IBM Automated Cyber Threat Triage and Response

Summary.

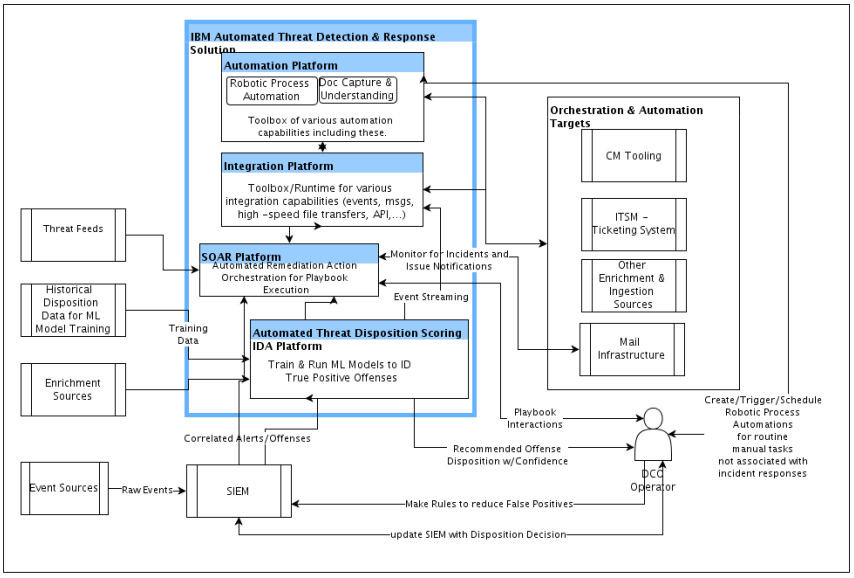
The IBM Automated Threat Detection and Response solution **both automatically detects true cyber threats AND responds appropriately and automatically**. Our solution includes not only a market-leading COTS security orchestration capability (SOAR) for response playbook development and execution but even more critically, it also includes a **proven AI-powered threat detection and scoring capability** that feeds the SOAR in real-time with **actionable, confidence-ranked triaging** recommendations. Internally, our IBM Managed Security Service (MSS) uses this patented Automated Threat Disposition Scoring (ATDS) capability with hundreds of commercial customers to **automatically perform 70-75% of all Level One analyst triaging**. Using this same solution, the USAF too can measurably accelerate detection, response, and mitigation of cyber-attacks and reduce costs by virtually eliminating time and effort spent processing false positive cyber events.

How it Works.

Using your existing SIEM-provided signals, our AI/ML-based ATDS technique automatically characterizes attacks and provides actionable, confidence-ranked disposition recommendations that IBM's or any third-party SOAR capability uses to automatically or semi-automatically trigger targeted response playbooks. IBM's end-to-end solution includes comprehensive integration and automation capabilities needed by any SOAR platform to interact with external systems for automated incident enrichment, notification, response, and remediation. In addition to a SOAR, USAF cyber operators and analysts will use a rich set of self-service automation capabilities provided with the automation platform, for example, Robotic Process Automation (RPA), to quickly and easily automate remediation and response actions as well as any day-to-day manual, toilsome, tedious, time-consuming tasks that detract from their primary duties.

IBM Automated Cyber Threat Triaging and Response Solution Overview

Automated Cyber-Attack Offense Detection, Disposition, and Response Orchestration



To summarize the solution flow, IBM ATDS ingests correlated Alerts and Events from any SIEM, scores their threat potential with 95% accuracy using ML models trained using your historical operator disposition data, and assigns a quantified confidence rating that is either 1) True positive requiring escalation 2) False positive that can

be automatically closed or 3) Likely positive that needs further investigation before escalation. The ML models continue to learn and improve with every disposition action, further increasing the percentage of alerts that can be automatically triaged with high accuracy.

These automated actionable recommendations are then provided to cyber operators, the orchestration (SOAR) platform, and other subscribers via the integration platform for adjudication and automatic or semi-automatic response and remediation.

Why IBM. With IBM's solution, the USAF can measurably accelerate detection, response, and mitigation of cyber-attacks and reduce operational costs by virtually eliminating time and effort spent manually triaging and responding to SIEM-generated incidents/offenses. The compelling advantages of IBM's solution stems from its unique combination of patented commercially proven, AI-powered, automated threat classification (ATDS); market-leading SOAR platform; and open Red Hat OpenShift Kubernetes platform hosting containerized, cloud-native market-leading enterprise-class IBM, third-party, and open-source integration and automation middleware.

The IBM Automated Cyber Threat Triage and Response solution:

- **Works.** Internally, IBM Managed Security Services use the same patented ATDFS technique with commercial customers to automate 70-75% of L1 triaging; reduce overall Triage cycle times 40%; lower L1 time-to-respond 49%; cut L1 time-to-investigate 9%; and slash L1 cycle time for high value Threat Escalation 74%.
- **Scales**. Our containerized solution runs on the Red Hat OpenShift (RHOCP) Kubernetes platform which is resilient and scalable by design, deployable to virtually any on-prem or cloud-environment, and dynamically and automatically scales as demand fluctuates.
- **Comes Pre-integrated**. Not just a jumble of pieces and parts, each solution component is a pre-integrated collection of market-leading, best-of-breed enterprise-class IBM, Red Hat and third-party commercially and commercially-supported open source middleware tied together beind a unified, role-based user experience.
- **Is Low risk**. RHOCP is running on the C2S cloud, AWS GovCloud, and USAF CloudOne platform and is part of the DoD DevSecOps Initiative Reference Architecture. A cloud-hosted version of the ATDS solution has been in production use by IBM's commercial Managed Security Services with hundreds of their commercial customers for over a year. It works with any SIEM.
- **Is future-proof**. The AI/ML models continually learn and can incorporate new data.
- **2020 AFWERX Showcase Selectee and available on AFWERX Commercial Solutions Opening (CSO) contract vehicle**. The CSO is for any AFWERX Challenge team that was selected to take part in a showcase. It is a method to expedite the contracting process.