Optimize Threat Intelligence Lifecycle with Managed Security Service Providers (MSSPs)

Today, organizations deal with millions of threat indicators, making it difficult to gauge the value drawn from their threat intelligence framework. This has enhanced the need for automation-powered threat intelligence platforms that are managed by security service providers. Such platforms can help security teams to get actionable insights over their attack surface, push the right intelligence across their entire enterprise, and act faster against potential threats.

Companies are readily outsourcing threat intelligence to future-proof their security operations.

68% of organizations use threat feeds from general security vendors

How MSSPs Improve Threat Intelligence Lifecycle

Automate	Collaborate	Communicate
Automatic mapping of threat information to incidents.	Gathering intel from multiple sources, such as open-source feeds and intel providers.	Preparing detailed post-event analysis reports.
	How it Helps	
Expand the investigation scope, quickly identify relevant threat/attack patterns, and develop connections between diverse threat actors.	Better develop threat intel from raw data, broaden access to talented security analysts, and decisively act against critical vulnerabilities.	Efficiently summarize incidents for leadership teams to guide high-level business decisions and take actions to mitigate future damage.

SAMI-AEC's Approach to Threat Intelligence Management

Data collection

- Open source intel
- Verified external source feeds
- Internal incident alerts from organization

Processing

- Classification
- Data modeling
- Indicator enrichment & data normalization

Analysis

- Indicator & incident correlation
- Detailed visualization
- Automated alert prioritization

Sharing

- Threat intelligence platform (integrated with SIEM and EDR)

SAMI
ADVANCED
ELECTRONICS
شركة الإلكترونيات المتقدمة