Building a Ransomware Response Plan with Fidelis Elevate XDR: Technical Guide

Ransomware attacks are projected to occur every 2 seconds by 2031, up from every 11 seconds in 2021. Organizations paid approximately $813.55 million to ransomware groups in 2024. Email remains the primary attack vector, with malicious attachments twice as common as phishing links. Organizations with compromised backups face $3M average recovery costs, with 45% requiring more than a month to recover. Active ransomware groups increased 55% from Q1 2023 (29) to Q1 2024 (45).

Ransomware Attack Methodology: MITRE ATT&CK Framework

Modern ransomware attacks follow a systematic approach:

1. **Reconnaissance**: Information gathering about target systems
2. **Resource Development**: Creating tools and establishing infrastructure
3. **Initial Access**: Entry via phishing, vulnerabilities, compromised credentials
4. **Execution**: Running malicious code in the target environment
5. **Persistence**: Establishing backdoors for sustained access
6. **Privilege Escalation**: Gaining higher system permissions
7. **Defense Evasion**: Bypassing security controls
8. **Credential Access**: Stealing authentication credentials
9. **Discovery**: Mapping environment for valuable assets
10. **Lateral Movement**: Spreading through network
11. **Collection**: Gathering sensitive data
12. **Command and Control**: Establishing communication channels
13. **Exfiltration**: Transferring data to attacker-controlled locations
14. **Impact**: Deploying ransomware encryption

Response Plan Components with Fidelis Elevate XDR

1. Preparation Phase

Asset Inventory and Risk Assessment:

- Implement continuous terrain mapping for asset inventory
- Apply risk profiling for critical systems identification
- Deploy Network Detection and Response (NDR) across all ports/protocols

Security Controls:

- Deploy Endpoint Detection and Response (EDR) on all endpoints
- Implement Deception technology for early attacker detection
- Configure Active Directory Intercept for AD vulnerability mitigation

Backup Strategy:

- Establish offline/secure backups with frequent updates

- Monitor data traffic for backup sabotage attempts
- Test recovery processes regularly

2. Detection Phase

Real-Time Monitoring:

- Configure XDR across all environments
- Utilize Deep Session Inspection for nested files and encrypted traffic
- Leverage MITRE ATT&CK integration for ransomware pattern identification

Threat Hunting:

- Search for indicators of compromise (IoCs)
- Use anomaly detection for early-stage activity
- Analyze metadata from previous sessions for malware exposure

Incident Triage:

- Correlate alerts across multiple detection points
- Validate incidents between endpoint and network data
- Use Deception technology for high-fidelity alerts

3. Containment Phase

Rapid Isolation:

- Quarantine compromised systems via automated response
- Implement pre-configured containment playbooks
- Block command-and-control communications

Limiting Lateral Movement:

- Deploy deception breadcrumbs and decoys
- Monitor for credential theft and suspicious account activities
- Implement network segmentation based on visibility data

Preventing Data Exfiltration:

- Utilize data loss prevention capabilities
- Analyze for abnormal data transfers in real-time
- Monitor cloud environments for unauthorized access

4. Eradication Phase

Malware Removal:

- Identify and remove ransomware binaries
- Perform retrospective analysis for persistence mechanisms
- Analyze suspicious files for behavior determination

Security Gap Remediation:

- Detect system misconfigurations

- Implement immediate patching and hardening
- Remediate AD-related vulnerabilities

Credential Reset:

- Identify compromised credentials through usage pattern monitoring
- Reset passwords and implement stricter access controls
- Review security permissions using least privilege principle

5. Recovery Phase

System Restoration:

- Restore from clean backups verified by integrity monitoring
- Prioritize restoration based on asset criticality
- Implement phased system recovery approach

Verification and Monitoring:

- Scan restored systems thoroughly
- Implement continuous monitoring for reinfection detection
- Deploy Deception to identify persistent attacker presence

- Suggested Reading: 10 Deployment Considerations for your Deception Strategy

6. Post-Incident Phase

Forensic Analysis:

- Analyze attack timeline using metadata collection
- Identify initial access vector and attack progression
- Document tactics, techniques, and procedures (TTPs)

Lessons Learned:

- Identify security control gaps
- Review containment measure effectiveness
- Update security policies based on findings

Your Complete Ransomware Defense Blueprint, Powered by Fidelis XDR

Download the Fidelis guide to building a resilient ransomware defense framework with integrated XDR.

- Ransomware trends and tactics
- MITRE ATT&CK-aligned detection and response strategies
- XDR-driven best practices

Download the Whitepaper

Key Fidelis Elevate XDR Capabilities

Comprehensive Visibility and Contextual Mapping

- Fidelis Elevate provides continuous cyber terrain mapping and risk analysis, enabling organizations to maintain a real-time inventory of all assets-including managed and unmanaged devices, network traffic across all ports and protocols, and cloud resources.
- Patented Deep Session Inspection® delivers granular content and context beyond standard netflow, eliminating blind spots and enhancing network data loss prevention (DLP).

Integrated Deception Technology

- The platform employs deception techniques such as traps, decoys, and breadcrumbs to lure attackers, reveal their presence, and divert them from real assets.
- Deception is dynamically deployed, increasing attacker costs and risks while giving defenders the advantage to study attacker behavior and fortify defenses.

Unified Detection and Response Across Domains

- Fidelis Elevate integrates mature network, endpoint, and deception capabilities, offering holistic visibility and control across networks, endpoints, cloud, and users.
- Real-time and retrospective analysis on rich metadata enables detection and response at every step of the attack kill chain, including advanced threats and lateral movement.

Active Directory Defense

- The platform uniquely provides comprehensive Active Directory defense, identifying misconfigurations, monitoring for exploitation (e.g., brute force, abnormal ticket requests), and offering remediation interfaces.

Automated, Contextual Threat Detection and Response

- Automated defenses detect and alert in real-time, with instrumentation and monitoring across all environments (on-premises, cloud, hybrid).
- Automated playbooks and AI/ML-powered detections accelerate investigation, containment, and recovery.

Open XDR Architecture and Integration

- Fidelis Elevate is an open XDR solution, supporting integration with third-party EDR and security tools, preserving existing security investments and enabling flexible, tailored deployments.
- The CommandPost interface centralizes security configuration, management, and retrospective analysis.

Proactive Threat Hunting and Intelligence

- The platform leverages MITRE ATT&CK mappings, threat intelligence, and machine learning for predictive analysis, enabling proactive threat hunting and early-stage ransomware detection.

Endpoint Detection and Response (EDR)

Provides deep endpoint visibility, automated investigation, rapid quarantine, and on/off-network protection.

Data Loss Prevention and Exfiltration Control

- Combines threat detection, asset discovery, and deception to prevent data exfiltration, leveraging powerful DLP and anti-malware engines.

Operational Benefits

- 360° threat visualization, automated correlation of weak signals, and consistent policy enforcement across the enterprise.
- Multi-faceted professional support and role-based training resources.

Implementation Best Practices

1. Establish Clear Command Structures

- Define roles and responsibilities for all stakeholders involved in incident response.
- Set up escalation procedures based on alert severity and create decision matrices for critical actions.

2. Develop and Maintain Response Playbooks

- Create detailed, scenario-specific response playbooks for ransomware and related threats.
- Automate common response actions and regularly test playbooks through exercises and simulations to ensure readiness.

3. Enable Continuous Monitoring and Threat Hunting

- Implement real-time and retrospective analysis to detect both known and emerging threats.
- Regularly update detection rules and conduct periodic assessments of security controls to adapt to evolving ransomware tactics.

4. Secure Communications Protocols

- Establish out-of-band communication channels for use during incidents when standard systems may be compromised.
- Utilize secure command and control capabilities to coordinate response activities.

5. Integrate External Resources and Partnerships

- Build relationships with forensic experts and incident response partners before an incident occurs.
- Define protocols for communicating with external authorities and ensure cyber insurance requirements are addressed.

6. Enforce Security and Configuration Best Practices

- Continuously monitor and enforce configuration compliance and vulnerability

management across assets.
- Apply network segmentation to isolate critical systems and contain lateral movement during attacks.

7. Regularly Validate and Update Backups

- Maintain secure, offline backups and test recovery procedures frequently to ensure data integrity and rapid restoration.

8. Strengthen Identity and Access Management

- Enforce strong password policies, multi-factor authentication, and least-privilege access principles to reduce credential-related risks.

9. Provide Ongoing Training and Awareness

- Conduct regular training for security teams and end-users on ransomware tactics, phishing, and best practices for incident response.

By following these best practices and leveraging Fidelis Elevate XDR's integrated, proactive capabilities, organizations can build a resilient ransomware response plan that detects, contains, and neutralizes threats before they impact critical operations.

Conclusion

Ransomware attacks require comprehensive response capabilities. Fidelis Elevate XDR provides technology to detect early-stage ransomware, contain threats before network-wide spread, recover from attacks, and improve security posture. An effective ransomware response plan combines defined processes with XDR technology for resilience against evolving threats.

Explore how Fidelis Security can help you!

Talk to an Expert