BREACH INCIDENT RESPONSE PLAN

TRINITY SYSTEMS INC. -
INTERNATIONAL APPLE MAC RETAILER

CYBR3000, Gregory Stephens
Instructor: Sami Haji

Incident Overview

Incident: Unauthorized access and data exfiltration detected within Trinity Systems payment network.

Date & Time: March 8, 2025 – 02:13 AM

Detection: SOC identified suspicious API calls to external IP ranges.

Impact: Compromised customer records (2,140 entries – names, emails, partial card data).

Status: Confirmed critical breach – active investigation initiated.

Objective: Minimize financial and reputational damage, restore services securely.

Estimated incident cost impact: approx. $50K recovery, $20K in lost sales.

Trinity Systems

Incident Response Team

Top Layer:

CEO – Amanda Foster

CIO – Robert Chen

Incident Manager – Gregory Stephens

- Coordinates response, approves containment actions, liaises with executives.

Second Layer (reporting to Incident Manager):

- **SOC Lead** – Alex Tan
  - Monitors alerts, triages events
- **Network Engineer** – Samira Qureshi
  - Isolates affected segments
- **Forensic Analyst** – Ravi Patel
  - Preserves and analyzes evidence
- **PR / Communications** – Jordan Lee
  - Manages stakeholder and public communication
- **Legal Advisor** – Kara Nguyen
  - Handles compliance, notifies regulators

Trinity Systems

Policies & Procedures

- Frameworks: NIST SP 800-61 Rev 2 & ISO/IEC 27035-1.
- Response steps follow: Preparation → Detection → Containment → Eradication → Recovery → Post-Incident.
- All actions logged in Incident Management System (Splunk SOAR).
- Mandatory reporting within 24 hours of confirmation.
- Regular table-top exercises and SOC drills every quarter.
- Acceptable Use Policy: Defines authorized behavior and endpoint controls.
- Vendor Management Policy: Ensures third-party payment gateway compliance with PCI-DSS.

Trinity Systems

Detection & Analysis

- **Initial Indicators:** Outbound traffic spikes, multiple failed VPN logins, anomalous PowerShell execution.
- **Tools:** Splunk SIEM, FortiAnalyzer, and Zeek Network Monitor.
- **Timeline:** Detection at 02:13 AM, confirmed by 02:30 AM via hash correlation.
- **Root Cause:** Unpatched Apache vulnerability (CVE-2024-21713).
- **Evidence:** Logs, memory dumps, and packet captures secured in forensics vault.

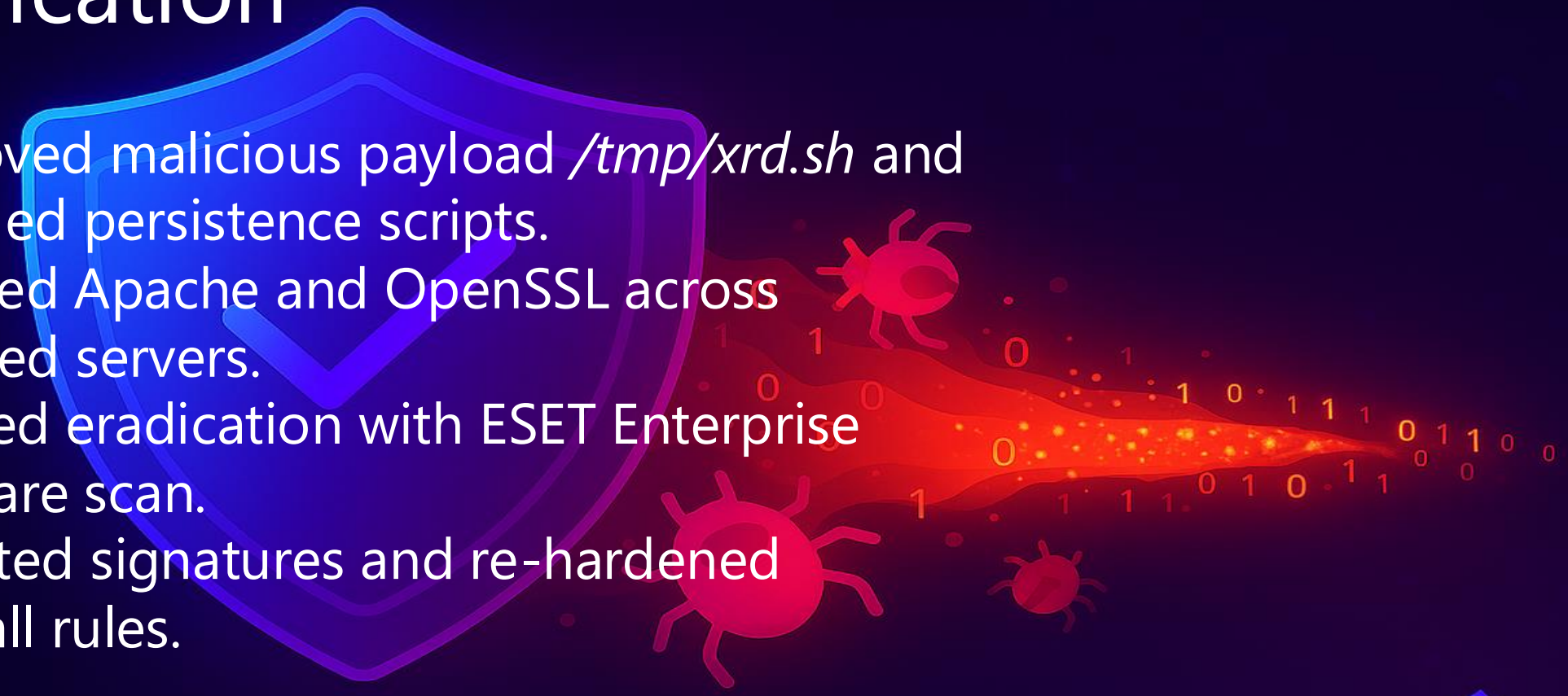
Trinity Systems

Containment

- **Short-term:** Isolated affected subnet 192.168.50.0/24 using FortiGate ACLs.
- **Long-term:** Disabled compromised admin accounts and revoked API tokens.
- **Data Protection:** Encrypted all backup archives and suspended cloud sync.
- **System Preservation:** Snapshots taken for forensic review.

Eradication

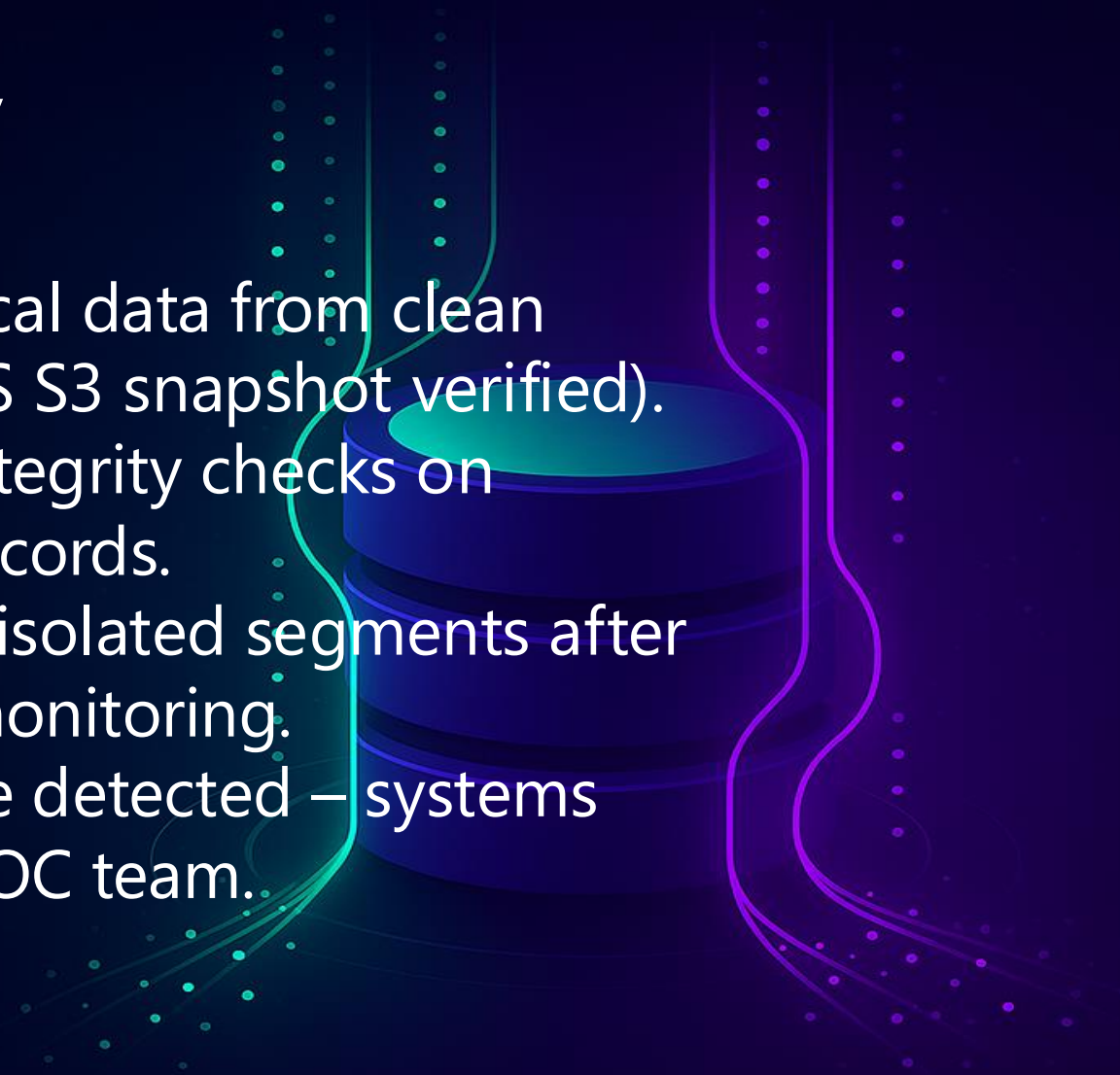
- Removed malicious payload */tmp/xrd.sh* and disabled persistence scripts.
- Patched Apache and OpenSSL across affected servers.
- Verified eradication with ESET Enterprise malware scan.
- Updated signatures and re-hardened firewall rules.



Trinity Systems

Recovery

- Restored critical data from clean backups (AWS S3 snapshot verified).
- Conducted integrity checks on transaction records.
- Reconnected isolated segments after 72 hours of monitoring.
- No recurrence detected – systems certified by SOC team.



Trinity Systems

Post-Incident Activity

- 72-hour post-mortem meeting conducted.
- Key findings: Delayed patch cycle and excessive privileges on admin accounts.
- Actions: MFA enforced organization-wide, IAM review initiated.
- Follow-up training for IT staff and awareness session for executives.

Trinity Systems

Legal & Regulatory Review

- Legal advised reporting under PIPEDA and GDPR.
- Notification to Office of the Privacy Commissioner completed within 72 hours.
- Preserved digital evidence per chain of custody requirements.
- Coordinated with law enforcement (Cybercrime Division RCMP).
- Media Spokesperson: Jordan Lee (PR / Communications) under Crisis Communication for compliance with rubric wording.

Trinity Systems

Crisis Communication

- Internal Notice sent to employees within 2 hours.
- Executive brief to board at 08:00 AM.
- External press release 24 hours post-incident.
- Client FAQs and credit monitoring offered.
- Social media posts reviewed by Legal and PR to ensure accuracy.

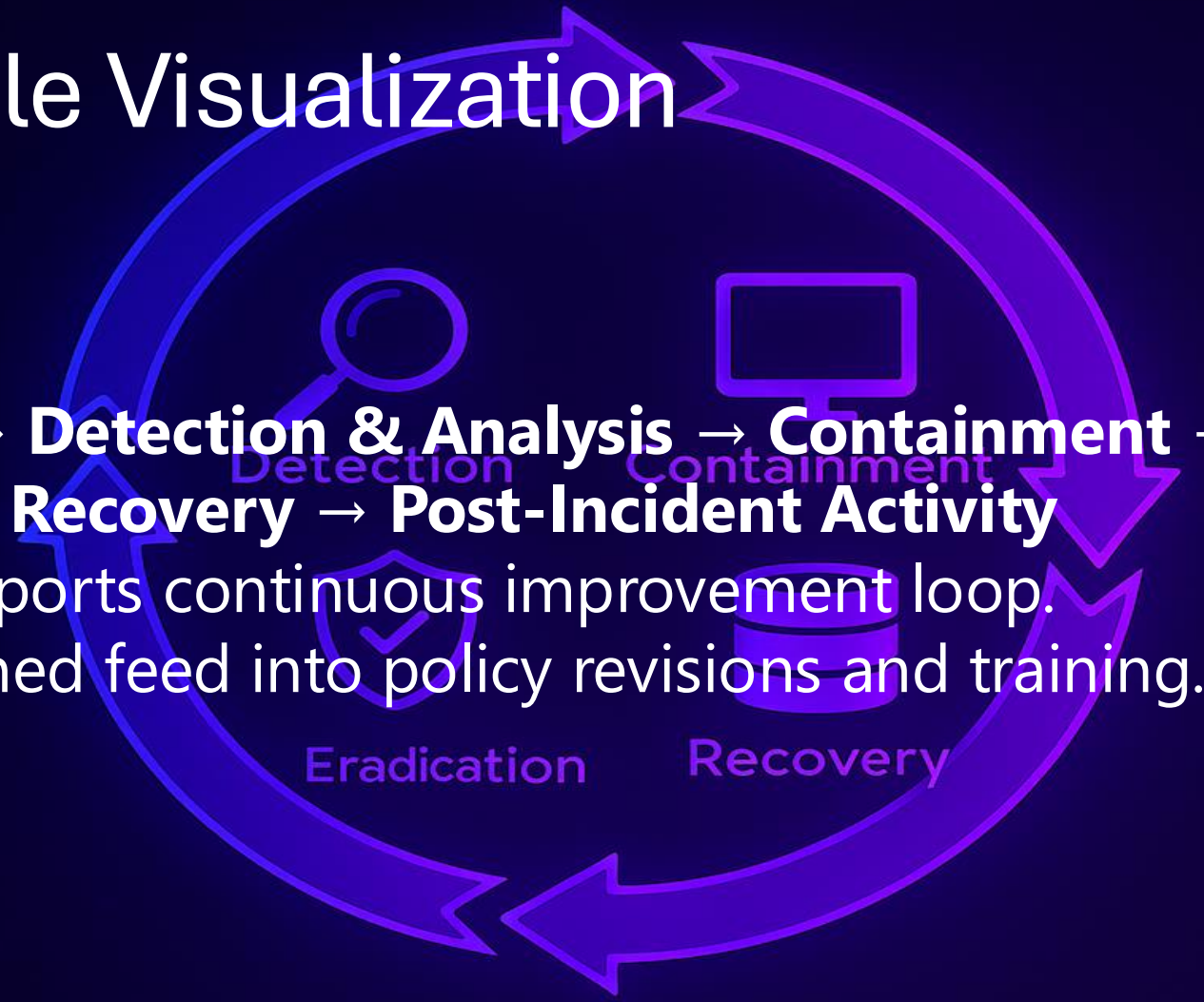
Trinity Systems

Stakeholder Notification Timeline

Time	Action	Responsible
0–1 hr	*Detection + Triage*	*SOC Lead*
1–3 hrs	*Isolation + Containment*	*Incident Manager*
3–8 hrs	*Forensic Preservation*	*Forensics Team*
8–12 hrs	*Legal + PR Review*	*Legal + PR*
12–24 hrs	*Public Disclosure*	*Executive Team*
24–72 hrs	*Recovery + Post Review*	*IR Team*

Trimity Systems

IR Lifecycle Visualization



Preparation → Detection & Analysis → Containment → Eradication → Recovery → Post-Incident Activity

- Lifecycle supports continuous improvement loop.
- Lessons learned feed into policy revisions and training.

Trinity Systems

References

- National Institute of Standards and Technology. (2012). *NIST SP 800-61 Rev. 2: Computer Security Incident Handling Guide*. Gaithersburg, MD.
- ISO/IEC 27035-1:2016. *Information security incident management — Principles of incident management*.
- Okta. (2023). *Identity as the New Security Perimeter*. White Paper.
- Fortinet. (2024). *Best Practices for Network Segmentation and Incident Response*.

Trinity Systems