

# SecOps Analysis Report

Generated: December 6, 2025 16:30:00 EST | Analysis Period: Last 2 hours vs. 26-24 hours ago |  
Confidence: HIGH

QUERY PROMPT

"Analyze all security events from the 2 hours compared to the same 2-hour window yesterday (26 hours ago to 24 hours ago). Correlate authentication failures, attack patterns, and malware detections across all systems to identify coordinated threats. Include a priority matrix that ranks incidents by severity and blast radius. Identify the root cause for any attack chains and provide specific remediation commands."

## | Executive Summary

SEVERITY: CRITICAL

Active multi-vector cyber attack detected with coordinated ransomware deployment, massive data exfiltration, and widespread system compromise.









### Key Findings (Last 2 Hours vs. Yesterday)

| Metric                  | Current (2 hrs)      | Yesterday (2 hrs) | Change        |
|-------------------------|----------------------|-------------------|---------------|
| Authentication Failures | 3,000+ events        | 0 events          | ⚠️ NEW ATTACK |
| Malware Detections      | 11,000+ events       | 0 events          | ⚠️ NEW ATTACK |
| Ransomware Incidents    | 100+ variants        | 0 events          | ⚠️ NEW ATTACK |
| Data Exfiltration       | 100+ events (12+ TB) | 0 events          | ⚠️ NEW ATTACK |
| DDoS/Flood Attacks      | 100+ events          | 0 events          | ⚠️ NEW ATTACK |
| Brute Force Attempts    | 100+ events          | 0 events          | ⚠️ NEW ATTACK |
| SQL/Command Injection   | 100+ events          | 0 events          | ⚠️ NEW ATTACK |

| Metric               | Current (2 hrs)         | Yesterday (2 hrs) | Change      |
|----------------------|-------------------------|-------------------|-------------|
| Unexpected Shutdowns | 106 events (14 systems) | Unknown           | ⚠️ CRITICAL |

⚠️ **CRITICAL ALERT:** This represents a **zero-to-massive** escalation indicating a coordinated, sophisticated cyber attack campaign that began within the last 24 hours.

## | Priority Matrix - Incidents by Severity & Blast Radius

| Priority | Incident Type                       | Severity  | Blast Radius    | Count   | Impact                                                                                     |
|----------|-------------------------------------|-----------|-----------------|---------|--------------------------------------------------------------------------------------------|
| P0       | Ransomware Deployment               | CRITICAL  | Enterprise-Wide | 100+    |  10/10  |
| P0       | Data Exfiltration (12+ TB)          | CRITICAL  | Enterprise-Wide | 100+    |  10/10  |
| P0       | Coordinated Attack on workstation05 | EMERGENCY | Department      | 1       |  10/10  |
| P1       | Malware Infections                  | CRITICAL  | Enterprise-Wide | 11,000+ |  9/10   |
| P1       | Distributed Brute Force             | HIGH      | Enterprise-Wide | 3,000+  |  8/10   |
| P2       | DDoS/Flood Attacks                  | HIGH      | Multiple Hosts  | 100+    |  7/10   |
| P2       | SQL/Command Injection               | HIGH      | Multiple Hosts  | 100+    |  7/10 |
| P3       | Unexpected System Shutdowns         | MEDIUM    | Department      | 106     |  6/10 |

---

# | Attack Chain Analysis

## INCIDENT #1: Coordinated Ransomware Campaign

**Target:** workstation05.company.com

**Root Cause:** Multi-stage Advanced Persistent Threat (APT) attack

### Attack Timeline & Kill Chain

1. INITIAL ACCESS (T1566 – Phishing)
  - ↳ Emotet dropper delivered via email attachment
2. EXECUTION (T1204 – User Execution)
  - ↳ Malicious payload executed from user directory
3. PERSISTENCE (T1543 – Create/Modify System Process)
  - ↳ Multiple malware variants installed:
    - Emotet, TrickBot, Cobalt Strike
    - Backdoors established
    - Rootkits deployed
4. CREDENTIAL ACCESS (T1003 – OS Credential Dumping)
  - ↳ Mimikatz executed multiple times
  - ↳ LSASS memory dumps via wce.exe
  - ↳ SAM database dumps
5. LATERAL MOVEMENT (T1021 – Remote Services)
  - ↳ PSEXEC used for SMB-based lateral movement
  - ↳ Compromised credentials used across network
6. COMMAND & CONTROL (T1071 – Application Layer Protocol)
  - ↳ C2 beacons to external IPs
7. EXFILTRATION (T1048 – Exfiltration Over Alternative Protocol)
  - ↳ 12,715 GB total exfiltrated
  - ↳ DNS tunneling, GDrive, Rclone
8. IMPACT (T1486 – Data Encrypted for Impact)

↳ Multiple ransomware variants deployed

## Blast Radius

- **Primary:** workstation05.company.com (fully compromised)
  - **Secondary:** fileserver01.company.com, mailserver01.company.com
  - **Tertiary:** 50+ hosts referenced in lateral movement
  - **Data Loss:** 12.7 TB of sensitive data exfiltrated
-

# | Data Exfiltration Analysis

| Host             | Data Exfiltrated | Method             | Destination         |
|------------------|------------------|--------------------|---------------------|
| workstation05    | 4,026 GB         | Multiple           | External IPs        |
| workstation05    | 3,135 GB         | Encrypted transfer | Unauthorized GDrive |
| workstation05    | 2,371 GB         | DNS tunneling      | Various             |
| workstation05    | 2,208 GB         | Rclone sync        | Cloud storage       |
| workstation05    | 671 GB           | Database dump      | External IP         |
| workstation05    | 174 GB           | HTTP POST          | External IP         |
| TOTAL: 12,585 GB |                  |                    |                     |

---

# | Remediation Commands

## IMMEDIATE ACTIONS (Execute Now)

### 1. Isolate Compromised Systems

```
# Disconnect workstation05 from network immediately
ssh admin@firewall "configure; set security zones security-zone trust \
  interfaces ge-0/0/5 host-inbound-traffic system-services none; commit"

# Block workstation05 at core switch
ssh admin@core-switch "conf t; interface GigabitEthernet1/0/24; \
  shutdown; end; write mem"
```

### 2. Block Malicious C2 IPs

```
# Block C2 servers at perimeter firewall
C2_IPS="168.35.36.83 27.91.8.209 154.234.68.3 192.139.249.92"

for ip in $C2_IPS; do
  # Cisco ASA
  ssh admin@asa-firewall "configure terminal; \
    access-list BLOCK_C2 extended deny ip any host $ip; exit; write mem"

  # PaloAlto
  ssh admin@paloalto "configure; set address C2-$ip ip-netmask $ip/32; \
    set address-group Blocked-C2 static C2-$ip; commit"

  # Linux iptables
  iptables -I INPUT -s $ip -j DROP
  iptables -I OUTPUT -d $ip -j DROP
done
```

### 3. Disable Compromised Accounts

```
# Disable accounts with credential dumps
COMPROMISED_USERS="admin mwilson kjohnson jsmith agarcia jdoe tadams"

for user in $COMPROMISED_USERS; do
  # Active Directory
  net user "$user" /active:no /domain
```

```
# Force password reset on next login
net user "$user" /logonpasswordchg:yes /domain

# Linux systems
passwd -l $user
pkill -u $user
done
```

## 4. Stop Ransomware Encryption

```
# Emergency shutdown of affected file servers
for host in fileserver01 mailserver01 server-db-01; do
  ssh root@$host "shutdown -h now"
done

# Disable SMB/CIFS shares immediately
ssh root@fileserver01 "systemctl stop smbd nmbd; systemctl disable smbd nmbd"

# Block SMB at firewall
ssh admin@firewall "configure; set security policies from-zone any \
  to-zone any policy block-smb match application junos-smb; \
  set security policies from-zone any to-zone any policy block-smb \
  then deny; commit"
```

---



## | Threat Intelligence Summary

### Malicious IPs (C2 Servers)

168.35.36.83:443

27.91.8.209

154.234.68.3

192.139.249.92

### Ransomware Families Detected

WannaCry, Ryuk, LockBit

Conti, BlackCat, Cryptolocker

Maze, REvil, NotPetya

### Attack Tools Identified

- **Mimikatz** - credential dumping
  - **PSEXEC** - lateral movement
  - **Cobalt Strike** - C2 framework
  - **Emotet** - dropper
  - **TrickBot** - banking trojan
  - **Rclone** - data exfiltration
-

## | Critical Next Steps

1. **ISOLATE** workstation05.company.com, fileserver01.company.com, mailserver01.company.com
2. **BLOCK** C2 IPs: 168.35.36.83, 27.91.8.209, 154.234.68.3, 192.139.249.92
3. **DISABLE** compromised accounts: admin, mwilson, kjohnson, jsmith, agarcia, jdoe, tadams
4. **SHUTDOWN** affected file servers to prevent ransomware spread
5. **ACTIVATE** incident response team and notify leadership
6. **PRESERVE** forensic evidence for investigation
7. **ENGAGE** external incident response firm if needed

**Time is critical - every minute counts in preventing further damage!**

---

*Report Generated: 2025-12-06 16:30:00 EST*

*Analysis Period: Last 2 hours vs. 26-24 hours ago*

*Confidence Level: HIGH (based on 14,000+ correlated security events)*