Automated Threat Intelligence Platform (ATIP)

ATIP equips Raytheon Foreground Security’s team of highly skilled cyber experts with the data and tools needed to identify, assess, manage, and respond quickly to security threats.

**Benefits**
- Research and link analysis
- Metrics, trending and tracking
- MD5 file, IRL, Internet protocol (IP), domain and ASN indicators
- Virtual desktop interfaces
- Vendor agnostic

Raytheon Foreground Security recognizes vulnerability in the traditional approach of applying threat intelligence to enterprise security. This security gap exists because corporations typically do not have the manpower to process and contextualize intelligence feeds across their business units and information assets. Foreground offers a proven approach that optimizes threat intelligence for our client’s specific industry. We ingest hundreds of distinct threat feeds, normalize the feeds, and provide context, including: current status of threat, applicability to client industry, trustworthiness, impact if exposed, and related indicators of compromise (e.g., file hashes, URLs, IP addresses, domains, email headers). Our Automated Threat Intelligence Platform (ATIP) uses a foundation of machine learning to intelligently interrogate client security infrastructure to identify known and unknown threats.

**Threat Intelligence Sources**
ATIP ingests threat intelligence from a balanced set of threat sources. This variety ensures that our threat detection is not dependent on which source happens to have the most relevant intelligence at any moment. By working with as many disparate sources as possible, Foreground ensures that ATIP provides maximum value at all times. We categorize our threat sources, as follows:
- Public (open source)
- Private (commercial)
- Invitation-only (community)
- Customer-sourced
- Foreground-sourced (research, forensics, incident response, and malware analysis)

Once in hand, threat intelligence is standardized and de-duplicated for insertion into our Analytics and Threat Modeling Engine. Records are then tagged to support ATIP’s client/server subscription model for the distribution of intelligence to field appliances based upon factors including: intelligence source, industries impacted, geo-location, and behavior profile.

**Application**
ATIP leverages the known (aggregated threat intelligence), as well as the unknown (malicious patterns of behavior), to interrogate client security platforms using the platform’s vendor-supported application programming interface (API). ATIP is compatible with a growing list of security technologies in the following product classes:
- Security information and event management (SIEM)
- Network security monitoring (NSM)
- End-point Detection and Response (EDR)
ATIP’s hunting with the client’s SIEM platform ensures inclusion of system, application, and layered security control logs and events.

**Analyst/Client Portal**

When events of interest are identified, ATIP collects the relevant metadata from the security platform, applies a risk score, and presents the event in a secure web portal on the ATIP server. The risk score is an aggregate score derived from confidence (i.e., trustworthiness of the matched indicators, source, and metadata) and severity (i.e., expected impact of a confirmed threat) values.

Virtual Security Operations Center (V-SOC) analyst teams investigate the events of interest and log their findings and recommendations in ATIP’s embedded ticketing system. Client analysts and incident responders have full access to ATIP’s investigation and ticketing workflows. In support of client management teams, ATIP provides multiple dashboards to provide reporting on platform results and analyst reports.

**Machine Learning and Analytics**

The core of ATIP is a machine learning engine that continuously learns what is “bad” in each client’s enterprise based upon the event data processed by the system, as well as the way in which analysts handle each event. Analyst feedback is required to close out investigations, which ensures the system has the opportunity to understand and learn from the full incident life cycle. Based upon analyst feedback from the incidents and investigations, the confidence and severity ratings of the intelligence sources and threat indicators are continuously adjusted using mathematical algorithms.