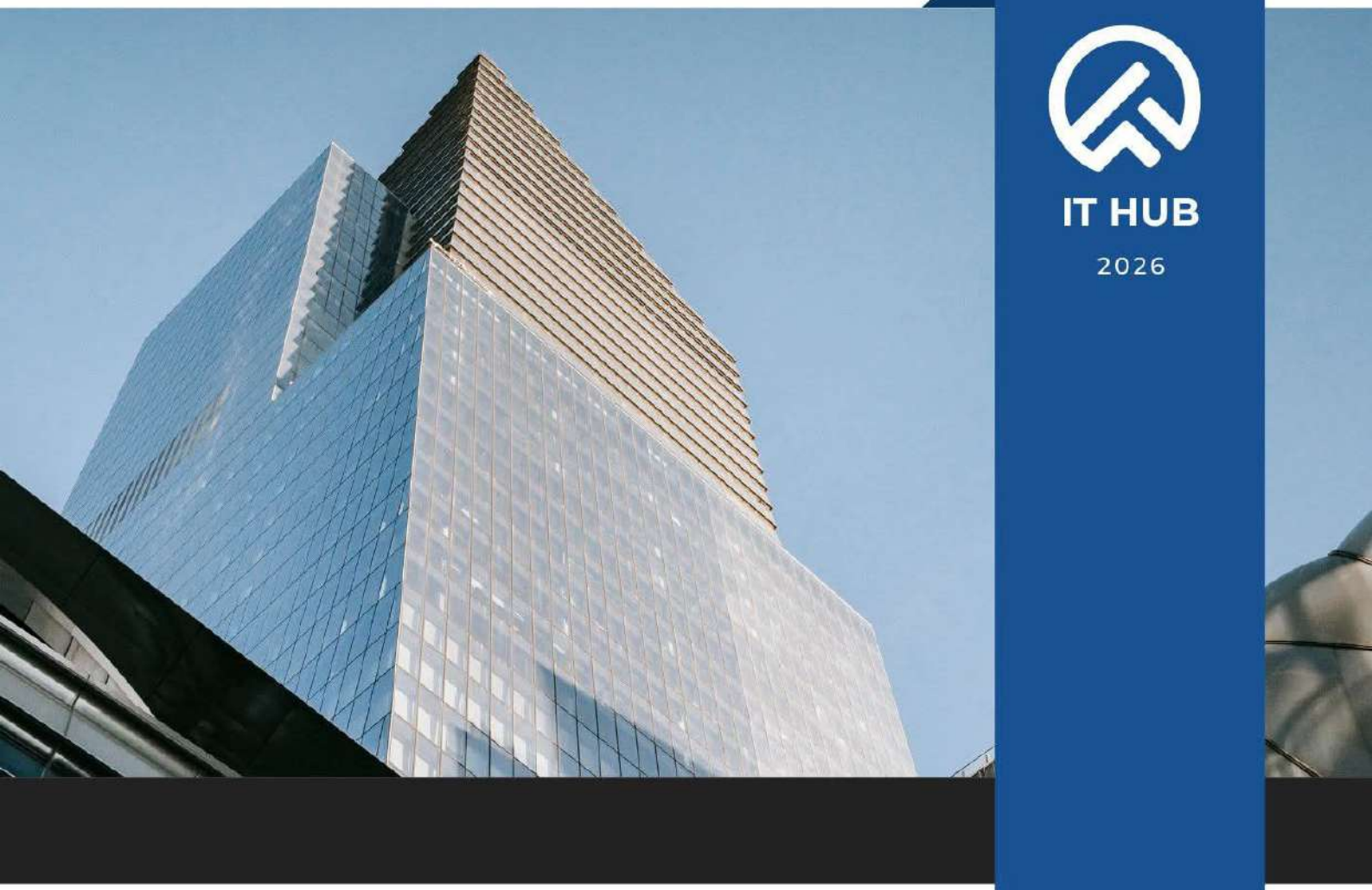

IT HUB

2026

SOC

INCIDENT RESPONSE PLAYBOOK 1

SOC Incident Response Playbook 1: Ransomware Infection

Scenario

An endpoint or server exhibits signs of ransomware activity such as file encryption, ransom notes or alerts from EDR/XDR tools.

Incident Classification

Category	Details
Incident Type	Malware – Ransomware
Severity	High
Priority	Critical (due to potential business impact and data loss)
Detection Sources	EDR/XDR, SIEM, User Report, Antivirus, NDR

Phases and Actions

1. Preparation (Pre-Incident Setup)

Task	Tool/Action
Backup and recovery strategy	Periodic offline backups, test restoration
Endpoint protection	EDR with behavioural detection and rollback features
User awareness training	Email and USB media handling education
Logging coverage	Windows logs, Sysmon, file access logs, network flows
IOC and threat feed subscriptions	Include ransomware-specific indicators

2. Detection & Analysis

Step	Action
Confirm ransomware activity	EDR alert, presence of ransom note, encrypted file extensions
Isolate affected host	Disconnect from the network or use EDR containment
Identify ransomware strain	Based on ransom note, file hash or filename pattern
Analyse logs and behaviour	Track source of execution, lateral movement, suspicious scheduled tasks or services
MITRE ATT&CK mapping	T1486 (Data Encrypted for Impact), T1059 (Command Execution), T1021.002 (SMB Lateral Movement)

3. Containment

Step	Action
Isolate affected systems	Block at switch, firewall or via EDR
Disable infected accounts	Especially if used for lateral movement
Block external communication	Prevent C2 and key exchange over the internet
Snapshot impacted systems	For forensic analysis (if required)

4. Eradication

Step	Action
Remove malware artifacts	Delete ransomware files, scripts, scheduled tasks
Patch vulnerabilities	Address exploited attack vectors such as RDP, SMB, outdated software
Perform full antivirus/EDR scan	Across all hosts within affected VLAN/subnet
Validate removal	Ensure no persistence mechanisms remain (registry keys, startup items, services)

5. Recovery

Step	Action
Restore from clean backup	Confirm backups are unaffected before restoration
Rebuild systems if needed	For systems without clean backups
Monitor restored systems	Use SIEM and EDR to ensure no reinfection occurs
Reset passwords	Particularly for privileged and affected users

6. Lessons Learned & Reporting

Step	Action
Conduct post-incident review	Analyse root cause, initial access method and response efficiency
Update detection rules	Enhance SIEM and EDR correlation rules and triggers
Document findings	Include indicators, affected systems and timeline
Share IOCs	Internally and with threat intel communities if allowed

Tools Typically Involved

- SIEM (e.g., Splunk, QRadar, Sentinel)
- EDR/XDR (e.g., CrowdStrike, Cortex XDR, SentinelOne)
- Forensics tools (e.g., FTK, Velociraptor, KAPE)
- Network logs (e.g., Zeek, Suricata, NetFlow)
- Backup systems (e.g., Veeam, Rubrik, Commvault)