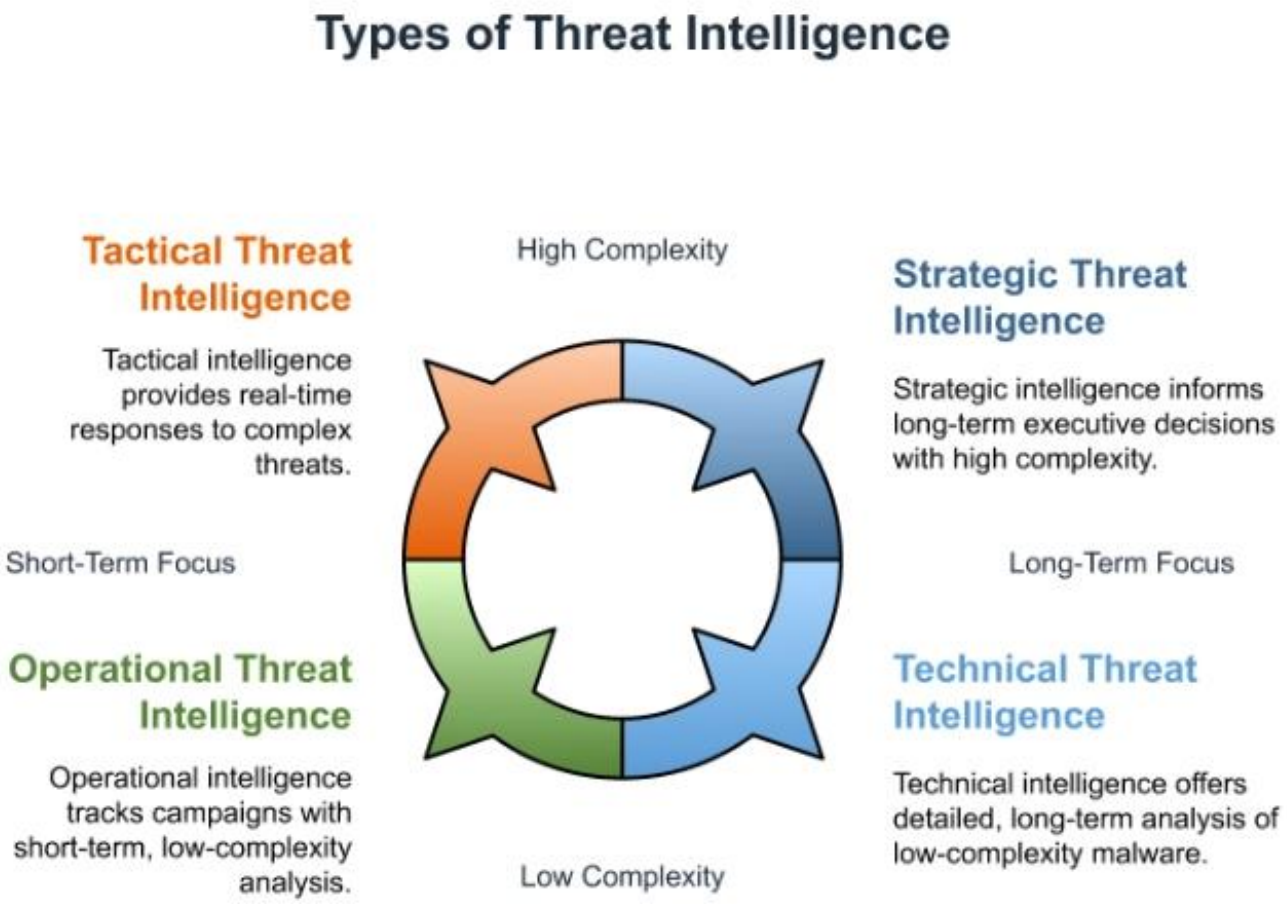
Types of Threat Intelligence: Complete Guide for Cyber Security Intelligence

Ransomware hits an organization every eleven seconds. Healthcare systems are particularly vulnerable; 90% report ransomware and DDoS attacks targeting their high-value medical data and critical patient services. Strategic and operational threat intelligence is essential to proactively protect them.

Modern cyber threat intelligence goes beyond basic indicator feeds. Security teams work with four distinct types of threat intelligence, each serving different functions and timeframes. Understanding these differences helps build actionable threat intelligence programs and effective defense strategies.



Strategic Threat Intelligence: Executive Decision Making for Cyber Risk Management

Strategic threat intelligence informs executive decisions over 6-18 months. CISOs use this

intelligence to justify budgets, infrastructure investments, and policy changes to boards and executive teams. This type of threat intelligence focuses on long-term security posture improvements.

Healthcare faces increasing threats as cybercriminals recognize medical facilities as high-value targets. These organizations historically pay ransoms quickly to restore patient services. Strategic intelligence drives executive decisions about Zero Trust implementations and comprehensive security architectures.

Board presentations need intelligence that connects cyber threats to business risks. Strategic threat intelligence quantifies operational disruptions, compliance impacts, and reputational damage. This helps executives understand why perimeter-based security fails against evolving threats.

The process involves analyzing geopolitical factors, industry trends, and threat actor evolution. Security professionals translate technical assessments into business language for executives focused on operational continuity and cyber risk mitigation.

Operational Threat Intelligence: Campaign Tracking and Threat Actor Analysis

Operational threat intelligence tracks specific threat campaigns over 1-6 months. Security teams and threat hunters use this intelligence to understand sustained adversary operations against their industry or region. This intelligence type bridges strategic planning with tactical response capabilities.

This analysis produces detailed threat actor profiles including preferred attack vectors, timing patterns, and target selection methods. Security professionals can position defenses proactively to disrupt attack sequences and stay ahead of emerging threats.

Advanced threat intelligence programs integrate deception capabilities to study adversary behaviors. Fidelis Elevate uses automated deception layers that distract attackers while defenders study their tactics, techniques and procedures. When threat actors interact with decoys, organizations gather behavioral intelligence and buy time for additional protections.

Campaign analysis shows how attackers adapt across different targets and environments. Understanding these adaptations helps security teams anticipate variations and prepare countermeasures against future attacks.

Analysis extends beyond individual campaigns to identify relationships between threat groups and operational patterns. This perspective helps organizations understand the threat landscape affecting their industry and prepare for advanced persistent threats.

Tactical Threat Intelligence: Real-Time Threat Detection and Response

Tactical threat intelligence provides actionable intelligence for real-time security operations. SOC analysts use this for alert triage, threat hunting, and rapid incident response within real-time to weekly cycles. This intelligence type focuses on immediate threats and active threat detection.

Traditional tactical intelligence included basic indicators like malicious IP addresses, domains, and file hashes. Modern approaches use behavioral rules that identify suspicious activities even when technical indicators change, enabling detection of advanced persistent threats.

Fidelis Elevate demonstrates advanced integration by correlating weak signals from multiple sources. The platform uses automated models based on MITRE ATT&CK to produce high-confidence detections while reducing alert fatigue through intelligent filtering of threat data.

Behavioral rules map to established attack frameworks, giving security teams contextual awareness about adversary progression. Teams understand what happened and where attacks might go next, accelerating response decisions and enabling effective containment of cyber attacks.

Integration ensures tactical intelligence flows across diverse security tools. Network detection, endpoint protection, and cloud security controls share threat intelligence data automatically, creating unified responses without manual coordination.

Machine learning identifies anomalous behaviors indicative of advanced persistent threats, helping detect sophisticated attacks that evade signature-based detection and providing actionable insights for security incidents.

Technical Threat Intelligence: Deep Malware Analysis and Vulnerability Research

Technical threat intelligence provides malware analysis, vulnerability research, and detailed attack documentation. Forensics specialists, malware analysts, and incident response teams use this for investigation, attribution, and countermeasure development against specific cyber threats.

Malware analysis reports detail functionality, persistence mechanisms, C2 protocols, and evasion techniques. Security teams use this information to understand compromise scope and develop targeted remediation strategies for cybersecurity threats.

Sandbox environments execute suspicious files under controlled conditions mimicking operational environments. These systems observe behavioral patterns, network communications, and system modifications. Fidelis Insight includes the Content Analysis Platform with sandbox execution and active networking, allowing malware to communicate as in actual environments.

Analysis extends beyond basic execution to behavioral scoring. Malware scores range 0-100, with higher scores indicating greater confidence in malicious activity requiring immediate incident response.

Vulnerability intelligence tracks active exploitation trends, patch timelines, and proof-of-concept development. This helps security teams prioritize vulnerability management based on actual threat actor exploitation rather than theoretical vulnerability scores.

Technical intelligence supports attribution by identifying code similarities, infrastructure overlaps, and operational pattern matches between campaigns. This helps organizations understand which threat groups target their industry and their tactics, techniques and procedures.

Intelligence That Knows What to Flag—and Why

- Inside the datasheet, learn how Fidelis Insight delivers:

- Real-time behavior rules
- Malware scoring (0–100)

- Global threat cache
- MITRE-mapped indicators

[Download the Datasheet Now]

Threat Intelligence Standards and Information Sharing Programs

STIX provides consistent language for describing cyber threat intelligence. TAXII defines secure protocols for intelligence distribution and consumption, enabling automated processing and secure sharing across organizations. These standards support strong threat intelligence programs.

Information Sharing and Analysis Centers facilitate sector-specific intelligence distribution. Healthcare organizations use H-ISAC to receive intelligence focused on medical facility threats and defensive requirements specific to healthcare cyber risks.

These frameworks create community-driven intelligence ecosystems reflecting actual attack patterns. Participants contribute threat observations and defensive insights while receiving actionable threat intelligence from peer institutions facing similar adversaries.

Industry sharing shows significant value through collective defense. Organizations actively participating in sharing communities report improved threat detection capabilities and more effective incident response compared to isolated operations.

Advanced Threat Intelligence Platforms and Integration Technologies

XDR platforms integrate multiple intelligence sources through automated processing pipelines handling large-scale threat data collection and correlation. Fidelis Elevate connects with major SOAR platforms like Splunk and Palo Alto Cortex XDR, SIEM systems including IBM QRadar and HPE ArcSight, and threat intelligence services like ReversingLabs and McAfee.

Integration extends across diverse security tools including packet brokers, endpoint detection, and secure service edge solutions. Comprehensive connectivity enhances existing security investments rather than requiring expensive replacements, supporting integrating threat intelligence across existing infrastructure.

Machine learning algorithms analyze intelligence patterns to identify emerging threats and predict attack vector evolution. Automated systems correlate new indicators with historical data, potentially identifying previously undetected compromises while updating security controls in real-time.

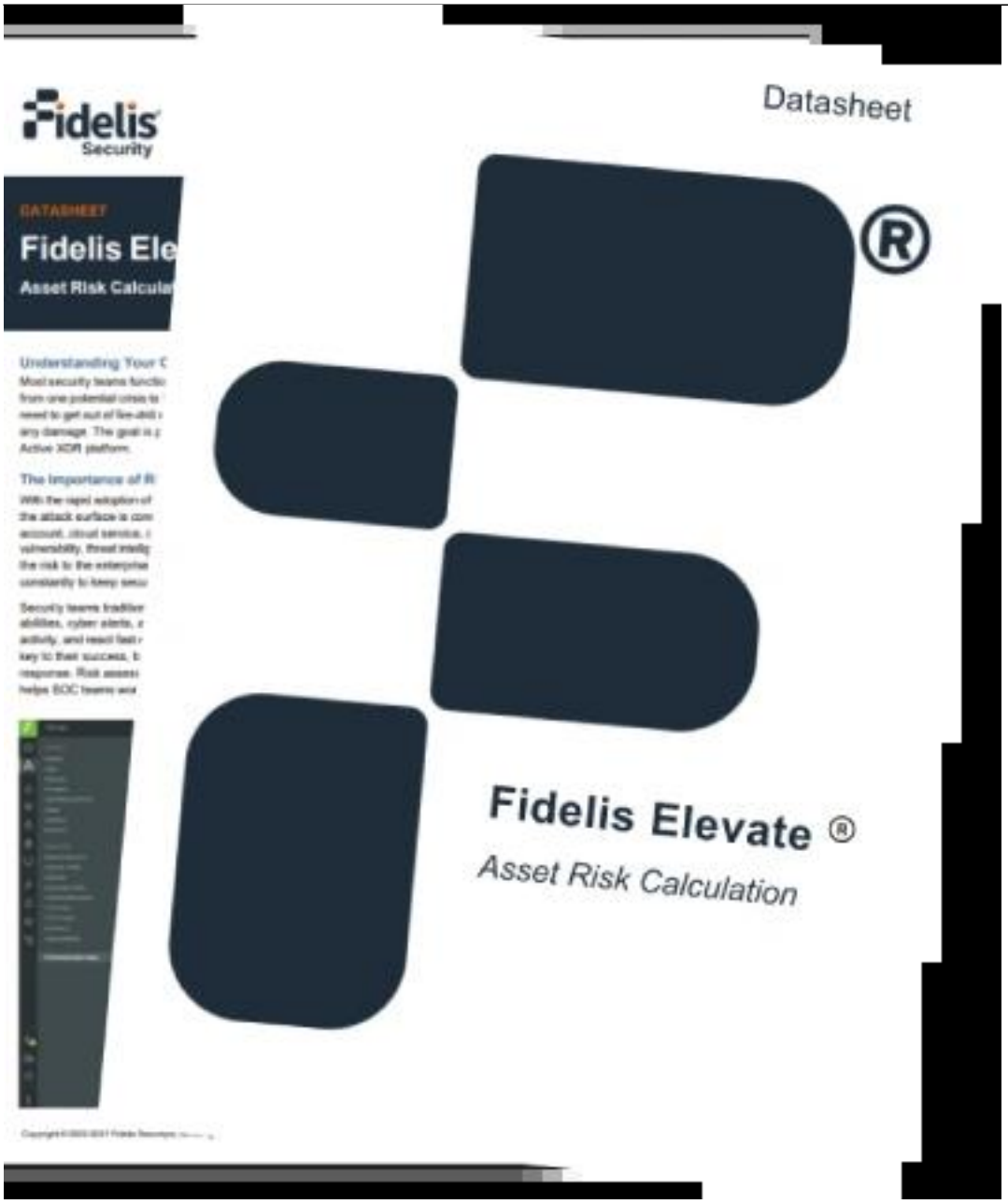
Deep Session Inspection technology analyzes network traffic across all ports and protocols, detecting threats in nested files, encrypted communications, and ephemeral containerized workloads that traditional security tools miss.

- Built for Detection. Powered by Deception.

In this datasheet, you’ll see how Fidelis Elevate enables:

- MITRE ATT&CK-based threat correlation
- Seamless SIEM/SOAR integrations
- Encrypted traffic inspection
- Automated threat response

Download the Datasheet



Types of Threat Intelligence Comparison: Strategic vs Tactical vs Operational

Intelligence Type Timeframe Primary Users Core Applications Update Frequency Strategic Threat Intelligence 6-18 months Executives, CISOs Budget planning, cyber risk management Quarterly Operational Threat Intelligence 1-6 months Security teams, threat hunters Campaign analysis, threat actor profiling Weekly/monthly Tactical Threat Intelligence Real-time – weeks SOC analysts, security tools Threat detection, incident response Real-time/daily Technical Threat Intelligence Variable Forensics, researchers Malware analysis, attribution Per-incident

Threat Intelligence Program Implementation and Best Practices

Cyber threat intelligence programs must align multiple intelligence categories with organizational capabilities, resources, and security objectives. Assessment processes identify intelligence gaps across strategic, operational, tactical, and technical domains while considering

available expertise and infrastructure.

59% of organizations report cybersecurity skill shortages affecting incident response capabilities. Threat intelligence programs must maximize automation for routine tasks while focusing human expertise on high-value analysis requiring specialized knowledge and experience.

Zero Trust implementations depend on continuous intelligence integration across security controls. The “never trust, always verify” principle requires constant validation of user behaviors, device activities, and application communications against current threat intelligence feeds and behavioral baselines.

Fidelis Elevate provides contextual visibility and integrated deception capabilities accelerating threat detection and response. The platform’s unified approach consolidates IT security operations to shrink attack surfaces while automating critical detection processes.

Effective cyber threat intelligence programs balance internal intelligence development through security operations with external threat intelligence services providing broader threat landscape awareness and industry-specific insights.

Advanced Threat Intelligence Processing and Analytics Capabilities

Machine learning supports threat intelligence lifecycle workflows by processing larger volumes of threat data and identifying subtle patterns traditional methods might miss. These technologies augment rather than replace human expertise in complex analysis requiring contextual understanding of cyber threat intelligence.

Automated correlation engines connect disparate security incidents through intelligence context and historical analysis. When new threat indicators emerge, systems automatically search historical repositories for related activities, potentially revealing previously undetected compromises or complex attack relationships.

Correlation extends to identifying relationships between different campaigns, threat actor groups, and attack methodologies. This analytical perspective helps organizations understand the complete threat landscape affecting their industry and prepare for coordinated cyber attacks.

Evolving Threat Landscape and Future Threat Intelligence Requirements

Cloud environments, IoT deployments, and distributed workforces create new threat intelligence requirements traditional approaches may not address. Digital transformation expands attack surfaces while introducing novel attack vectors requiring specialized intelligence coverage for emerging threats.

Healthcare exemplifies these evolving challenges. Medical IoT devices, cloud-based EHR systems, and telehealth platforms expand attack surfaces while maintaining critical availability requirements that cannot tolerate extended downtime from cyber attacks.

Proactive defense depends on comprehensive threat intelligence programs to guide security investments and operational priorities. As cyber threats increasingly target critical infrastructure, robust digital threat intelligence capabilities become essential for maintaining operational continuity during active attacks.

Business Integration and Organizational Value of Threat Intelligence

Threat intelligence programs integrate across organizational functions beyond traditional security operations. Risk management teams, compliance departments, and business continuity planners consume threat intelligence data for strategic planning and informed security decisions.

Fidelis Security’s approach consolidates IT security operations to shrink attack surfaces while automating critical threat detection and response processes. The platform accelerates analysis, forensics, and response capabilities, enabling organizations to maintain resilience through cyber attacks and improve overall security posture.

Organizations implementing integrated intelligence frameworks maintain better operational resilience despite evolving threat sophistication. The frameworks provide capabilities for faster threat detection, improved understanding of threat actor operations, and more effective response coordination during critical security incidents.

Modern cybersecurity environments demand intelligence-driven approaches addressing threats across multiple timeframes and organizational levels. Strategic threat intelligence guides executive resource allocation, operational intelligence tracks adversary campaigns, tactical intelligence enables real-time detection, and technical intelligence supports detailed forensics and countermeasure development.

Healthcare organizations cannot treat comprehensive threat intelligence programs as optional given current attack frequency and sophistication levels. Success requires integrating multiple types of threat intelligence into cohesive security operations leveraging automation while preserving human expertise for complex analytical tasks requiring specialized knowledge and contextual understanding of the threat landscape.