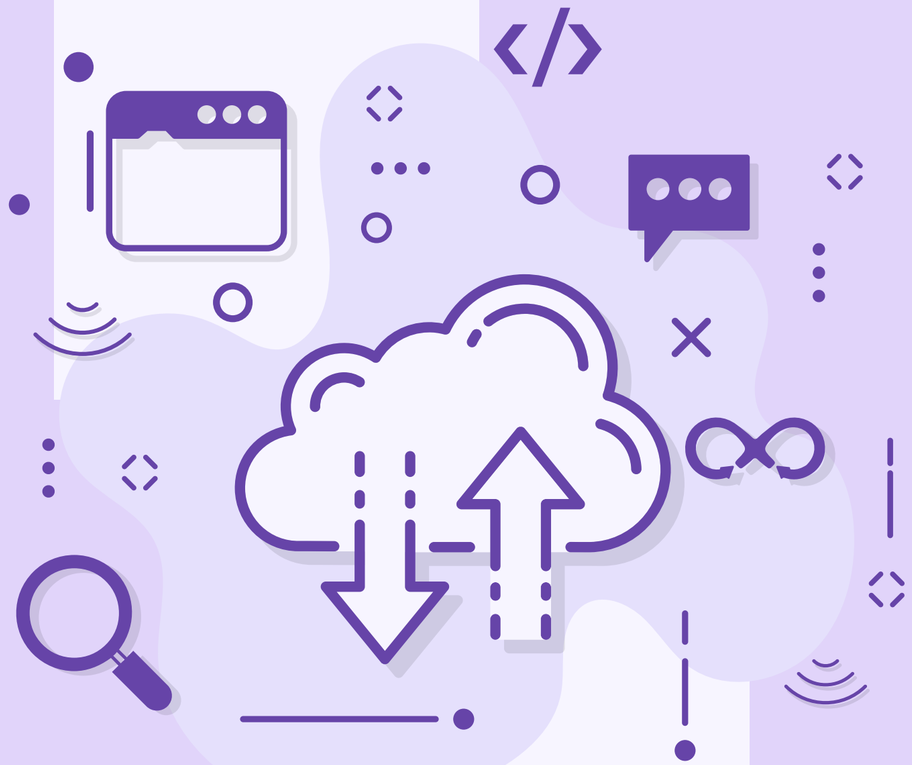
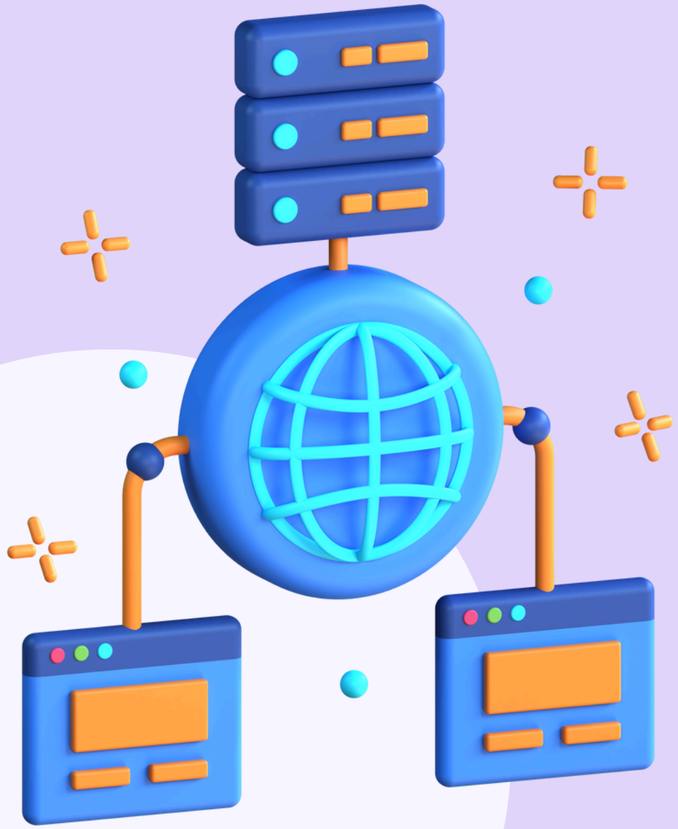


COMPROMISED DATA CENTRE AND CLOUD INFRASTRUCTURE

CyTrex Global Solutions Case Study

TABLE OF CONTENT



COMPROMISED DATA CENTRE & CLOUD INFRASTRUCTURE

CyTrex Global Solutions Case Study

- **Name**: Vrushabh Tak | Harsh Dilip Soni | Indrajeet Yadav

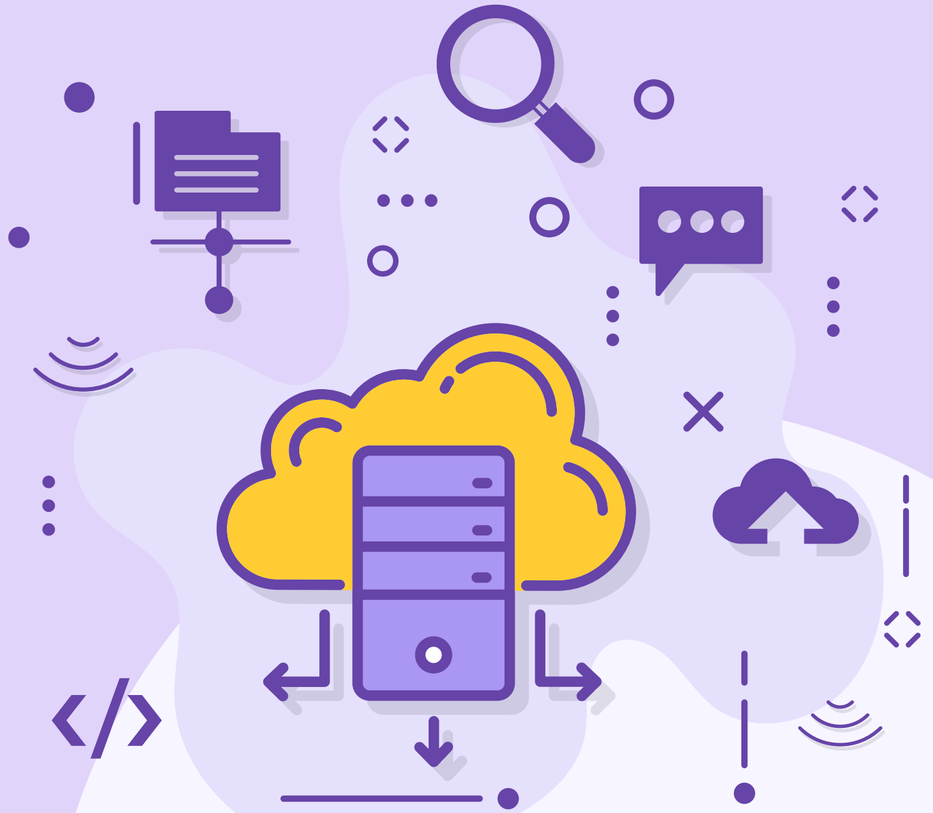
- **Date**: November 05, 2024

AGENDA

- **Incident Overview**: Introduction to the breach, explaining the key background information.
- **Key Events Timeline**: Chronological breakdown of the critical moments in the incident.
- **Task Assignments**: Discuss the roles and responsibilities of the response teams.
- **Policy and Governance Failures**: Identify gaps in current policies and how these contributed to the breach.
- **Tactics, Techniques, and Procedures (TTPs)**: Understanding how the attackers penetrated the systems.
- **CERT-IN Breach Notification and Regulatory Implications**: Legal and regulatory aspects surrounding the breach.
- **NIST 800-61 Incident Response Lifecycle**: A framework for managing and improving the response to such incidents.
- **Conclusion and Recommendations**: Key findings and suggested steps to prevent similar breaches.

INCIDENT OVERVIEW

- **Company**: CyTrex Global Solutions
- **Industry**: IT Services & Software Development
- **Location**: Global, with headquarters in the US and cloud services hosted in the EU
- **Incident Date**: October 12, 2024
- **Discovery Date**: October 14, 2024



INCIDENT STORY

- **Detection**: CyTrex's Security Operations Centre (SOC) noticed unusual outbound traffic and irregular access patterns.
- **Vulnerability Exploited**: Attackers exploited an unpatched firewall vulnerability (CVE-2024-XXXX).
- **Impact**:
  - Privilege escalation allowed attackers to gain unauthorized access to cloud services.
  - Exfiltration of sensitive customer data, including financial and personal information.
  - Deployment of ransomware on cloud-hosted virtual machines, demanding a cryptocurrency ransom.
  - Disruption of healthcare client services, impacting essential operations.

KEY EVENTS TIMELINE

- **Oct 10**: Firewall misconfiguration exposed a known vulnerability.
- **Oct 12**: Attackers exploited the vulnerability and escalated privileges within the data centre.
- **Oct 13**: Attackers moved laterally, compromising backup systems and encrypting critical data.
- **Oct 14**: SOC detected unusual network traffic and initiated the incident response protocol.
- **Oct 15**: Ransomware demand received, requesting 100 Bitcoin.

IDENTIFY POLICY / GOVERNANCE FAILURES

- **Ineffective Patch Management**: A failure to regularly update systems left critical vulnerabilities unpatched.
- **Insufficient Access Controls**: The absence of granular controls allowed attackers to escalate privileges once inside.
- **Lack of Secure Backups**: Backup systems were not isolated or encrypted, making them vulnerable to compromise.
- **Untested Incident Response Playbooks**: The lack of rehearsal of incident response plans led to delayed actions.
- **Inadequate Cloud Security Monitoring**: The absence of proactive monitoring allowed attackers to exploit cloud resources.

IDENTIFY TTPs

- **Initial Access (T1078)**: Exploitation of an unpatched firewall vulnerability.
- **Privilege Escalation (T1068)**: Attackers gained higher-level access once inside.
- **Lateral Movement (T1021)**: Attackers spread to other systems, including backup systems.
- **Exfiltration (T1041)**: Sensitive data was moved out of the network.
- **Impact (T1486)**: Ransomware encrypted systems, locking critical files.
- **Recommendations**:
  - Automate Patch Management to keep systems up-to-date.
  - Implement Least Privilege Access controls to minimize the damage potential.
  - Use Network Segmentation to isolate sensitive systems.
  - Deploy DLP (Data Loss Prevention) tools to monitor and protect sensitive data.
  - Use EDR (Endpoint Detection and Response) tools for better visibility and quicker responses.

CERT- IN BREACH NOTIFICATION AND OTHER REGULATORY IMPLICATIONS

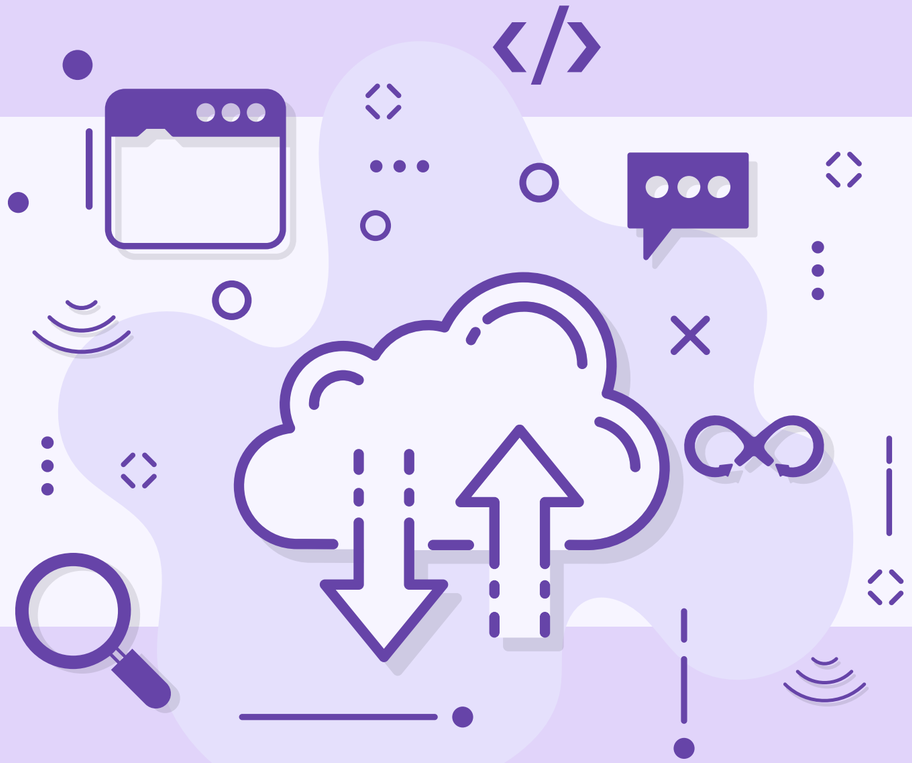
- **CERT-In Guidelines:**
  - Notify CERT-In within 6 hours of breach detection.
  - Provide specific incident details and actions taken.
  - Maintain ongoing updates to regulators until the breach is resolved.
- **GDPR Considerations**:
  - Notify affected individuals within 72 hours if sensitive data (e.g., financial data) is involved.
  - Penalties could include fines and reputational damage.
- **Penalties**:
  - Regulatory fines for non-compliance.
  - Contractual penalties from affected clients.
  - Long-term reputational damage to the company's credibility.

NIST 800-61 INCIDENT RESPONSE LIFECYCLE

- **Preparation**: Create and test incident response playbooks, conduct drills.
- **Detection and Analysis**: Improve threat detection systems and train SOC staff.
- **Containment**: Implement containment strategies for both immediate and long-term response.
- **Eradication**: Remove any malicious artifacts and restore clean backups.
- **Recovery**: Verify the integrity of restored systems and begin normal operations.

CONCLUSION AND RECOMMENDATIONS

- **Summary**:
  - A recap of the gaps in policy, identified TTPs, and regulatory considerations.
- **Actionable Insights**:
  - Staff Training: Regular training to ensure personnel know how to respond to incidents.
  - Continuous Monitoring: Enhance SOC capabilities to detect and prevent attacks.
  - Incident Response Testing: Regularly test response playbooks to ensure quick and effective action in future incidents.



THANK YOU