Red Team Assessment

Sample Deliverable — Assumed Breach Model

This portfolio sample illustrates AIComply360's control-validation reporting format for internal assumed-breach red team engagements. It is intentionally sanitized and omits environment-specific details and operational exploitation steps.

Service position: We offer red team engagements in an **Assumed Breach** model only—starting from internal standard-user access with objectives to validate privilege escalation controls, sensitive information protection, and SOC visibility.

Prepared for	Portfolio / Sample
Prepared by	AIComply360
Date	December 30, 2025

Table of Contents

- 1. Engagement Overview
- 2. Assumed Breach Model and Objectives
- 3. Scope and Rules of Engagement
- 4. Methodology and Control Validation Approach
- 5. Executive Summary (Outcome-Driven)
- 6. Findings Summary and Recommendations
- 7. Control Validation Matrix
- 8. Remediation Roadmap
- 9. Deliverables and Retest Options
- Appendix A: Evidence and Artifact Checklist
- Appendix B: Severity Rating Guidance
- Appendix C: Example Graph View (Illustrative)

1. Engagement Overview

AIComply360 provides control-focused red team services that emulate realistic post-compromise behavior to evaluate whether security controls **prevent**, **detect**, and **respond** to privilege escalation and sensitive information access.

Engagement definition

- **Model:** Assumed Breach (internal starting access provided).
- **Primary outcome:** Validate control effectiveness and SOC visibility across identity, privileged access governance, endpoint security, network/segmentation controls, and logging/monitoring.
- **Reporting style:** Executive summary begins with starting access, access gained, control gaps, telemetry outcomes, and a clear data validation statement.

Starting access (internal)

- Standard user identity in the primary identity platform (no administrative rights).
- One managed endpoint (device remains managed; security controls stay enabled).
- No privileged credentials, secrets, or pre-authorized administrative sessions provided.

Service offering note (Assumed Breach only)

AIComply360 offers red team engagements in an **Assumed Breach** model only. The engagement starts from internal access and validates whether controls and the SOC can prevent or detect escalation to privileged roles and access to sensitive information repositories.

2. Assumed Breach Model and Objectives

Under the Assumed Breach model, the assessment starts from an internal foothold and tests whether controls prevent or detect lateral movement and privilege escalation attempts. The focus is on validating controls and detection coverage rather than maximizing impact.

Objectives

- Validate that privileged access is governed, time-bound, and resistant to unauthorized elevation.
- Validate that sensitive information repositories are protected by least privilege and monitored access.
- Validate that key security events are logged, routed to the SIEM, and generate actionable alerts.
- Validate that the SOC can observe and triage relevant activity with sufficient context and timeliness.

Success criteria (examples)

- Privilege escalation pathways are blocked or require approvals that are enforced and auditable.
- High-risk events are visible in the SIEM with correct identity attribution and device context.
- Alerting is routed to the correct responder group and supports rapid triage.
- No sensitive data is extracted; access is validated via controlled proof-of-access methods.

3. Scope and Rules of Engagement

Scope (typical)

- Identity and access controls (MFA, conditional access, authentication policy enforcement).
- Privileged access governance (role assignments, just-in-time elevation controls, break-glass handling).
- Endpoint security controls (EDR visibility, device compliance, local admin restrictions).
- Network controls and segmentation (east-west access controls, egress visibility).
- Logging and monitoring controls (telemetry coverage, SIEM routing, retention, alerting).

Out of scope (examples)

- Denial-of-service activity and any disruption of production services.
- High-risk changes to production data or configuration without explicit written approval.
- Social engineering of end users unless explicitly included in the engagement agreement.

Safety and constraints

- Testing prioritizes safety, stability, and control validation over impact.
- Any discovered critical exposure is reported promptly through an agreed escalation path.
- Data access validation is performed using controlled methods; no production data extraction.
- Operational exploitation steps and environment-specific details are intentionally omitted from this sample.

4. Methodology and Control Validation Approach

The assessment follows a phased approach to validate controls and visibility. Activities are designed to produce audit-ready evidence (policy alignment, configuration observations, and SIEM/EDR artifacts) without disclosing sensitive operational details.

Phases

- Kickoff: Confirm scope, success criteria, communication, and escalation paths.
- Baseline validation: Review identity and device posture relevant to assumed breach.
- Privilege governance checks: Validate role assignment hygiene, approvals, and time-bound elevation controls.
- Detection validation: Confirm telemetry coverage and alerting for high-risk events; validate routing to responders.
- Reporting: Provide executive summary, findings, control validation matrix, and prioritized roadmap.

SOC and detection validation (purple-team checkpoints)

- Confirm which identity, endpoint, server, and network events are collected and forwarded to the SIEM.
- Validate alert logic for privileged activity and unusual authentication events.
- Validate responder visibility: correct enrichment, ownership, and escalation procedures.
- Document gaps in coverage, attribution, retention, or alert routing.

5. Executive Summary (Outcome-Driven)

Engagement definition

This sample engagement was defined as an Assumed Breach assessment starting with internal access as a standard user on one managed endpoint. The primary goal was to validate controls that prevent or detect privilege escalation and sensitive information access, and to confirm whether relevant telemetry reaches the SIEM with actionable alerts.

Starting access

- Standard user identity (no administrative roles).
- One managed endpoint within the corporate device management boundary.
- No privileged credentials, secrets, or pre-authorized administrative sessions.

High-level access gained (sanitized)

- A service principal (SPN-associated) account with excessive privileges was identified, enabling a rapid escalation path from standard user context to domain-level administrative impact.
- An encrypted outbound communications channel (simulated adversary command channel) did not produce sufficient visibility for high-confidence detection.
- Privilege escalation culminated in enterprise-level administrative risk due to privileged access governance gaps and incomplete protections on tier-0 assets.

Key control gaps (themes)

- Over-privileged service identities and weak service-account governance.
- Credential hygiene exposure (credential artifacts accessible from a standard user context).
- Limited visibility into encrypted web egress and insufficient east-west monitoring/segmentation.
- Incomplete endpoint protection / telemetry coverage on identity tier-0 systems.
- Detection and alerting gaps: inconsistent routing, enrichment, and SOC actionability.

Logging and visibility outcomes

- Encrypted web traffic lacked the telemetry required to confidently identify simulated adversary communications and pivot activity.
- Lateral activity and unusual server access did not generate high-confidence detections or actionable alerts.
- Tier-0 system telemetry coverage was incomplete, increasing the likelihood of undetected persistence.

Data access and exfiltration statement

No production data was extracted. Where sensitive access exposure was validated, it was confirmed through controlled proof-of-access methods (e.g., metadata-only validation and test artifacts) to avoid handling business data.

> **Redaction note:** This portfolio sample intentionally omits operational exploitation steps. Where command examples are normally included, they are represented as **[REDACTED]** placeholders.

6. Findings Summary and Recommendations

The following findings are representative examples. They are written to be control-focused and remediation-oriented, with sufficient context for leadership, engineering owners, and audit stakeholders.

ID	Finding (summary)	Severity	Control area	Recommended remediation (summary)
F-01	Over-privileged service principal (SPN-associated) account enabled rapid privilege escalation to domain-level administrative impact	Critical	IAM / AD / PAM	Implement service identity governance; remove excessive privileges; enforce strong secret management; add detection for anomalous service-account activity
F-02	Credential artifacts accessible in an IT shared folder from standard user context created a low-friction escalation vector	High	Credential Hygiene / Data Access	Remove credentials from shares; migrate to approved vault; restrict share permissions; rotate impacted secrets; enable secret scanning / DLP where feasible
F-03	Limited visibility into encrypted web (HTTPS) egress reduced detection of simulated adversary communications	High	Monitoring / Network Security	Enforce egress controls; enrich network telemetry; alert on anomalous destinations/volumes; ensure logs reach SIEM with host/user context

F-04	Insufficient east-west monitoring and segmentation for server access reduced detection of abnormal access patterns	High	Network Segmentation	Implement tiered segmentation; constrain admin paths; add lateral movement telemetry and alerting; validate server access controls
F-05	Incomplete endpoint protection/telemetry on tier-0 systems increased risk of undetected persistence	High	Endpoint Security	Deploy/enable approved endpoint telemetry on tier-0; harden configurations; route identity/DC events to SIEM; validate retention and alerting
F-06	Privileged session hygiene and admin tiering weaknesses increased the likelihood of privilege spread	Medium	PAM / Admin Practices	Adopt admin tiering; use privileged workstations/jump paths; enforce JIT elevation; restrict cross-tier logons; run periodic access reviews

Notes

- Findings are phrased to support remediation planning and evidence-driven validation.
- This sample omits environment-specific details and operational exploitation steps.
- Where credential recovery or persistence risk is referenced (e.g., Kerberos ticket abuse), it is described at a high level to avoid enabling misuse.

7. Control Validation Matrix

This matrix summarizes representative control areas validated during an assumed breach engagement, including validation focus, example evidence types, and outcome themes.

Control area	Validation focus	Example evidence	Outcome theme
Identity & MFA	Authentication policy enforcement, risky sign-in coverage, legacy authentication exposure	Authentication policy export; sign-in logs; risky sign-in alerts (where enabled)	Policy gaps reduced; exceptions tracked and justified
Service Identities (SPN)	Service account governance, privilege assignments, secret hygiene	Service-account inventory; privileged group membership; rotation/ownership records	Over-privilege removed; governance implemented
Privileged Access	Role assignment hygiene, JIT elevation, admin tiering, break-glass governance	Privileged role inventory; elevation approvals; access review artifacts	Elevation constrained; admin paths hardened
Endpoint & Tier-0	EDR/telemetry coverage, hardening baselines, DC visibility	Endpoint coverage reports; hardening baselines; tier-0 telemetry checklist	Tier-0 blind spots closed; persistence risk reduced
Network Segmentation	East-west controls, server access pathways, constrained admin routes	Firewall/segmentation rules; server access logs; jump path configuration	Lateral movement constrained and detected
Egress Visibility	Encrypted web egress monitoring, proxy enforcement, anomaly detection	Proxy logs; egress allowlists; SIEM network telemetry mappings	HTTPS visibility improved; anomaly alerts actionable
Logging & Monitoring	Audit coverage, SIEM routing, retention settings, alerting quality	SIEM ingestion map; alert rules; retention configurations	Coverage expanded to critical events

8. Remediation Roadmap

A prioritized roadmap helps teams sequence remediation to reduce risk quickly while improving detection and audit evidence quality.

Timeframe	Priority actions	Primary owners
0–30 days	Remove excessive privileges from service identities; restrict access to IT shares; rotate impacted credentials; confirm tier-0 telemetry coverage gaps (DC/identity)	Identity, IT Admin, SOC
30–60 days	Implement service-account governance (ownership, inventory, rotation); enforce JIT elevation and admin tiering; standardize SIEM routing/enrichment for high-risk events	Identity, Security Governance, SOC
60–90 days	Improve egress visibility and anomaly detection; implement segmentation for servers and privileged pathways; expand detection content for privileged and service-account anomalies	Network, SOC, Endpoint
90+ days	Establish continuous validation cadence (quarterly assumed-breach control checks); mature response playbooks; refine alerting based on lessons learned and evidence gaps	Security Governance, SOC

9. Deliverables and Retest Options

Deliverables

- Executive summary with starting access, access gained, control gaps, visibility outcomes, and a data validation statement.
- Findings summary with prioritized remediation guidance and control-area mapping.
- Control validation matrix and evidence checklist supporting audit-ready documentation.
- Remediation roadmap aligned to near-term risk reduction and long-term control maturity.

Retest (optional)

- A time-boxed retest validates remediation outcomes against the same success criteria.
- Retest outputs include an updated findings status table and a delta summary for leadership.

Appendix A: Evidence and Artifact Checklist

The following artifacts are commonly collected to support control validation and audit-ready evidence.

- Identity sign-in logs and risky sign-in detections (where enabled).
- Conditional access / authentication policy exports and exception lists.
- Service identity (SPN/service account) inventory, ownership records, and privileged membership reports.
- Privileged role inventory, access review artifacts, and time-bound elevation approval records.
- Endpoint telemetry coverage reports (including tier-0/DC coverage) and hardening baselines.
- File share access reviews and evidence of credential-hygiene remediation (vaulting, rotation).
- SIEM ingestion map (sources, event types, retention) and alerting rule set.
- Egress and proxy telemetry mappings (HTTPS visibility) and anomaly detection rules (where applicable).
- Incident response and escalation process documentation (roles and routing).

Appendix B: Severity Rating Guidance

Severity	Definition (summary)	Typical characteristics
Critical	Enterprise-compromise risk or immediate high-impact exposure	Privilege escalation to tier-0 / domain-level impact; widespread credential exposure; missing tier-0 telemetry
High	Material risk requiring prioritized remediation	Control gaps enabling escalation paths; major monitoring blind spots; weak segmentation for critical assets
Medium	Meaningful weakness with moderate exploitation likelihood/impact	Policy exceptions; incomplete governance processes; alerting quality issues
Low	Minor issue or best-practice improvement	Hardening opportunities; documentation gaps; minor tuning improvements

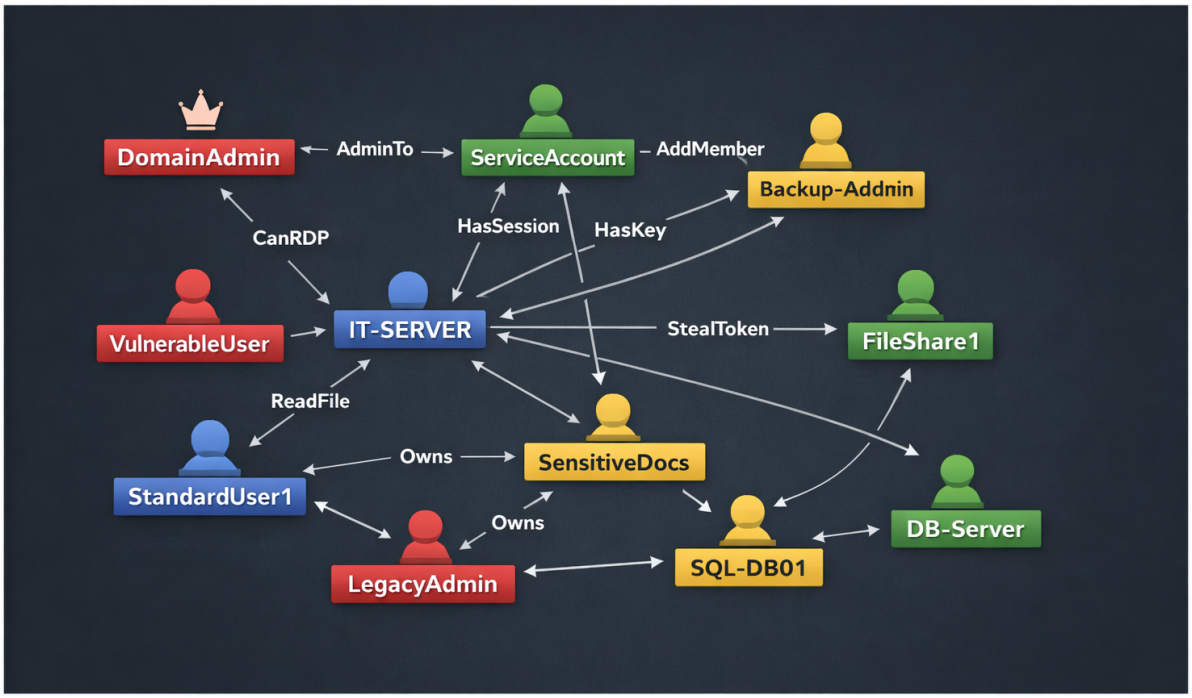
Redacted command examples (illustrative)

In a full client report, this section may include short command excerpts and outputs. In this portfolio sample, all operational commands are redacted to prevent misuse.

```
[REDACTED]
[REDACTED] Kerberos service identity validation step
[REDACTED] Output and artifact hashes
[REDACTED] Ticket/persistence validation (simulated)
[REDACTED]
```

Appendix C: Example Graph View (Illustrative)

The following image is an illustrative example of a relationship/attack-path graph commonly produced during identity and privilege-path validation. Node labels are generic and not tied to any client environment.



*Example **BloodHound** graph view (illustrative)*

Example graph view (illustrative)