Tabletop Exercise: Incident Response for Tim-Force

Organizational Profile – Tim-Force

Industry: Online automotive marketplace (C2C/B2B)
Size: Mid-sized, fast-scaling technology company
Business Model: Digital auction platform for dealer-to-dealer used vehicle sales, with bundled services like title processing, logistics, inspection reports, and financing
Mission: Increase trust and efficiency in the used car ecosystem using data-driven tools and modern infrastructure
Key Operations:

- Online auction platform (critical for revenue generation)
- Vehicle title team (requires secure, on-site printing)
- Inspection & logistics coordination (TrueGrade, Tim-Force Transport)
- Dealer financing (Tim-Force Capital)

Workforce Model: Mostly remote, but title processing depends on a single physical location housing expensive, secure printers
Key Assets: Marketplace platform, customer/dealer PII, sensitive financial data, secure title printers

---

Technical Profile – Security Posture and Controls

Controls in Place:

- MFA and SSO integrated with cloud IAM
- Endpoint Detection and Response (EDR) across employee devices
- Centralized SIEM with automated behavioral alerts
- Isolated production network for auction platform
- Routine vulnerability scans

Known Gaps or Weaknesses:

- Service accounts with limited monitoring and no MFA
- Inconsistent offboarding procedures
- Dependency on one facility for mission-critical printing
- Limited disaster recovery plans beyond cloud backups

Tabletop Exercise: Incident Response for Tim-Force

The Incident

Part 1 – The Repeating Breach (Day 1–2)

Tim-Force's SOC begins investigating an unusual pattern: Over the course of several days, they have seen a greater than average uptick in compromised accounts. Every time a compromised user account is secured, within 24 hours a few more show signs of unauthorized access. These new logins often appear from unusual geolocations or outside business hours.

Upon review, all affected users had interacted with a deprecated internal tool that had been integrated using a legacy service account—one that was exempt from MFA.

Further anomalies include:

- Failed login attempts followed by successful ones within minutes
- Temporary user accounts appearing in logs, then vanishing
- One account ("system.tempuser99") that appears in logins, but not in the IAM system. Note: The IAM is connected to the legacy system in question, using the MFA exempt legacy service account.

Student Prompts (Part 1):

- What initial actions should the incident response team take?
- How would you assess and contain the scope of the compromise?
- Should business operations be altered at this point?

Tabletop Exercise: Incident Response for Tim-Force

Part 2 – Persistent Ghost (Day 3–5)

Despite attempts to rotate credentials and disable the legacy service account, intrusions continue. The mysterious account (`system.tempuser99`) remains visible in log activity, interacting with non-production repositories and scanning internal documentation—particularly focused on title processing workflows.

Key complications emerge:

- Attempts to remove or disable the ghost user fail; new logs show reappearance within hours
- Security notices elevated—behavioral analysis suggests attacker is escalating access
- Title processing begins slowing down; job queues are stalling unexpectedly
- Internal communications hint that the attacker may be simulating or altering system behavior

Student Prompts (Part 2):

- What changes in your containment and response strategy now that persistence is confirmed?
- How do you verify attacker goals or exfiltration attempts?
- What risks emerge if title processing is delayed or disrupted further?
- When and how do you escalate internally and externally (e.g., executives, legal, partners)?