PROJECT 1: SOC Alert Investigation & Incident Report

*(Based on SOC L1 Alert Triage – Example Using Dashboard Alerts**)***

1. Executive Summary

The present report was created during the investigation of a SOC Level 1 security alert identified in a SOC centralized monitoring dashboard. The alarm was raised because of the large number of failed authentication attempts as a result of an external IP address who had targeted a system facing the internet. Contextual metadata and alert properties and related activity were evaluated to understand the character of the behavior. According to the evidence gained, the alert has been defined as a True Positive since the activity was associated with an ongoing brute-force attack on a remotely accessible system.

2. Alert Overview

- **Alert Name:** Brute Force Attack from External
- **Severity:** Medium
- **Priority:** P3
- **Detection Time:** Mar 21st 2025 at 11:53

The alert was raised due to abnormal authentication patterns indicative of a potential brute-force attack and thus needed more investigation by the SOC team.

---

3. Alert Properties & Context

- **Alert Source:** SOC Dashboard (SIEM)
- **Targeted Users:** Administrator, admin, adm
- **Affected Host:** WIN-ITDEV
- **Source IP Address:** 45.148.10.50
- **Initial Risk Level:** Medium

Authentication alerts are usually used to identify credential abuse and brute-force. The external source in this case has attacked several privileged account names through the RDP service. The vulnerable host was a virtual development machine that was accidentally made accessible to the internet increasing its attack surface.

---

4. Investigation Steps

The following investigation steps were performed as part of the SOC Level 1 triage process:

1. Audited alert information in the SOC dashboard.
2. Examined activity of authentication in relation to the user account that was impacted.
3. Assessed the source IP and established whether it was an in-house or an external.
4. Examined the time of the activity and contrasted it with the normal working hours.
5. Checked for additional related alerts or indicators such as privilege escalation or lateral movement.
6. Evaluated the overall activity to determine whether the behavior indicated malicious intent or unauthorized access attempts.

---

5. Evidence Collected

- Alert metadata indicating a high volume of failed authentication attempts.
- An external IP address repeatedly attempting authentication via the RDP service.
- Attack on multiple privileged account names.
- There were 1620 unsuccessful attempts over a period of time.
- System that is exposed to the internet that is known to be the target of the attack.

The gathered data prove the existence of long-lasting attempts of unauthorized access that corresponds with automated brute-force attacks.

---

6. MITRE ATT&CK Mapping

- **Tactic:** Credential Access
- **Technique:** Brute Force (T1110)

The identified activity can be directly associated with the MITRE ATT&CK Brute Force technique since the external attacker tried to perform several authentication attacks on privileged accounts with the help of the RDP service.

---

7. Final Verdict

Classification: True Positive

Justification:
The alert represents a confirmed brute-force attack originating from an external IP address targeting

multiple privileged user accounts via the RDP service. The high volume of failed authentication attempts (1620), combined with the exposure of the system to the internet, clearly indicates malicious automated activity. Although no successful authentication occurred, the presence of sustained unauthorized access attempts confirms this as a true positive security incident.

---

8. Recommendations

- Immediately block or forcefully shut down RDP from the public internet.
- Implement firewall rules or VPN-based access for remote administration.
- Use Multi-Factor Authentication (MFA) on every privileged account.
- Use policies to lock-out accounts to remove brute force attacks.
- Test and solidify temporary or development virtual machines prior to deployment.
- Keep watching out on similar brute-force attacks by external parties.

Report Status

- **Incident Status:** Closed
- **SOC Analyst Level:** L1
- **Escalation Required:** Yes (Escalated to L2 for IT remediation)