TASK 2

🛡 SECURITY ALERT MONITORING & INCIDENT RESPONSE

🔷 Task: Monitor simulated security alerts using a SIEM tool, identify suspicious activities, classify incidents, and draft an incident response report.

In this task , I have used Splunk tool

[CONFIDENTIAL] Incident Response Report

Field	Value
Incident ID:	IR-20250820-001
Date of Report:	August 20, 2025
Incident Status:	**Declared - Containment in Progress**
Severity Classification:	**High**
Lead Analyst:	S.Srinubabu (SOC Analyst)

1.0 Executive Summary

On August 20, 2025, a security investigation confirmed that a targeted cyberattack resulted in the successful compromise of a production webserver, WEB-PROD-01. The attack was identified as a brute-force campaign originating from the external IP address 185.220.101.245. The attacker successfully guessed the password for the svc_admin service account at approximately 11:14 AM IST, gaining unauthorized administrative access to the system.

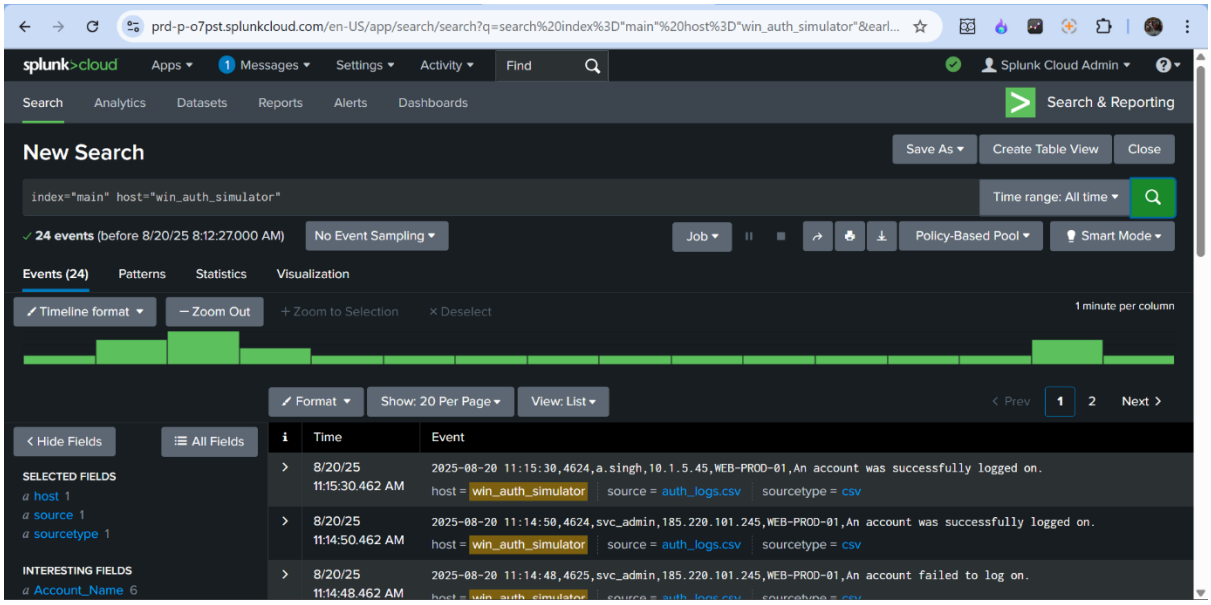
This incident is classified as **High** severity due to the breach of a privileged account on a critical production asset. Immediate actions are underway to contain the threat, and this report outlines the detailed findings and provides actionable recommendations to eradicate the threat and strengthen our security posture.

2.0 Alert Analysis & Investigative Timeline

The investigation was conducted by a SOC Analyst using the Splunk SIEM platform. The process followed a logical progression from broad analysis to specific, conclusive evidence.

2.1 Data Ingestion and Validation

The foundation of the investigation was a set of authentication logs (auth_logs.csv) which were successfully ingested into the Splunk index main. Initial validation confirmed that all 24 log events were correctly parsed and available for analysis, a step confirmed by your initial search (Shown as below Screenshot).

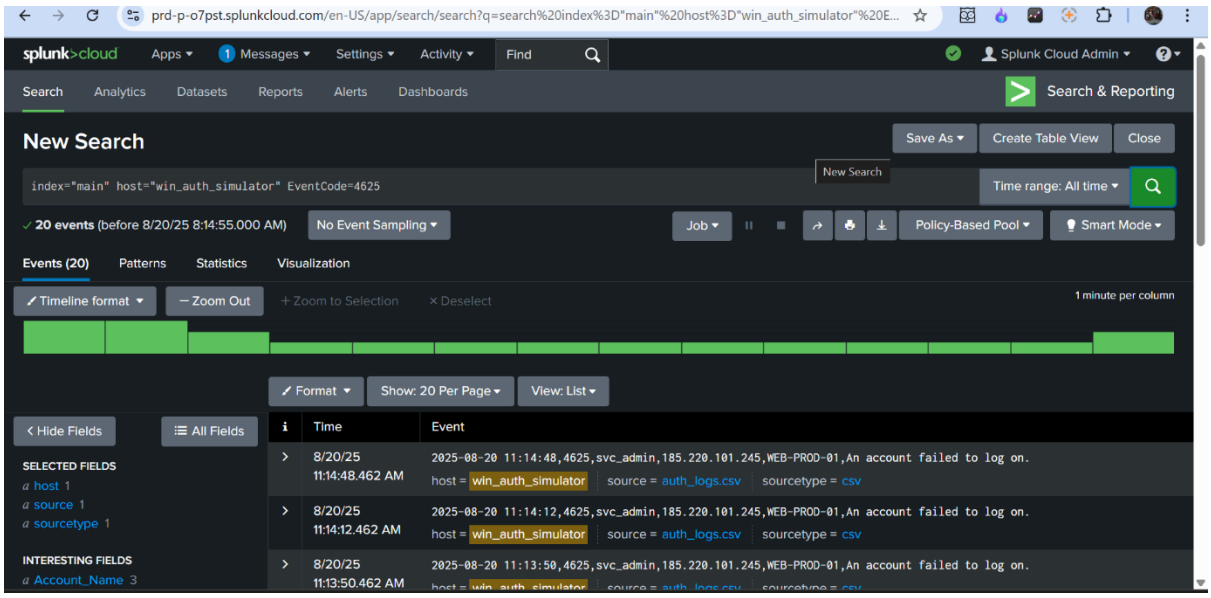


2.2 Step-by-Step Investigation

Phase 1: Identifying Anomalous Activity

The investigation began by searching for signs of suspicious behavior. The first logical step was to hunt for failed login attempts using the Windows Security EventCode=4625.

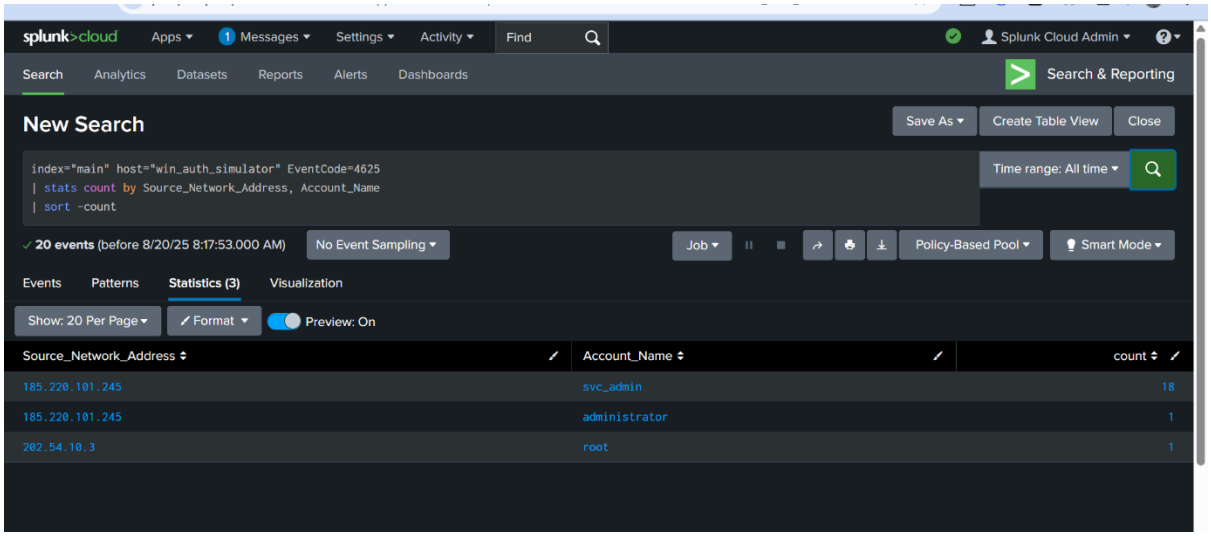
- **Query:** index="main" host="win_auth_simulator" EventCode=4625
- **Finding:** The query returned **20 failed login events**, an unusually high number for a short time frame, which warranted a deeper look.



Phase 2: Uncovering the Attack Pattern

To understand if the 20 failures were related, we grouped them by source IP address and target account. This is the crucial step where a targeted attack becomes visible.

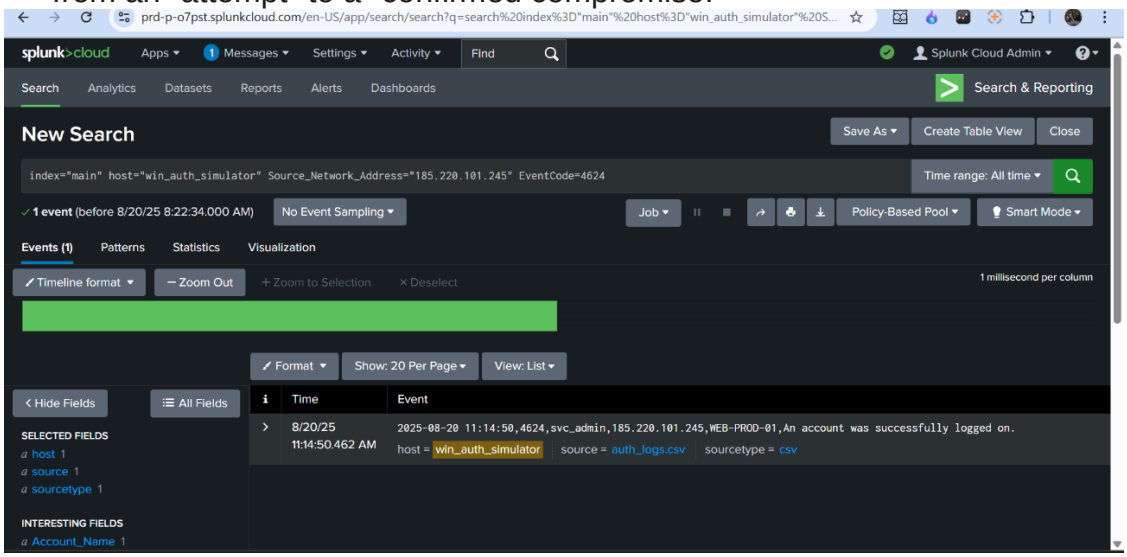
- **Query:** index="main" host="win_auth_simulator" EventCode=4625 | stats count by Source_Network_Address, Account_Name | sort -count
- **Finding:** This query produced a clear and alarming table. As documented in your screenshot (**Screenshot 2025-08-20 134841.png**), the top result showed that **18 of the 20 failures** came from a single IP, 185.220.101.245, all targeting the svc_admin account. This definitively identified the activity as a brute-force attack.



Phase 3: Confirmation of System Compromise

With a targeted attack identified, the final and most critical step was to determine if the attacker ever succeeded. A new search was run to look for a successful login (EventCode=4624) from the attacker's IP.

- **Query:** index="main" host="win_auth_simulator" Source_Network_Address="185.220.101.245" EventCode=4624
- **Finding:** This search returned a single, critical event. As captured in your screenshot (**image_5200c0.png**), this was the "smoking gun": a successful login from the attacker's IP at **11:14:50 AM IST**. This finding elevated the incident from an "attempt" to a "confirmed compromise."



3.0 Incident Classification

Classification	Justification
Severity Level: HIGH	The classification is based on the following factors: **- Data Impact:** The compromised svc_admin account possesses administrative privileges, granting the attacker the ability to access, modify, or exfiltrate sensitive application data and server configurations. **- Scope:** A critical production server (WEB-PROD-01) was breached. **- Attacker Presence:** The successful login confirms an active, unauthorized presence within our production environment.

4.0 Remediation Recommendations

The following actions are recommended to contain, eradicate, and recover from this incident.

4.1 Immediate Actions (Containment - Within the next hour)

- **Isolate the Host:** Immediately disconnect WEB-PROD-01 from the network to prevent any potential lateral movement by the attacker.
- **Block Attacker IP:** Create a firewall rule to block all traffic from 185.220.101.245.
- **Disable and Reset Account:** Disable the svc_admin account in Active Directory and immediately reset its password to a long (25+ character), complex, randomly generated value.

4.2 Short-Term Actions (Eradication & Recovery - Within 24-48 hours)

- **Forensic Analysis:** Conduct a forensic analysis of WEB-PROD-01 to determine the extent of the attacker's activities post-compromise.
- **Log Review:** Analyze firewall and server logs for any connections originating *from* WEB-PROD-01 to other internal systems since the time of compromise.
- **System Restore:** Based on forensic findings, restore the server from a known-good backup created prior to 11:14 AM on August 20, 2025.

4.3 Long-Term Actions (Hardening & Prevention - Within 1-2 weeks)

- **Secure Remote Access:** Prohibit direct RDP access from the internet. All administrative access should be routed through a secure VPN that requires Multi-Factor Authentication (MFA).
- **Implement Strong Policies:** Enforce a mandatory strong password policy and a strict account lockout policy (e.g., 5 invalid attempts lock an account for 30 minutes).
- **Audit Service Accounts:** Perform a complete audit of all service accounts to ensure they adhere to the principle of least privilege and that their passwords are secure and regularly rotated.

5.Conclusion

Ultimately, this investigation proved that our systems were compromised not by a sophisticated zero-day exploit, but by a simple brute-force attack that succeeded due

to fundamental security oversights. The attacker essentially knocked on an unlocked door until it opened, giving them control of a critical server. This incident is a stark reminder that without enforcing basic security hygiene—like strong passwords, account lockouts, and restricting direct internet access to sensitive services—our defenses remain fragile. The recommendations in this report are therefore not just improvements, but essential fixes required to secure our environment against these common, yet highly effective, types of attacks.