6 Stages in a Threat Intelligence Lifecycle: Where Does Fidelis Fit In?

Key Takeaways

- **The cybersecurity lifecycle operates through five stages** (Identify, Protect, Detect, Respond, Recover) while threat intelligence follows a six-phase intelligence cycle that transforms raw data into actionable intelligence for proactive defense.
- **Threat intelligence serves as strategic connective tissue** linking cybersecurity investments with tactical operations, enabling security teams to understand attack lifecycle patterns and implement targeted countermeasures.
- **Effective incident management lifecycle phases** require systematic preparation, detection, containment, and recovery procedures supported by continuous threat intelligence feedback loops.
- **Modern organizations need unified platforms** that integrate network, endpoint, and cloud security rather than managing multiple disparate tools across hybrid environments.
- **Fidelis Elevate XDR and Halo CNAPP deliver integrated threat intelligence capabilities** that unify the complete intelligence lifecycle across traditional and cloud infrastructure.

Contemporary threat actors employ sophisticated methodologies to execute advanced persistent threats that may remain undetected for extended periods. The evolving threat landscape necessitates comprehensive threat intelligence programs capable of transforming raw data into strategic threat intelligence. Organizations require structured processes that enable proactive security measures rather than reactive responses to cyber threats.

Intelligence Cycle Framework

The cyber threat intelligence lifecycle establishes a systematic framework for converting raw data collected into relevant intelligence through a structured process. This threat intelligence lifecycle framework enables security teams to implement operational threat intelligence capabilities. The intelligence cycle ensures continuous feedback mechanisms that enhance threat detection and response across hybrid environments.

Understanding why the threat intelligence lifecycle important extends beyond theoretical knowledge. Modern enterprises deploying comprehensive threat intelligence services require platforms supporting each phase effectively. Fidelis solutions integrate within this structured process to deliver actionable threat intelligence across traditional and cloud infrastructures.

Stage 1: Direction and Planning

The direction phase establishes foundational requirements for effective intelligence lifecycle operations. Threat intelligence teams collaborate with stakeholders to define strategic threat intelligence requirements and identify critical assets. This structured process ensures security investments align with actual business risks within the current threat landscape.

Fidelis Elevate XDR provides comprehensive terrain mapping and risk analysis that supports planning initiatives. The platform maintains accurate asset inventories across hybrid computing environments through continuous discovery capabilities. This visibility enables threat

intelligence teams to understand attack surfaces and prioritize security efforts effectively.

Fidelis Halo CNAPP enhances planning through automated inventory management of IaaS resources across AWS, Azure, and GCP environments. This cloud visibility enables security teams to focus their threat intelligence program on high-risk assets. The platform identifies configuration vulnerabilities that threat actors commonly exploit to establish persistence.

Stage 2: Collection

Raw data collection encompasses network traffic analysis, endpoint telemetry, cloud configurations, and identity events essential for operational threat intelligence. Effective threat intelligence services require comprehensive data gathering across attack vectors to detect sophisticated cyber threats. This collection phase forms the foundation for subsequent intelligence cycle activities.

Collection Capabilities:

- **Fidelis Network**: Captures sessions using patented Deep Session Inspection technology
- **Fidelis Endpoint**: Aggregates detailed telemetry from Windows, Linux, and Mac systems
- Fidelis Halo: Collects cloud data through agentless API connectors

Fidelis Elevate correlates these diverse data streams into unified datasets essential for actionable threat intelligence generation. This integrated methodology eliminates visibility gaps that emerge when security tools operate independently. The correlation transforms raw data collected into structured threat intelligence feeds suitable for analysis.

Stage 3: Processing and Enrichment

Raw data requires normalization, deduplication, and contextualization before becoming operationally useful. The processing stage transforms information into structured formats enabling effective pattern recognition within the intelligence cycle. This transformation converts unstructured data into actionable threat intelligence for security teams.

Fidelis Elevate excels through advanced enrichment engines integrating asset risk data, terrain mapping, and external threat intelligence feeds. The platform automatically enriches security events with contextual details including criticality assessments and behavior patterns. Machine learning algorithms identify subtle patterns that manual analysis might overlook, transforming emerging threats into relevant intelligence.

Fidelis Halo contributes through contextual cloud enrichment mapping risks to MITRE ATT&CK framework. The platform enriches events with sensitivity levels, compliance posture, and configuration drift information. This enrichment enables tactical threat intelligence applications prioritizing potential threats based on business impact.

Stage 4: Analysis and Production

Analysis transforms processed data into actionable threat intelligence through pattern recognition and risk prioritization. Advanced operations combine human expertise with automated analytics to identify attack patterns and assess business impact. This stage converts enriched data into tactical threat intelligence guiding security measures and operational decisions.

Analysis Capabilities:

- **Elevate XDR:** MITRE ATT&CK-based automated models correlating weak signals into high-confidence detections
- **Active Threat Detection**: Detailed event context and timelines streamlining investigation workflows
- **Halo CNAPP**: Cloud-native threat detection identifying IAM abuse and lateral movement
- **AD Intercept**: Identity-based threat analysis combining network detection with deception technology

These solutions extend beyond detecting potential threats by correlating intelligence across

environments. This contextual analysis supports informed response decisions enabling security teams to prioritize security efforts effectively. The integrated approach ensures actionable threat intelligence reaches decision-makers in formats supporting rapid responses.

Stage 5: Dissemination

Effective threat intelligence must reach appropriate stakeholders promptly to enable rapid response actions. The dissemination phase distributes intelligence across systems while ensuring decision-makers receive actionable formats. This distribution ensures relevant intelligence reaches operational teams responsible for implementing security measures.

Fidelis Elevate ARM (Automated Response & Mitigation) distributes indicators to enforcement points and triggers automated responses. The platform integrates with leading SIEM, SOAR, and threat intelligence platforms including Splunk, IBM QRadar, and Cortex XDR. This automation enables consistent enforcement across security infrastructures without manual intervention.

Fidelis Halo exports cloud security alerts to SIEM platforms, ticketing systems, and messaging applications. The platform's REST API enables custom integrations with DevOps tools and CICD pipelines. This comprehensive dissemination ensures accelerated response times and consistent application across hybrid environments.

Stage 6: Feedback and Integration

The final intelligence cycle phase validates effectiveness through performance metrics and feedback analysis. Organizations monitor dwell time, false positive rates, and response effectiveness to refine their threat intelligence lifecycle framework. This feedback ensures security investments produce measurable improvements in threat detection capabilities.

Fidelis Elevate provides comprehensive metrics including dwell time analysis and detection accuracy measurements. Security teams monitor these metrics to refine response playbooks based on empirical performance data. Retrospective analysis capabilities enable threat hunting teams to investigate historical data and identify previously undetected threats.

Fidelis Halo monitors cloud configuration drift and compliance trends providing feedback on security posture changes. The platform tracks remediation efforts measuring configuration improvements over time. This continuous feedback enables organizations to maintain superiority over emerging threats by refining detection capabilities.

Comprehensive Solution Integration

Fidelis Security delivers complete cyber threat intelligence lifecycle support through complementary XDR and CNAPP platforms. Rather than managing separate vendor relationships, organizations benefit from unified strategy eliminating complexity. This approach ensures coverage spanning traditional infrastructure and modern cloud environments.

Platform Synergy:

- **Elevate XDR:** Correlation engine for network, endpoint, and identity layers with extensive integration capabilities
- **Halo CNAPP:** Cloud visibility, posture management, and container security across application stacks

Common integration frameworks enable both platforms to feed data into centralized operations

platforms creating unified visibility. Security teams correlate network-based indicators with cloud configuration risks through existing SIEM integrations. This provides comprehensive threat context without custom development while enabling tactical threat intelligence across diverse environments.

The cyber threat intelligence lifecycle delivers maximum value when supported by integrated security tools unifying collection, analysis, and response capabilities. Organizations implementing mature threat intelligence programs require platforms eliminating visibility gaps and providing actionable intelligence driving informed security decisions. These capabilities ensure security devices and security controls work cohesively protecting against advanced persistent threats.

Discover how Fidelis Elevate XDR and Fidelis Halo CNAPP unify your threat intelligence lifecycle from strategic planning through operational improvement. These platforms transform raw data into actionable threat intelligence while automating response capabilities maintaining superiority over evolving cyber threats.

Request a personalized demo or explore our latest threat defense solutions to discover how comprehensive threat intelligence integration strengthens security posture and accelerates threat response across your infrastructure.

Give Us 10 Minutes – We’ll Show You the Future of Security

See why security teams trust Fidelis to:

- Cut threat detection time by 9x
- Simplify security operations
- Provide unmatched visibility and control

Book a Demo Now!