# The First Responder Service powered by the Respond Analyst

## Power Your Security Team with Automated Monitoring and Triage

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

Due to these issues, some organizations are outsourcing their security operations to Managed Security Service Providers (MSSP) or Managed Detection and Response (MDR) services. However, these services rely on humans, so organizations are seeing the same problems – too many false positives to manage, not enough visibility or coverage and inexperienced security analysts in charge of escalations that create more work for internal security teams, opening the business up to more risk.

Additionally, MDRs utilize their own security stack, limiting visibility to a single telemetry, while locking customers into their infrastructure. In essence, the problems organizations are trying to solve are simply being shifted to expensive services that provide the same or lesser results.

For organizations that are interested in a better way to approach these traditional security problems, Respond Software offers the First Responder Service. The First Responder Service takes a "software first" approach that employs modern math to reason through billions of events to find the malicious and actionable incidents that are creating risk inside your company.

The First Responder Service leverages the Respond Analyst™ to detect, investigate and escalate security incidents across the technology and data you already have, freeing your team to focus on the tasks that are important to your business. The Respond Analyst delivers the power of thousands of expert analysts to your team when you need it, 24 hours a day – all through software.

## Performing the Security Operations Tasks of an Expert Analyst

Using patented, probabilistic mathematics, the Respond Analyst automates the human security analysis process converting raw security alerts directly into scoped, prioritized and well-articulated incidents, ready for investigation and remediation. 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 based on common attacker tactics, techniques and procedures (TTPs)
- Prioritizes incidents based on asset criticality, attack stage progression and likelihood of incident
- Provides detailed cases in an intuitive incident summary with all available evidence of malicious activity
- Learns from customer feedback and integrates with SIEM, Big Data, SOAR, ticketing and case management platforms


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

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

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

The Respond Analyst runs 24x7x365 and scales to the largest enterprises. The Respond Analyst specializes in monitoring high volume data sources, such as Intrusion Prevention Solutions, Web Proxies, Endpoint Protection, and Endpoint Detection removing the need to filter, tune-down or ignore security events to match the monitoring capacity of human analysts. The more data the Respond Analyst collects from your environment, the fewer incidents are typically escalated. The Respond Analyst also integrates with existing security infrastructure including SIEM and SOAR platforms, to help remediate security incidents faster reducing risk to your business.

The Respond Analyst focuses on the grey areas of security alerts using probability theory to determine if they are malicious and actionable, while cutting through the noise of false positives. More visibility allows the Respond Analyst to correlate across telemetry sources, creating even more value through highly enriched security incidents. Because the Respond Analyst automates decision-making, security analysts are enabled to go threat hunting instead of spending time chasing false positives.

## Human Judgement at the Speed-Scale and Consistency of Software

Traditional MDRs, MSSPs, and SIEM providers use rules and workflow automation, resulting in black or white escalations. Security incidents are not that simple. They require context, correlation, and a thorough understanding of your environment. The Respond Analyst uses judgement, just like an expert security professional, to identify and investigate security incidents and determine the probability that something is creating risk.


*Evaluates all alerts and performs extensive checks on each.*

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.

## The First Responder Service

For organizations that prefer an additional human touch, Respond offers a team of security experts that can assist you by answering questions about your security incidents and provide guidance on remediation steps. The First Responder Service is a new way of doing Managed Detection and Response at the fraction of the cost of traditional MDR services.

The Respond Analyst product, paired with on-demand access to our expert First Responder team, provides consistent monitoring coverage of security alerts in your environment with expert advice when you need it, that can free your team up to focus on other high value security projects that reduce business risk. Key features include:

- **Heterogenous Support:** Support for the best in class security technologies and solutions, freeing you from the proprietary technology stacks that many MSSP/MDR providers require you to deploy. We unlock considerable value from your security technology investment, enabling you to turn the volume up on events and data collection, allowing the Respond Analyst to see more without drowning your team in alerts.

# The First Responder Service

- **Automated incident escalation:** Within five minutes of incident creation, customers have 24x7x365 access to unrivaled situational awareness and a point of escalation when needed.
- **Live consultation:** Expert First Responders are available for customers to engage for incident assistance with intrusion/attack analysis, recommendations for remediation and more.
- **Quarterly briefings:** The First Responder Service includes regular updates to help customers understand key metrics and performance indicators specific to their environment and team.
- **Enhanced onboarding:** First Responders will interact with the customer's team for a white-glove onboarding experience during the first 30 days.


*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)