

Tim Force – Incident Response

Group 7 -

- Faraz Ahmed
- Pramath Yaji
- Rohan Dalvi
- Kathiresan Kandasamy
- Bhuvantej Ramachandra Reddy



Tim Force- Organization Overview

- It is a mid-sized, fast-growing technology company dealing with an online automotive marketplace.
- Helps in hosting a digital auction platform for used vehicle sales.
- Offers other services such as vehicle title processing, logistics coordination, Vehicle Inspection and dealer financing.
- Main aim is to build trust and efficiency in the used car ecosystem with some data-driven tools and modern infrastructure.
- Critical Resources of this organization includes the marketplace platform, sensitive customer and dealer data, financial data and secure title printer systems.



Tim Force- Risks or Weaknesses

Tim-Force often faces several operational and security risks.

- Service accounts are the special accounts with elevated permissions and access of sensitive information – Lack of Multi-factor Authentication (MFA) and limited monitoring.
- Offboarding procedures for departing employees are inconsistent – Potential risks of access control issues.
- The company heavily relies on a single physical facility for mission-critical vehicle title printing – when exhausted, leads to critical destruction of business operations.
- Disaster recovery planning is focused on the main cloud infrastructure – has limited resources for physical assets of security.



Tim Force- Controls in Place

Tim-Force has implemented several important cybersecurity controls to protect its operation and data.

- MFA and SSO are integrated with a Cloud-based IAM system – Helps in strengthening user and employee authentication and access management and security.
- Employee devices are made secure and safeguarded using EDR – Helps in monitoring any abnormal reading and malicious activities and threats.
- A centralized SIEM system – provides an automated alerts based on the attacker's behavior pattern.



The Incident...





The Recurring Breach (Day 1-2)

Tim-Force's SOC detected an abnormal and unusual pattern. An increase in user accounts got compromised.

Each time an account was secured, a new batch of unauthorized logins were recorded within 24 hours from different locations and time.

After a quick review, the security team found that all affected users utilized an outdated internal tool that was linked to a legacy service account and didn't have MFA configured.

Some anomalies include:

- An intermittent sequence of failed to successful attempts in login.
- Temporary user accounts that vanishes from the logs.
- An unidentified account ("system.tempuser99"), active in logins, absent in the overall IAM system.



Actions to be Taken

Disable the compromised legacy service accounts.

Back up critical accounts and system states.

Pull logs from IAM, legacy systems and firewalls.

Use SIEM tools like Splunk to study user behavior.

Containment –

Rotated Passwords.

Enforce MFA where possible.

Enable monitoring with alerts on critical systems.

Block suspicious IP addresses and geolocations using IDS/IPS.

Network Segmentation.

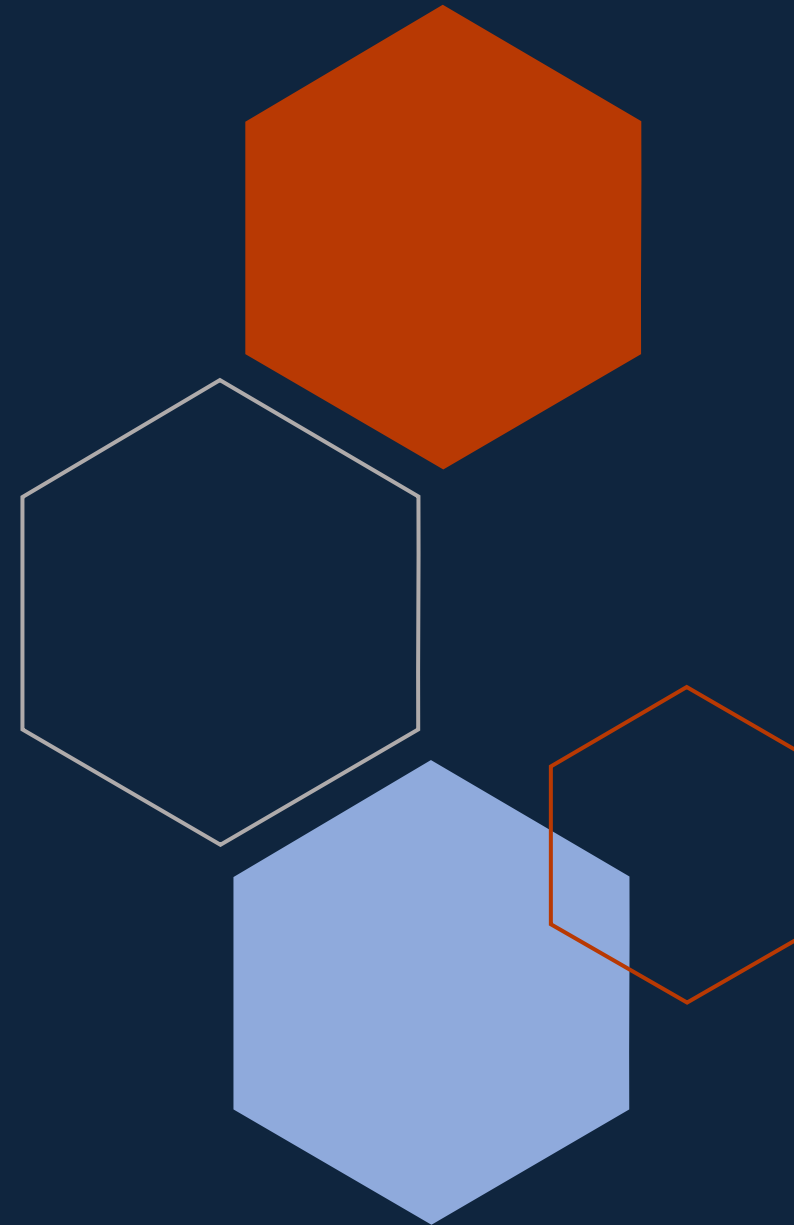
Should business operations be altered at this point?

No disruptions yet!

Critical Operations such as online auction platform and title processing should continue. These actions might possibly slow internal flow of operations.

Limit access to critical systems just to be safe.

Quietly tighten security controls internally.





Persistent Ghost (Day 3-5)

Despite efforts to rotate credentials and disable compromised legacy service account, intrusions continue.

The ghost account “system.tempuser99” remains conspicuous in logs.

Account interacts with non-production repositories and scanning internal documents that include title processing workflows.

- Attempts to remove or disable the account fail. It appears in new logs.
- Behavioral analysis suggests the attacker is escalating access.
- Title processing deteriorates, with a stave off in job queues.
- Internal communication indicates the attacker playing with the internal alerting system.



Actions to be Taken

Changes – Move to aggressive isolation

Immediately segment the network with title processing platform.

Eliminate persistence techniques.

Enable least-privilege access.

Identify the escalation of access tools that may be used.

To eradicate the threat, prepare for downtime.

Verifying exfiltration attempts –

Analysis of logs (SIEM).

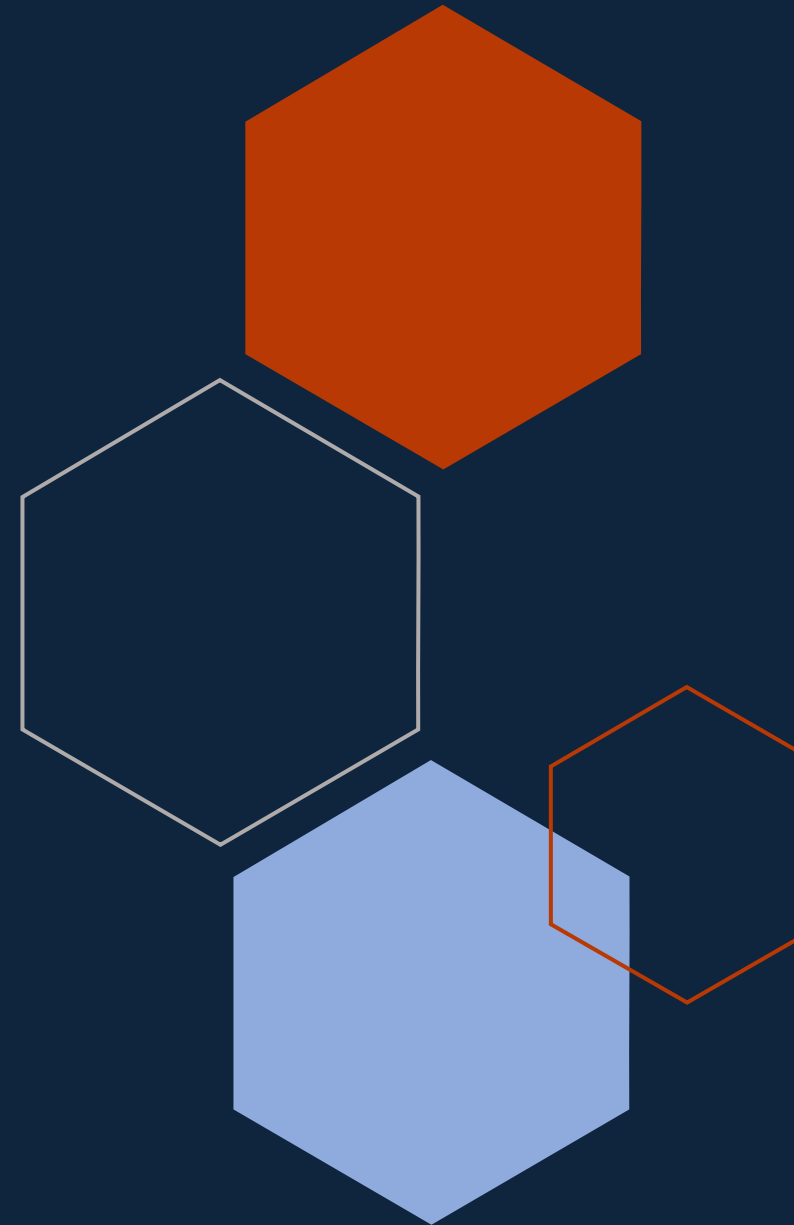
Network traffic analysis.

Use threat intelligence map.

Focus on exfiltration of title processing documents.

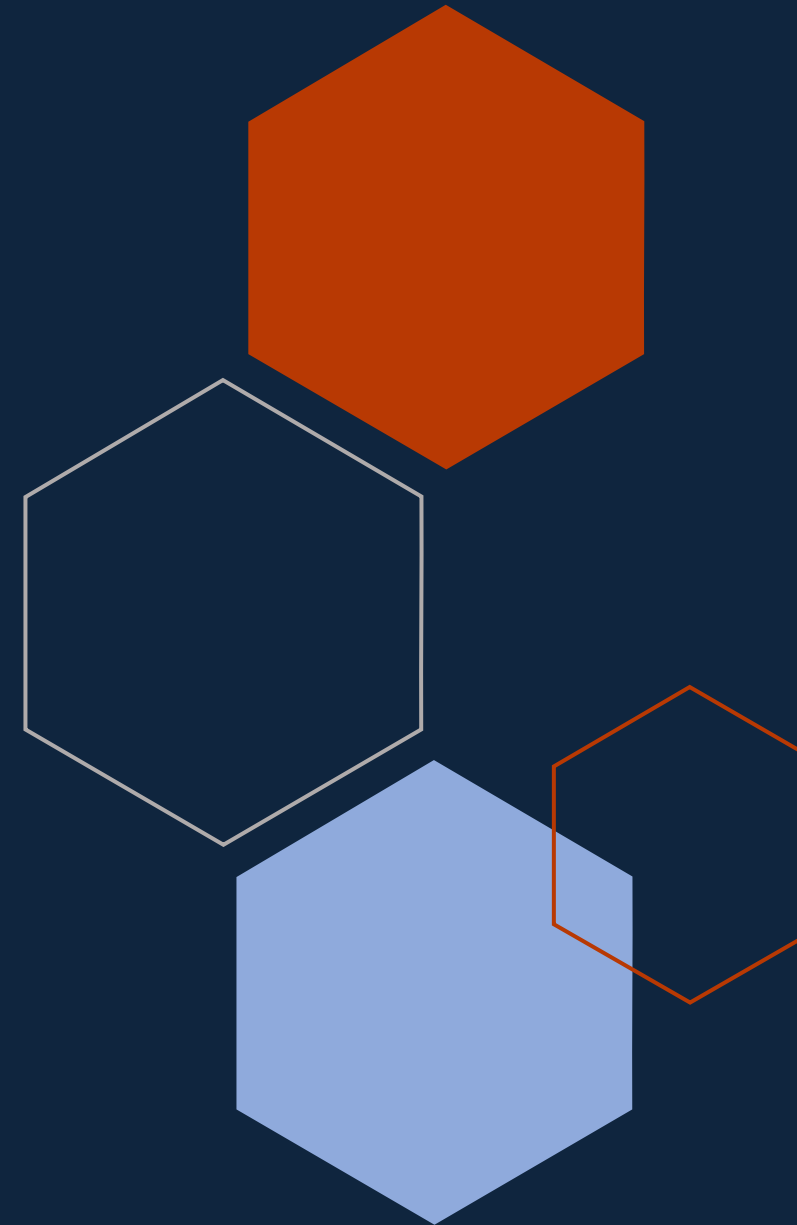
Risks in delayed and disrupted processing

- Loss of revenue – can halt sales.
- Customers dissatisfied – Dealers, and buyers may lose confidence.
- Reputational harm – Can lose future customers!
- Disruption of titles that involve PII and information of financial details could trigger penalties.



Escalating Internally & Externally

- Persistence was confirmed. ✓
- Internally notify CEO and CISO. Notify business owners.
- Externally notify Cyber Insurance if required and communicate with partners.
- Prepare communication with customers well ahead of time.





Recovery Stage

1. Restore Title Processing from verified backups.
2. Mandate MFA in every system.
3. Least Privilege.
4. Carefully reopen monitor the business operations.

Lessons Learned

- Attackers adapt fast.
- Legacy Systems are a huge risk.
- Improve detection and alerting – Must include anomaly detection.
- MANDATE MFA!



I AM READY TO GET HURT AGAIN



THANK YOU