

# Security Operations Assessment

## Executive Brief & Risk Reduction Plan

Independent portfolio simulation | Fictional 250-person organization | Synthetic 30-day dataset

**Important:** This is a demonstration using fabricated data, not a real client engagement or a real incident investigation.

### Executive summary

A review of 600 fabricated authentication events identified several patterns worth investigating in a real environment: repeated authentication failures across multiple accounts, successful sign-ins tagged as unusual-location scenarios, legacy-style authentication without an MFA challenge, and privileged sign-ins without an MFA challenge. These are simulated patterns, not evidence of a real compromise.

### Scope and method

The dataset contains 600 events and 63 distinct user identifiers. The analysis applies transparent triage rules to repeated failures, synthetic unusual-location sign-ins, legacy-style authentication without an MFA challenge, and privileged-account successes without an MFA challenge. Rules should be tuned against a real organization's baseline before production use.

### Priority findings

- **Critical — Privileged access without an MFA challenge.** Ten scenario events were created to test this control gap. Validate identity-provider records, account privilege, policy, and session context before concluding access was unauthorized.
- **High — Repeated failures across multiple accounts.** A synthetic burst of 60 failed attempts across eight accounts tests password-spray triage. Validate source and account activity, then review lockout, MFA, and alerting controls.
- **High — Legacy-style authentication without an MFA challenge.** Fifteen synthetic events test whether older authentication paths remain enabled. Confirm application dependencies before disabling protocols.
- **Medium pending validation — Unusual-location sign-ins.** Fifteen synthetic successful events test contextual triage. Location alone is not proof of malicious activity; compare VPN, device, travel, and sign-in history.

### Recommended 30/60/90-day plan

**Days 0–30:** Require MFA for privileged accounts; review privileged sessions and identity-policy exceptions; validate lockout controls; assign owners to high-priority findings.

**Days 31–60:** Inventory and restrict legacy authentication; create a repeatable sign-in triage playbook; correlate alerts with device and VPN context.

**Days 61–90:** Expand managed-device requirements for sensitive applications; test incident escalation and account-containment procedures; report control coverage and unresolved exceptions to leadership.

### Success measures

- All privileged accounts covered by MFA, with exceptions documented and time-bound.
- Repeated-failure alerts tested against representative benign and suspicious activity.
- Legacy authentication disabled or formally exception-approved.
- Triage playbook includes evidence capture, escalation, containment authority, and false-positive handling.
- Monthly reporting tracks alert volume, validation rate, time to triage, and overdue remediation.

### Limitations

Scenario tags are included to make the exercise reproducible. The results do not estimate real-world attack prevalence, prove compromise, or validate a production detection system. Cost estimates are omitted because no organization-specific

environment, licensing, staffing, or vendor quotes were available. A real engagement would confirm architecture, business requirements, control ownership, and baseline behavior before final recommendations.

## Reference frameworks

NIST Cybersecurity Framework 2.0 — [nist.gov/cyberframework](https://nist.gov/cyberframework)

NIST SP 800-61 Rev. 3 — [csrc.nist.gov/pubs/sp/800/61/r3/final](https://csrc.nist.gov/pubs/sp/800/61/r3/final)

CISA, Implementing Phishing-Resistant MFA — [cisa.gov/resources-tools/resources/implementing-phishing-resistant-mfa](https://cisa.gov/resources-tools/resources/implementing-phishing-resistant-mfa)

MITRE ATT&CK T1110 Brute Force — [attack.mitre.org/techniques/T1110/](https://attack.mitre.org/techniques/T1110/)