The Respond Analyst™

Power Your Security Team with Automated Monitoring and Triage

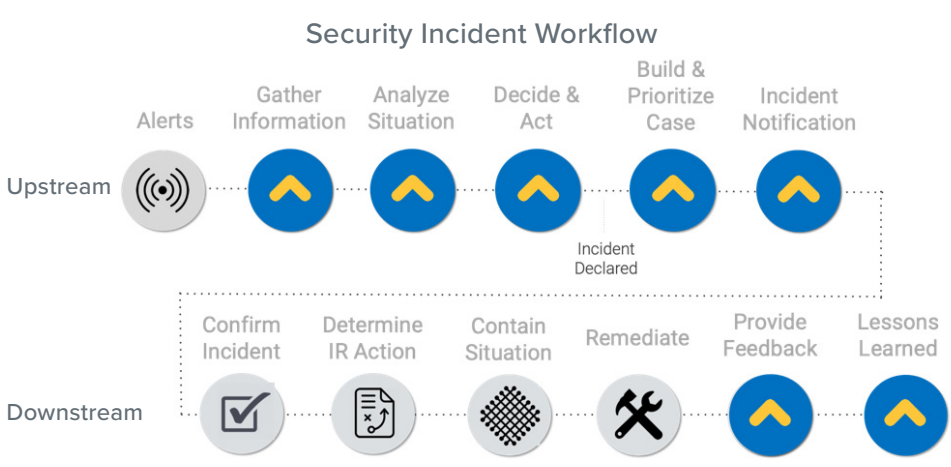
The growth of security related data coupled with the shortage of skilled security personnel leaves companies at risk. Security teams of all sizes are resource constrained, filtering alerts to match analysis capacity of their staff. In doing so, clues to potential threats stay hidden and attackers are able to achieve longer dwell times, increasing both the likelihood and impact of a security incident. These challenges are costing companies on average $3.86M per breach,[†] and 21,000 hours per year in wasted time chasing false positives.[††]

Respond Software addresses these issues with the Respond Analyst, the first decision automation system for cybersecurity. The Respond Analyst introduces a new class of security automation software called Robotic Decision Automation (RDA). RDA provides automated reasoning and decision-making skills to tackle high volumes of data, triaging security events at half the cost of a human analyst. Because the Respond Analyst is cloud based, not a platform, it provides near instantaneous ROI and is ready to go to work out-of-the-box with the speed, scale and consistency of modern software.

Performing the Security Operations like an Expert Analyst

Using patented techniques and probabilistic mathematics, the Respond Analyst monitors security event streams and automates expert human analysis of security alerts, accurately culling false positives and escalating actionable, prioritized and well-articulated incidents. The Respond Analyst conducts the following security operations tasks as a member of your security team:

- Monitors and evaluates every alert with consistency in real time
- Evaluates contextual information to triangulate assets, users and threats
- Scopes incidents together based on common attacker tactics, techniques and procedures (TTPs), then decides on the appropriate action to take based on context
- Prioritizes incidents based on asset criticality, attack stage progression and likelihood of incident



The Respond Analyst simplifies upstream and downstream by prioritizing security operation activities using business context and decision automation.

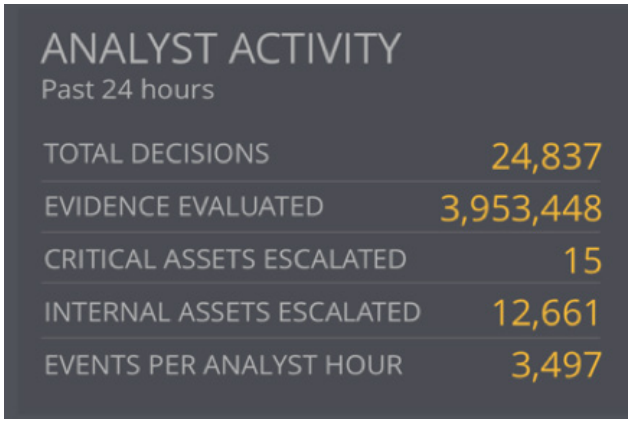
- Provides detailed cases in intuitive incident summaries with all available evidence of malicious activity
- Notifies incident response team via email/PagerDuty, re-notifies if priority is upgraded
- Learns from customer feedback and integrates with SIEM, Big Data, SOAR, ticketing and case management platforms

[†]Sydny Shepard, The Average Cost of a Data Breach, Security Today, July 2018 [††]The Ponemon Institute, The Cost of Malware Containment, January 2015

The Respond Analyst

Add a Virtual Analyst to your team, Automated and Continuous 24x7 Monitoring

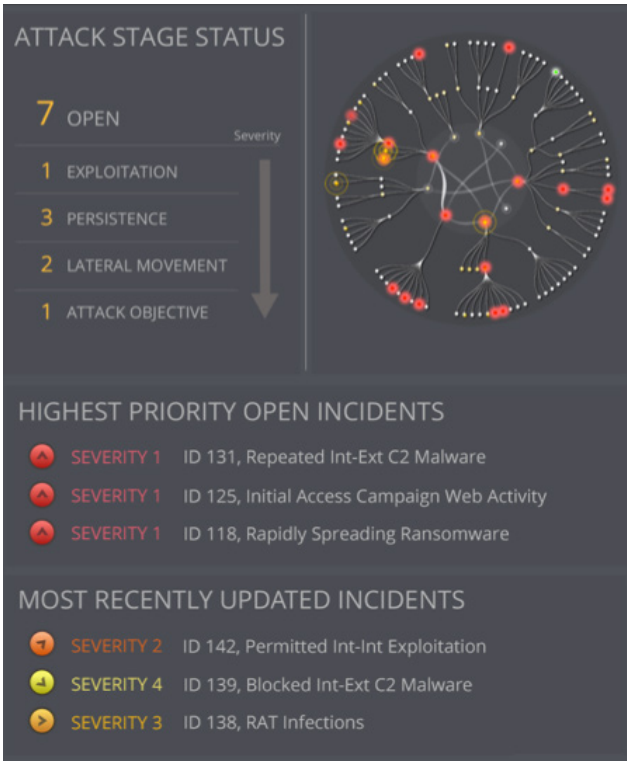
The Respond Analyst runs 24x7x365 and scales to the largest enterprises. It integrates with existing security infrastructure including SIEM and SOAR platforms, and removes the need to filter, tune-down or ignore security events to match the monitoring capacity of human analysis. Because the Respond Analyst automates decision-making, security analysts are enabled to go threat hunting instead of spending time chasing false positives.



Evaluates all alerts and performs extensive checks on each.

Human Judgement at the Speed, Scale and Consistency of Software

The Respond Analyst processes millions of alerts in real-time, eliminating human bias or fatigue. Because it uses probability-based reasoning, the Respond Analyst significantly reduces the number of false positives that need to be investigated.



As new related information is streamed and evaluated, the Respond Analyst dynamically rescopes, reinterprets the attack stage, and reprioritizes the incident.

The Value of the Respond Analyst

The Respond Analyst combines the best of human expert judgement with the scalability and consistency of software giving organizations a new and decisive advantage in their battle against cybercrime. It's a quick-to-implement solution that adds the virtual equivalent of more than 14 full-time best-of-breed analysts to security teams, dramatically improving monitoring and triage capabilities at a fraction of the cost.

Complete List of Product Integrations for the Respond Analyst
(https://respond-software.com/respond-analyst/integrations)