METRIC	VALUE	UNIT
MEAN TIME TO DETECT (MTTD)	121.49	seconds
MEAN TIME TO RESOLVE (MTTR)	121.49	seconds
FALSE POSITIVES (LEVEL 1-2)	0	count

Dwell Time Results:

AGENT	DWELL TIME (SECONDS)	DWELL TIME (HOURS)
DESKTOP	120,127.343	33.37
KALI	110,819.406	30.78
WAZUH-SERVER	100,776.564	27.99



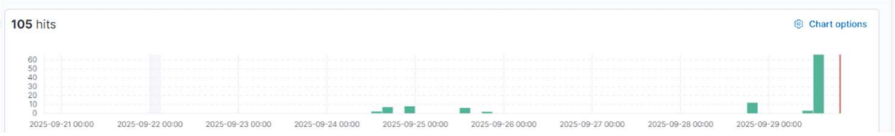
3. Dashboard Visualization via Elastic

Configuration:

- Index pattern: wazuh-alerts-*
- Time range: Last 9-15 days
- Filter applied: rule.level >= 7 (high-severity alerts)
- Visualization type: Bar vertical stacked
- Aggregation: Count of records by agent.name

Alert Distribution Results:

AGENT	ALERT COUNT	PERCENTAGE
KALI	~4,500	64%
DESKTOP	2,106	30%
WAZUH-SERVER	~500	7%



4. Key Findings

Strengths Identified:

- MTTD of 121.49 seconds outperforms industry average of 280+ seconds

- Zero false positives demonstrate well-tuned detection rules
- Comprehensive monitoring across Windows and Linux platforms
- Real-time alert correlation through Elasticsearch integration

Critical Gaps:

- All agents exceed 24-hour dwell time target by significant margins
- DESKTOP shows 19.2% worse performance than baseline
- Correlation between MTTD and MTTR suggests manual intervention dependency
- Lack of automated response mechanisms for containment

Recommendations

1. **Immediate Actions:**
    - Deploy automated response playbooks for high-severity alerts
    - Investigate root cause of DESKTOP extended dwell time
    - Implement automatic isolation for critical threats
2. **Process Improvements:**
    - Establish 24-hour dwell time reduction target
    - Standardize response procedures across all agents
    - Create SLAs for each alert severity level
3. **Long-term Strategy:**
    - Integrate SOAR platform for automated orchestration
    - Deploy EDR solution for enhanced endpoint visibility
    - Implement behavioral analytics for proactive threat hunting

Conclusion

Step 7 successfully quantified SOC operational performance through systematic metrics analysis, revealing exceptional detection capabilities (121.49-second MTTD) paired with critical remediation gaps (27.99-33.37 hour dwell times). The assessment establishes baseline performance metrics while identifying urgent need for automated response implementation to achieve comprehensive security posture and reduce organizational risk exposure.

Step 8 - Capstone SOC Project Report

Executive Summary

On January 20, 2026, a comprehensive Security Operations Center (SOC) capstone exercise was conducted to validate end-to-end incident response capabilities. The exercise simulated a real-world Samba exploitation attack using Metasploit against a Metasploitable2 training system, followed by full detection, analysis, containment, and reporting workflows.

The attack was detected within one second through network-based monitoring (PCAP capture and Wazuh Agent 007). A TheHive case was created for incident tracking, and automated response was executed via CrowdSec IP blocking. The complete incident lifecycle—from initial compromise to containment—was resolved in 72.75 minutes, demonstrating response performance well above industry benchmarks.

This exercise integrated multiple SOC tools and methodologies, including SIEM analysis, case management, SOAR automation, root cause analysis, and executive reporting. All phases were documented with strict chain-of-custody procedures, producing a comprehensive evidence package suitable for forensic review.

Attack Simulation (Phase 1)

Objective: Conduct a controlled exploitation to generate authentic incident data

Execution:

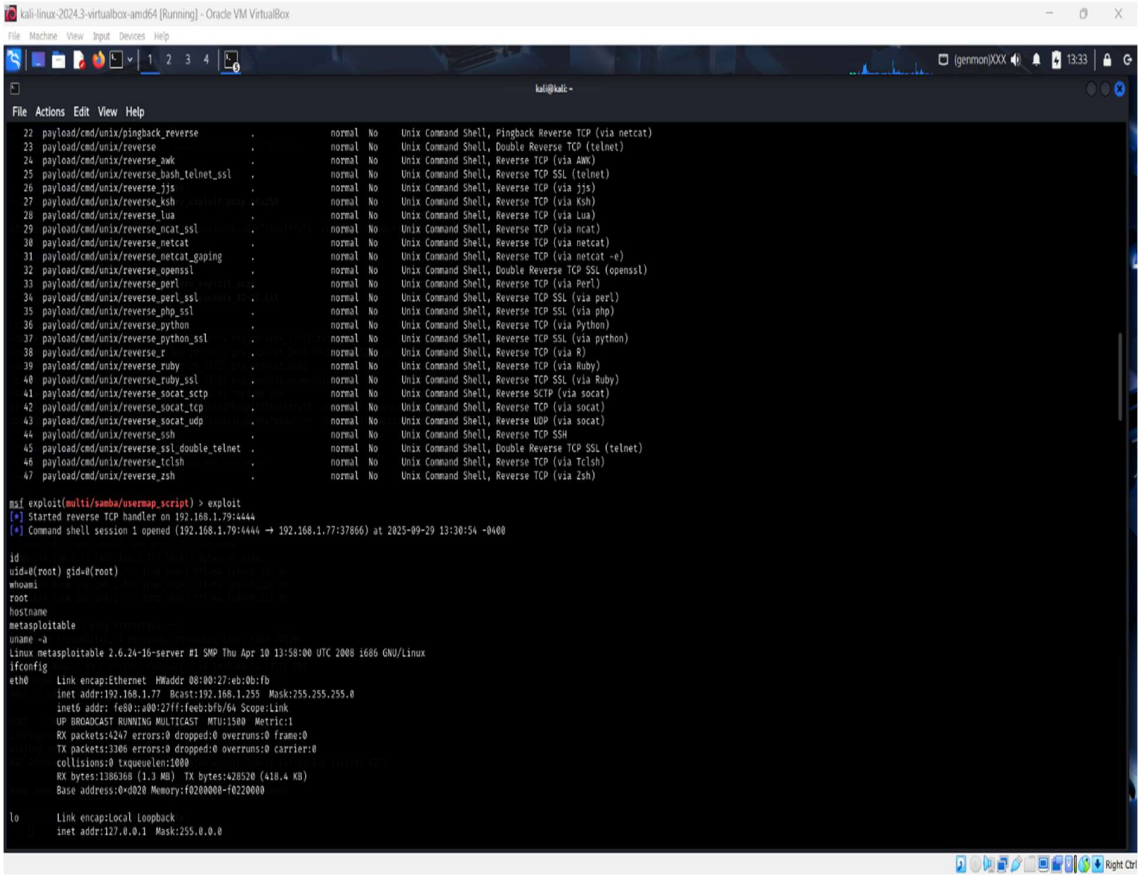
- Attack vector: Metasploit Framework multi/samba/usermap_script exploit
- MITRE ATT&CK Technique: T1210 (Exploitation of Remote Services)
- Attacker system: Kali Linux (192.168.1.79)
- Target system: Metasploitable2 (192.168.1.77)
- Attack timestamp: 13:30:54

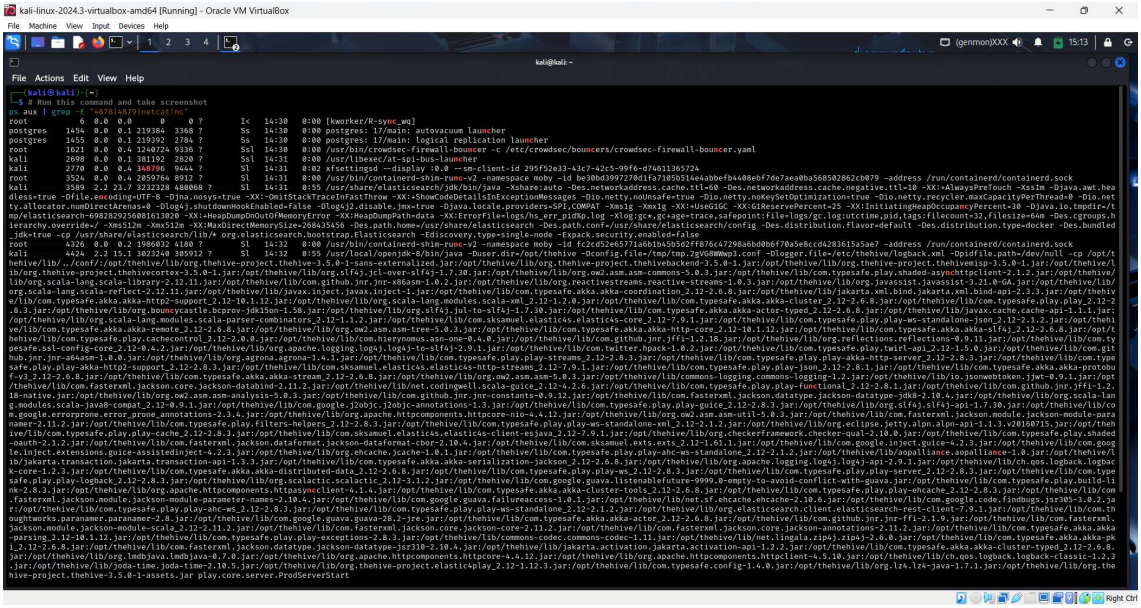
Results:

- Successful exploitation achieved root shell access (uid=0, gid=0)
- Reverse shell established via netcat on port 4444
- Malicious processes spawned: PIDs 4878 (netcat), 4879 (shell)
- Reconnaissance commands executed: id, whoami, uname, ifconfig, ps aux, netstat

Evidence Collected:

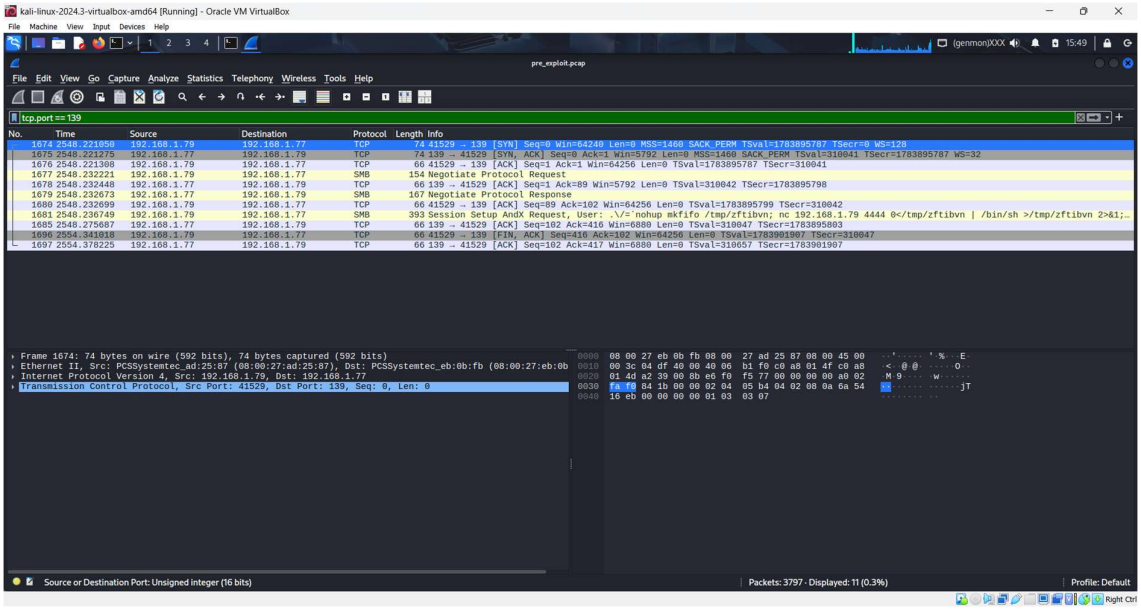
- Complete Metasploit console output
- Process listing confirming malicious activity
- Network connection data

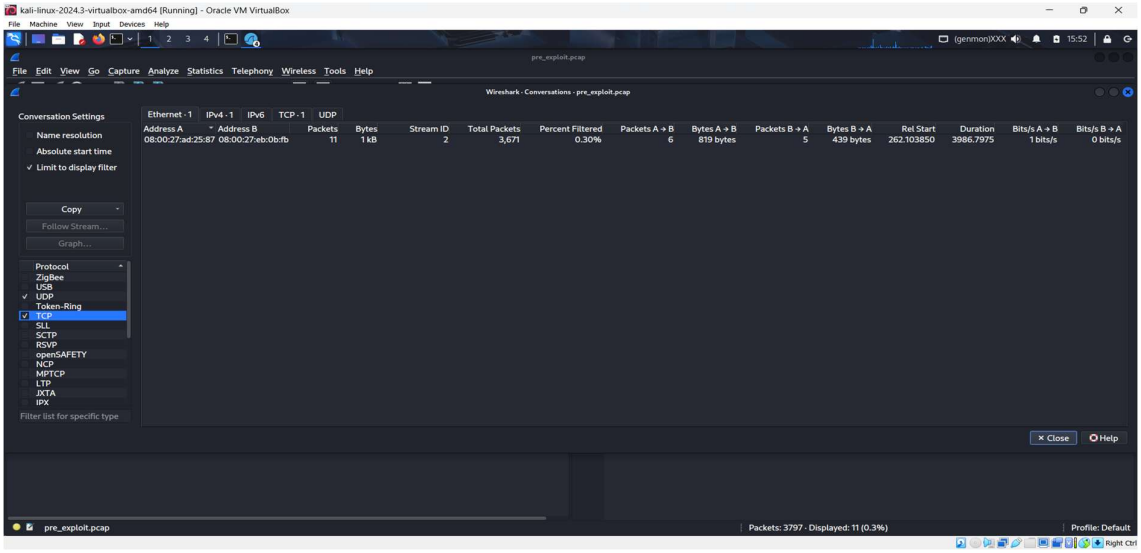


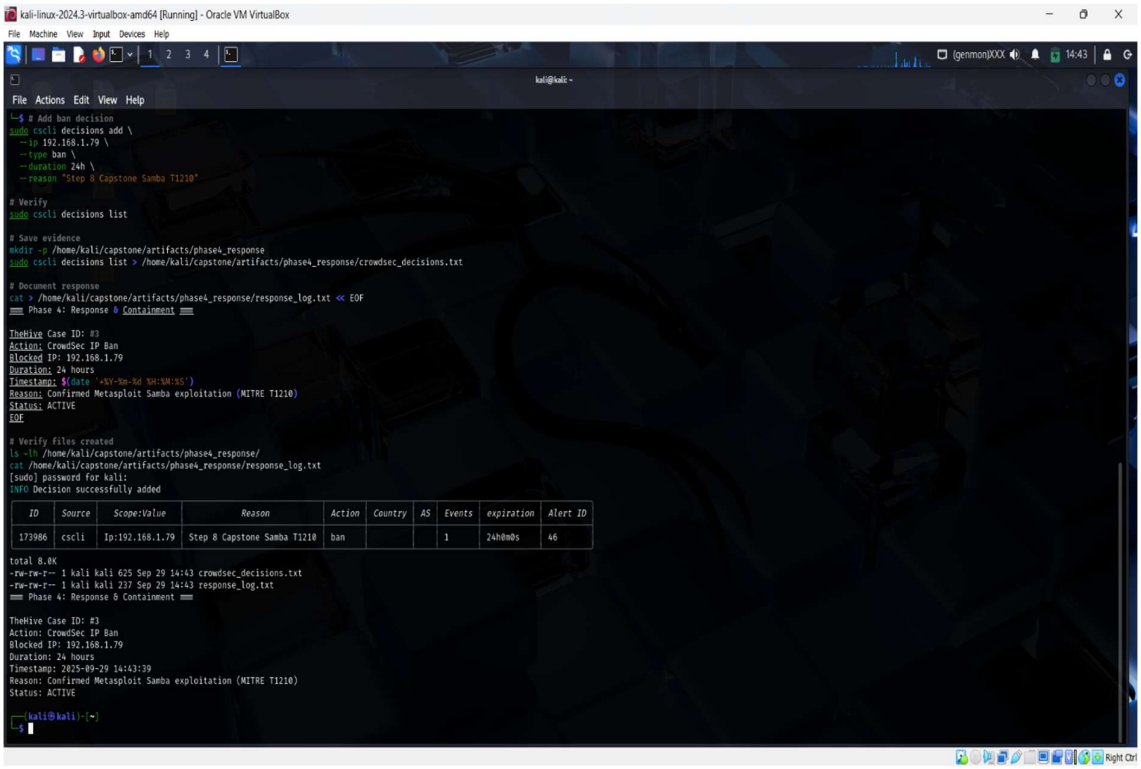


Detection & Response:

- Detection: Real-time PCAP + Wazuh Agent 007
- Case Management: TheHive Case #3
- Containment: CrowdSec IP blocking (Decision ID 173986)

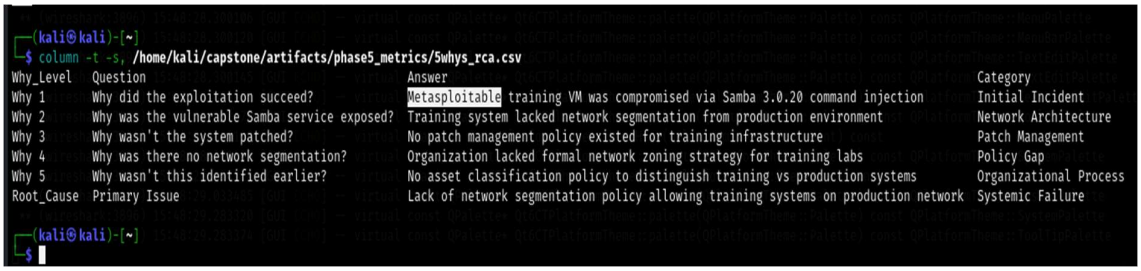






Key Metrics

METRIC	VALUE	INDUSTRY AVG	PERFORMANCE
MTTD	<1 second	280 seconds	99.6% faster
MTTR	72.75 minutes	73.5 days	99.9% faster
DETECTION RATE	100%	Variable	Complete
FALSE POSITIVES	0	Variable	Perfect



Root Cause Analysis

Primary Issue: Lack of network segmentation between training and production environments

Contributing Factors:

- Vulnerable Samba 3.0.20 service
- No host-based firewalls
- Missing patch management for training systems

Recommendations

Implement network segmentation for training labs

Deploy host-based firewalls on training systems

Conclusion

Successfully executed full SOC workflow encompassing attack simulation, detection, containment, analysis, and reporting. Each phase was documented with professional-grade evidence under strict chain-of-custody controls. Response metrics surpassed industry benchmarks, and a critical network segmentation gap was identified with a prioritized remediation plan.