Technology Brief

Indicators of Attack (IoA)

Context-sensitive clues unlock early attack detection and action.

Sophisticated attacks take time to unfold and involve much more than malware. Organizations must collect, assemble, interpret, and apply many fragments of information early in an attack chain to disrupt advanced and targeted attacks. More than raw data, organizational and situational context enrich other forms of intelligence to create "indicators of attack." These early warnings reveal suspicious events, letting systems and people contain and mitigate attack activities before they lead to system compromises and data loss. They also inform adaptive behaviors for sustainable advantage.

What happens when you see something suspicious outside your home? You gauge its risk and decide what to do. If it's a fire, you might call the fire department—but not if it's coming from the neighbor's grill. If it's someone looking through your neighbor's front window, and your neighbor is on vacation, you might take a picture and call the police—but not if you recognize their house sitter.

An IoA is a unique construction of unknown attributes, IoCs, and contextual information (including organizational intelligence and risk) into a dynamic, situational picture that guides response.

Suspicious or Benign? It Depends.

The key to this decision sequence is your definition of "something suspicious." Your neighborhood, line of business, and experience provide a baseline of "what is normal" as well as context to directly affect this definition. Context is often defined as "who, what, when, and where." It's the analyst's job to derive "why and how." In sizing up the context, we make a decision, one that can protect our neighborhood or our business.

In attack scenarios, the time factor is one of the most pivotal. It involves not just catching a snapshot of a point in time (12:36.12 a.m.), but capturing that event within an attack timeline by noting repetition (20 times) or related events (from different IP addresses) across a span of time (within 24 hours).

IoA versus IoC

These contextual attributes of a situation add up to "indicators of attack (IoAs)." Unlike "indicators of compromise (IoCs)," which are individual known bad, static events (IoC test: Is there a regulation against loss of that structured data? Is file blacklisting a relevant control?), IoAs only become bad based on what they mean to you and the situation.

intel Security

Earliest Possible Attack Detection

Because this situational picture can be created as early as the initial phase of an attack—reconnaissance—defenders gain an active role in blocking the attack's success. With visibility and contextualization throughout the attack chain, defenders have many more opportunities to fight off an attack before it succeeds. This is another contrast with IoCs, which primarily support after-the-fact forensic investigation, not the in-the-moment incident intervention made possible by an IoA.

A Bias for Action

The detailed nature of the situational picture increases the sensitivity and precision of attack containment and mitigation. It brings relevant information directly to the people and processes that need it, when they need it.

- Enhanced, dynamic threat and risk scoring can pinpoint and elevate events for immediate evaluation by security analysts.
- Actionable details permit targeted processes to automatically and selectively block, disrupt, monitor, or record activities.
- Fine-grained event attributes can be used to find other instances of an event.
- Event details can allow heuristics to predict attack behaviors, educate defenses, and suggest policy and control changes to prevent future repetitions.
- Context helps investigators reconstruct a complete forensic chain of events and look back in time to unearth other and similar attack evidence.

These proactive organizational behaviors demonstrate maturity in incident response, a maturity increasingly sought by enterprise leaders worried about data breaches and cyberattack costs.

An Intelligence-Sharing Architecture

To implement systems that support IoAs, each organization needs to adjust its mindset and controls to be more proactive and timely about sharing and acting on contextual data. This process turns raw data into actionable intelligence and then to intelligent action.

Figure 1. Collection and sharing of context and other forms of intelligence enable adaptive threat management.

Collection

The first hurdle is usually collection. Many sensors and products can collect raw data, but most "use it and lose it." The architecture needs to ensure the important (relevant) data is collected and shared, not just observed and discarded. This shared data supports immediate containment of the attack and can also factor into improvements in policies and defenses, essentially helping the infrastructure learn as it protects.

Next, the individual data points must be aggregated to construct an indicator of attack. Simple, intermittent data archival as implemented by first-generation security and information event management (SIEM) is not enough. Basic event data must be enriched with contextual data (such as time, prevalence, location) and the human factor of experience, risk values, and instinct. This contextualization can happen in different ways, in different segments of the infrastructure, but it needs to happen at a speed that supports immediate action.

Contextualization

Many products are designed for single functions, not to be part of a centrally managed, intelligence-sharing system. This advance requires a trusted way to exchange data in real time, such as the messaging bus used in the McAfee® data exchange layer. By defining clear ways to share precise types of information, the McAfee data exchange layer enables and encourages appropriate sharing.

Centralization

Centralized services help with both collection and contextualization. For example, endpoint sensor events can be baselined, aggregated, and contextualized using local threat intelligence and organizational preferences and risk scores, a model available with the McAfee Threat Intelligence Exchange. This process can reveal first contact and prevalence.

In addition, an advanced security intelligence platform can build on real-time SIEM technologies to normalize and correlate endpoint discoveries with network event data and other information—user data, application policies, threat intelligence, risk posture—and surface concrete IoAs. Correlation is important in this process as it aligns data into IoAs and assembles them into a sequence that reveals attack patterns and intent.

Aggregating a full picture from fragments of information, contextualized intelligence can rapidly become a "Big Data" problem, so an advanced analytics architecture is recommended. This system is available with McAfee Enterprise Security Manager.

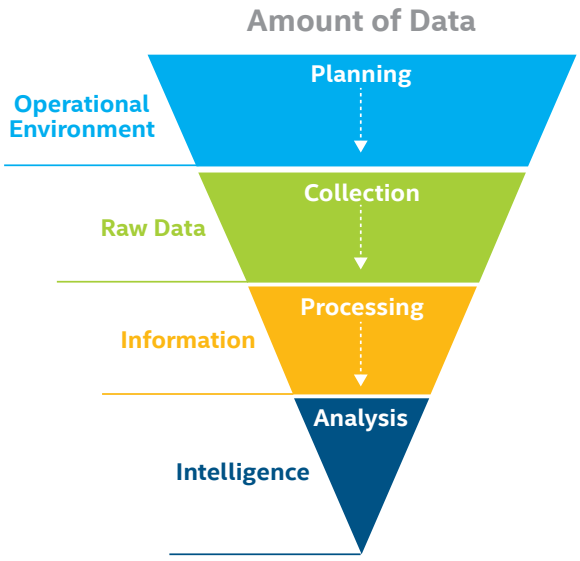

Figure 2. Conversion of massive amounts of data into actionable intelligence requires filtering, contextualization, and high-speed analytics.

Action and adaptation

Once the IoA is created, people and processes can act while the rich intelligence is distributed. Directly, alerts, and thresholds can guide enforcement actions such as quarantine. In near real time, new findings can factor into policy adjustments, authentication requirements, and human response workflows. Within hours and days, findings can influence risk scores, organizational policies, and end-user education. Over longer timelines—weeks and months—organizations can trend and surface anomalies, predict future attacks, and adjust sensitivities.

Getting Started

Support for IoAs will allow your organization to act earlier and more definitively to disrupt advanced and targeted threats. By sending rich IoA insights to cross-vector detection, containment, and remediation systems, security analysts get a sustainable advantage against evolving cyberthreats. Get started today with a visit to **mcafee.com/incidentresponse**.

McAfee. Part of Intel Security.
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com