respond

The Respond Analyst™ | an XDR Engine

Architecture White Paper

Fall 2020

Respond Software Inc. | 785 Castro Street, Suite C | Mountain View, CA 94041 | 650.282.2270 | info@respond-software.com

OVERVIEW

The Respond Analyst^{TM}, an XDR Engine, features decision automation software pre-built with reasoning and decision-making skills needed to tackle the complexity and high volume of data facing security teams today. The Respond Analyst automates the analysis and triage of security data, at machine speed, with depth and consistency. Its proprietary intelligent decision engine provides built-in reasoning and judgment to make better decisions, faster.

The Respond Analyst evaluates the event data stream in real-time, from an organization's existing security detection sensors and learns about its security infrastructure and network context. The Respond Analyst is able to analyze all events and alerts, regardless of volume; to build evidence and context around malicious activity. The Respond Analyst processes every event, not just alerts labeled "important" or "critical," and performs extensive checks against an internal repository of context to appropriately escalate incidents.

The Respond Analyst uses probability-based reasoning and provides 24x7 continuous monitoring removing the need to filter, tune-down or ignore security alerts resulting in a significantly reduced number of false positives. The Respond Analyst eliminates human bias or fatigue of monitoring security alerts, and maximizes the effectiveness of security teams by enabling analysts to go threat hunting.

Designed to easily integrate into any security infrastructure, the Respond Analyst brings additional value to existing investments by providing the capacity to thoroughly analyze all security events that are detected – without any learning mode or security rules to maintain.

Leveraging the latest advancement in artificial intelligence, machine learning, modern streaming architectures, and Respond Software's unique Integrated Reasoning, the Respond Analyst acts autonomously – without a heavy system management burden, security engineering, or long learning cycles.

TABLE OF CONTENTS

FUNCTIONAL APPLICATION

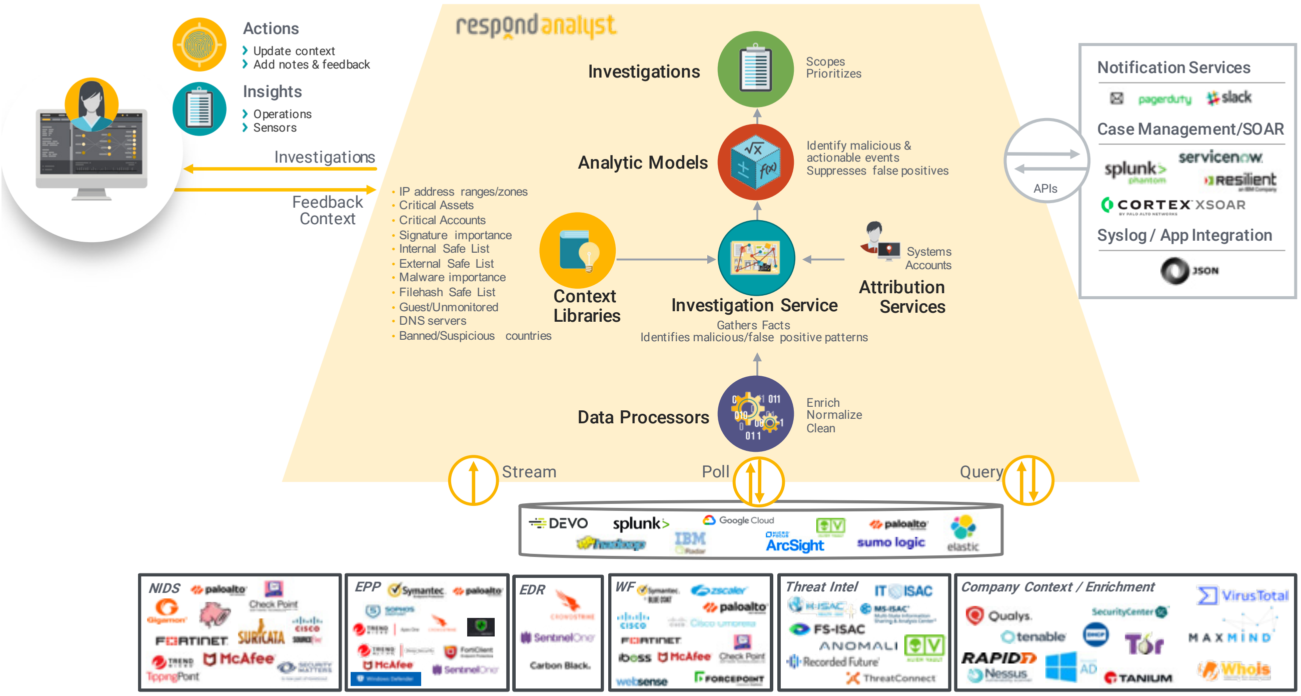
The Respond Analyst was built to support the exponential growth in security data and the variety of sensors and infrastructures deployed in today's security environments.

The Respond Analyst is a cloud based application that includes:

- Data Processors that enrich, normalize and clean data across multiple types of security sensors, threat intelligence and company context.
- Integrated Reasoning that analyzes all network events, equates malicious attacks and determines which incidents need investigation.

HOW IT WORKS

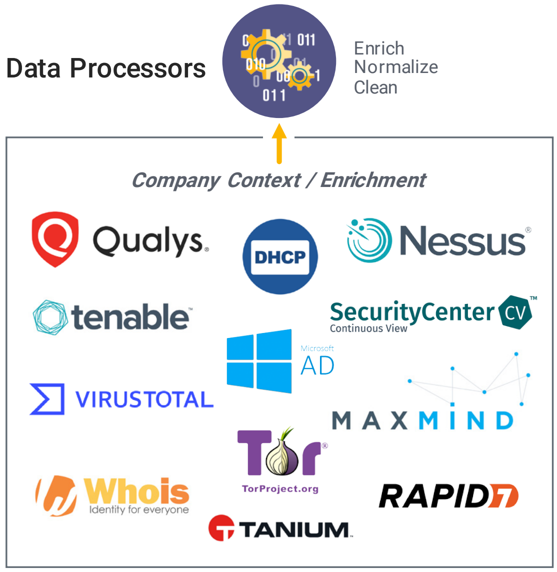
Functional Architecture



The Respond Analyst leverages existing security event collection infrastructure, extracting the data the Respond Analyst needs, executing deeper analysis with Integrated Reasoning.

THE RESPOND ANALYST

The Respond Analyst evaluates the event data stream from exisiting security sensors and learns about company context and the IT network environment in real-time. The Respond Analyst analyzes all events and alerts, regardless of volume, building evidence and context around malicious activity.



The Respond Analyst comes pre-structured with expert judgement, but learns and adapts while maintaining tribal knowledge. The Respond Analyst runs 24x7x365 performing without fatigue, loss of attention or staff attrition. This mix of expert judgment and self-adaption enables the Respond Analyst to immediately produce high-fidelity results and improve quickly as it works with a security response team.

THE RESPOND ANALYST – EVENTS & CONTEXT

During onboarding, the administrator of the Respond Analyst is asked to provide important context about the IT environment through the management dashboard including:

- The company's publicly owned IP space
- Critical assets and accounts
- Security and network infrastructure (vulnerability scanners and load balancers)
- Network IDS/IPS signatures (high or low importance)
- Dynamic Host Configuration Protocol (DHCP) leases
- Asset vulnerability information

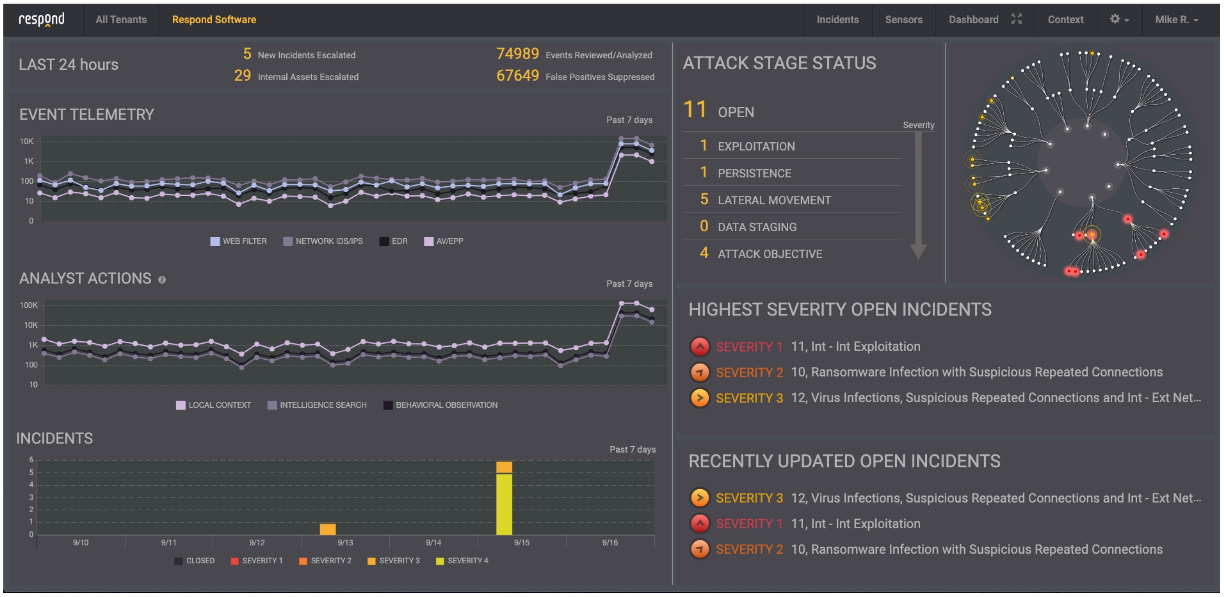
Not all context is required for the Respond Analyst to be operational; however, each additional contextual element, incrementally increases the certainty about whether the detected activity is malicious and actionable or benign.

During the initial setup, the administrator configures event sources that the Respond Analyst will utilize. A goal of Respond Software is to help organizations leverage their existing event-processing infrastructures; therefore, the Respond Analyst supports event sources including ELK, Hadoop, Splunk, and SIEM forwarders and connectors from products such as MicroFocus ArcSight, IBM QRadar, Sumo Logic, Amazon S3 Buckets, Splunk Phantom and Palo Alto Cortex. The Respond Analyst will also accept events streamed directly from the management consoles of Network IPS/IDS, Endpoint Protection Platforms, Web Proxy & Filtering solutions and Endpoint Detection and Response systems. Unlisted event sources are also possible since the the Respond Analyst listens for events on TCP-6060, UDP- 514, TLS-6514, and HTTP-6080.

THE RESPOND ANALYST: EVENT PROCESSING

As the Respond Analyst receives events, it checks IP addresses and hostnames against sensitive contextual references such as the critical asset list, the critical account list, file name checks, geolocation information, and vulnerability data.

The Respond Analyst dashboard exposes the number events reviewed, false positives that were suppressed, internal assets escalated and new incidents escalated. The Respond Analyst dashboard includes event telemetry data, analyst actions, incidents in the past seven days and other information regarding attack stage status and the severity of incidents as displayed below.



LAST 24 hours
5 New Incidents Escalated
29 Internal Assets Escalated
74989 Events Reviewed/Analyzed
67649 False Positives Suppressed

ATTACK STAGE STATUS

11	OPEN	Severity
1	EXPLOITATION	
1	PERSISTENCE	
5	LATERAL MOVEMENT	
0	DATA STAGING	
4	ATTACK OBJECTIVE	

HIGHEST SEVERITY OPEN INCIDENTS

SEVERITY 1 11, Int - Int Exploitation
SEVERITY 2 10, Ransomware Infection with Suspicious Repeated Connections
SEVERITY 3 12, Virus Infections, Suspicious Repeated Connections and Int - Ext Net...

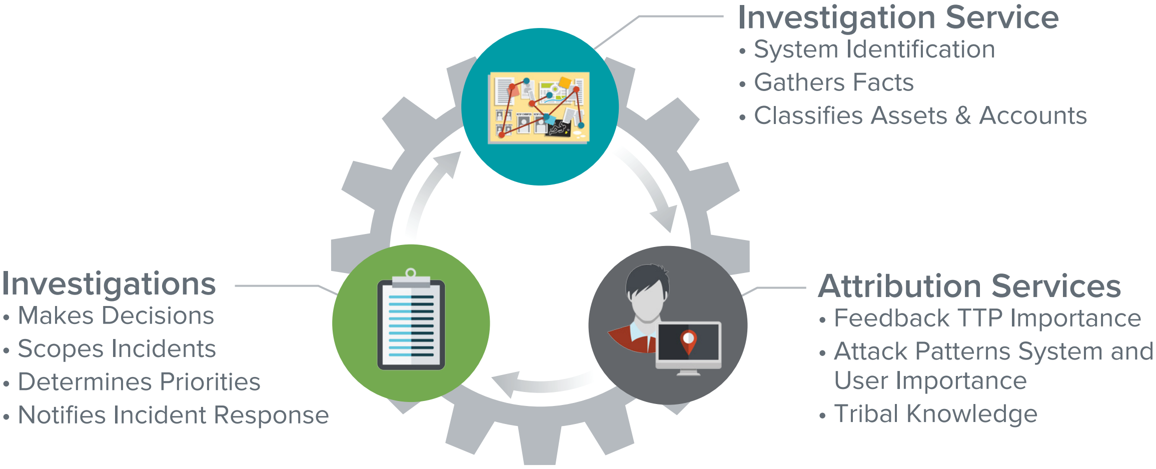
RECENTLY UPDATED OPEN INCIDENTS

SEVERITY 3 12, Virus Infections, Suspicious Repeated Connections and Int - Ext Net...
SEVERITY 1 11, Int - Int Exploitation
SEVERITY 2 10, Ransomware Infection with Suspicious Repeated Connections

INTEGRATED REASONING

Integrated Reasoning has three features that codify the foundational knowledge, complex decision-making process and ongoing learning of a highly skilled security analyst.

Integrated Reasoning



Investigation Service

- System Identification
- Gathers Facts
- Classifies Assets & Accounts

Attribution Services

- Feedback TTP Importance
- Attack Patterns System and User Importance
- Tribal Knowledge

Investigations

- Makes Decisions
- Scopes Incidents
- Determines Priorities
- Notifies Incident Response

What is Integrated Reasoning?

At the core of the Respond Analyst is its Integrated Reasoning capability, developed by Respond's security experts and data scientists to analyze all network events, equate malicious attacks and determine which incidents should be investigated. Integrated Reasoning utilizes the most critical variables a security analyst considers relevant and decides if an event is malicious and actionable.

Integrated Reasoning is a patent-pending, multi-layered technology developed at the unique intersection of applied mathematics, security expertise, knowledge engineering, and proprietary algorithms. With machine-level scalability, Integrated Reasoning utilizes all three of these elements to monitor, analyze, and determine which events are malicious across the organization's entire infrastructure. Through continuous learning and adaptation to an organization's environment, Integrated Reasoning becomes more efficient at prioritizing events and making actionable decisions.
It is purpose-built to emulate the decision-making process of an experienced security analyst. Integrated Reasoning is foundational to the Respond Analyst decision models, delivering efficient and effective security.

For more information on Integrated Reasoning, please download the Integrated Reasoning White Paper that describes how the Respond Analyst works.

INTEGRATED REASONING

Investigation Service

The Respond Analyst Investigation Service leverages events from DHCP and endpoint protection to constantly keep an up to date record of an IP addresses associated hostname. An accurate mapping between hostname and an IP address ensures that subsequent investigations appropriately map context and behaviors to the correct system.

The Investigation Service evaluates if the systems, accounts, external IPs and domains, signatures, hashes (or other event attributes) in the event result in an affirmative reference check that is maintained within the Knowledge Base.

Additionally, system attributes (e.g. open ports, operating systems) are used to classify the type and function of the internal system involved in the event.

System types inferred through the asset classification service include identifying if the internal system is a workstation or a server, or if the server is a Domain Controller, DNS server, Web server, Database server, or File server, for example. Account attributes, such as administrative access, are identified through integration with Active Directory. This feature gathers the information required for the Respond Analyst to answer a series of analytical questions for every event.

Attribution Services

Events from the the Respond Analyst are further annotated with checks made against the Knowledge Base, a repository of both local "tribal knowledge" about a customer's unique environment, and global threat intelligence.

Within the Network Intrusion Analytic Model, the Respond Analyst maintains a history of communications between sources and destinations (both internal and external to the company) in order to identify patterns and anomalies which indicate either suspicious or benign behavior.

Within the Malware Event Analytic Model, the Respond Analyst keeps a record of attributes shared across systems within your organization and leverages this knowledge base to look for patterns indicating malware may be spreading or isolated within the environment.

Within the Web Filter Analytic Module, the Respond Analyst maintains a history of web requests per system to identify if traffic patterns are suspicious and possibly an indication of command and control.

Within the Endpoint Detection and Response Analytic Module, the Respond Analyst classifies each process and evaluates the process's relationship with the parent and child processes for suspicious behaviors.

Additionally, the Respond Analyst keeps track of repeat offending systems and accounts, corroborating suspicion garnered from the Network Intrusion Model, Malware Event Analysis Model, Endpoint Detection and Response Model and the Web Filter Analysis Model.

Global threat intelligence sourced and utilized by Respond Software includes known bad indicators such as external IP addresses and file hashes, IP geolocation information, IP anonymization services such as public VPNs or TOR Nodes lists. Integration with STIX/TAXII enables customers to leverage additional threat intelligence sources.

INTEGRATED REASONING

Investigations

The Investigations component of Integrated Reasoning uses decision automation to structure the reasoning and judgement of expert security analysts and makes decisions to:

- Escalate the case, with the recommendation that incident response should perform containment and remediation actions
- Ignore the case, as it is not a threat and needs no further action at this time

Each escalated case is triaged to a priority based on the likelihood of the activity being malicious and actionable, current most progressed attack stage, number of internal systems involved, and asset importance of the involved systems.

If the escalated case is related to an ongoing and open incident (same system(s), attack techniques, etc.), the case is added to the existing incident and the incident is scoped and prioritized using the new information.

ANALYTIC MODELS

The Respond Analyst Analytic Models are currently available for data from Network Intrusion sensors, Endpoint Protection Platforms, Endpoint Detection and Response and Web & URL filtering devices. Analytic Models are streaming technologies – with the ability to evaluate, scope and prioritize events in near real-time.

Analytic Models do not filter or ignore any events using all collected data to create a clear picture of situation incidents when and if they occur.

Each Analytic Model is delivered pre-built with Knowledge Base, Investigation Service and Model content.

The Network Intrusion Analytic Model | analyzes Network Intrusion Detection System (NIDS) data, providing automated decisions on incidents that are malicious and actionable and visibility across a broad range of attacks, including damaging inbound and lateral exploitation, command and control communications, internal reconnaissance, and malware that is spreading across the network.

The Malware Event Analytic Model | provides automated decisions on incidents based on whether malware is spreading, the value of the system in question, how dangerous the malware is and enables rapid, efficient and effective incident response.

The Web Filter Analytic Model | autonomously monitors and analyzes all outbound web requests reported by web filtering technologies for malicious attacks, including the discovery of targeted campaigns against the network, identification of client-side exploitation, command and control traffic, and data exfiltration.

The Endpoint Detection and Response Analytic Model | autonomously evaluates the suspicious process alerts, and in some cases, executes an additional query against the endpoint agent to gather more contextual information before making a decision. This model is particularly suited to identify host intrusions that may go undetected by endpoint protection platforms, given that the model evaluates suspicious behaviors. The Respond Analyst goes beyond standalone EDR solutions by classifying the process behavior and incorporating other security events as corroborating evidence for the escalation.

SUPPORTED TECHNOLOGIES

To see a complete list of supported technologies, visit the Respond Software Supported Technologies page. The Respond Analyst is constantly learning new skills and capabilities. If there is a specific technology not listed on the website, please contact us at info@respond-software.com.

About Respond Software

Respond Software is the cybersecurity investigation automation company and creator of the Respond Analyst, an XDR engine built to accelerate investigations for security operations teams. Defense agencies, government bodies, universities, large enterprises, and leading managed service providers use the Respond Analyst to get investigation power at machine speed. The Respond Analyst works with the broadest range of vendors, sensors, threat intelligence and data repositories in the industry to improve detection and response while raising security analyst productivity. Since its founding in 2016, Respond Software has partnered with more than 100 customers to apply data science to help security operations defend their enterprise. **www.respond-software.com**.