SIEM Alert Correlation Report

Analyst: Samuel Jemal
Date of Investigation: 29 October 2025
Incident Type: Suspicious Login Activity
Severity Level: Medium
Status: Closed

1. Executive Summary

On October 29, 2025, a SIEM alert triggered due to multiple failed login attempts from a foreign IP address followed by a successful administrative login. Event correlation revealed lateral movement attempts across the internal network. The incident was investigated, contained, and user credentials were reset. No data exfiltration was observed.

2. Tools Used

• Splunk – Log correlation and query search
• Sysmon – Endpoint log generation
• Wireshark – Network capture verification
• MITRE ATT&CK; Framework – Technique mapping

3. Investigation Process

• Alert Triage: Splunk alert identified 10 failed logins from IP 203.0.113.77 followed by a successful login within 2 minutes.
• Log Correlation: Using SPL query, matched same user 'admin01' accessing three endpoints within 10 minutes.
• Network Verification: Wireshark confirmed SMB and RDP traffic between compromised endpoints.
• User Verification: Confirmed user did not perform remote login; credentials likely compromised.
• Containment: Disabled affected account and blocked source IP at firewall.

4. Findings

Indicator Type	Value	Description
User Account	admin01	Compromised account credentials
Source IP	203.0.113.77	Foreign IP used in attack
Destination Hosts	WIN-SRV1, HR-LAPTOP1, FIN-SRV2	Lateral movement targets
Protocol	RDP/SMB	Used for remote connection attempts
SIEM Alert ID	ALRT-1025	Splunk correlation rule ID

5. MITRE ATT&CK; Mapping

Phase	Technique ID	Technique Name
Initial Access	T1078	Valid Accounts
Lateral Movement	T1021.001	Remote Services: RDP
Credential Access	T1110.001	Brute Force
Defense Evasion	T1070.004	File Deletion

6. Containment & Remediation

• Disabled compromised admin account and reset password.
• Blocked source IP address and related subnets on the firewall.

• Enabled geolocation-based access restrictions for admin logins.
• Enhanced SIEM correlation rule to detect similar patterns earlier.
• Conducted security awareness session for privileged users.

7. Recommendations

• Implement MFA for all administrative accounts.
• Increase SIEM rule sensitivity for abnormal login patterns.
• Enable detailed audit logging across all domain controllers.
• Regularly review access control policies and privileged accounts.
• Integrate threat intelligence feeds into SIEM for faster detection.

8. Lessons Learned

• Timely SIEM alerting enabled early incident containment.
• Centralized log management is critical for correlation visibility.
• User credential hygiene and MFA can prevent unauthorized access.

9. Analyst Signature

Name: Samuel Jemal
Role: SOC Analyst (Intern)
Date: 29 October 2025