RESPOND ANALYST™

TECHNOLOGY WHITE PAPER

MAY, 2018

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

Overview

Respond Analyst is the first software expert system to automate the monitoring and analysis tasks performed by front-line security analysts. Respond Analyst emulates the judgment and reasoning of experienced security professionals with speed, scale and consistency unmatched by today's manual processes. Leveraging the latest advancements in artificial intelligence, machine learning and modern stream-based architectures, and leveraging Respond Software's unique Probabilistic Graphical Optimization (PGO™) technology, Respond Analyst acts autonomously – without a heavy system management burden, security engineering oversight, or long learning cycles.

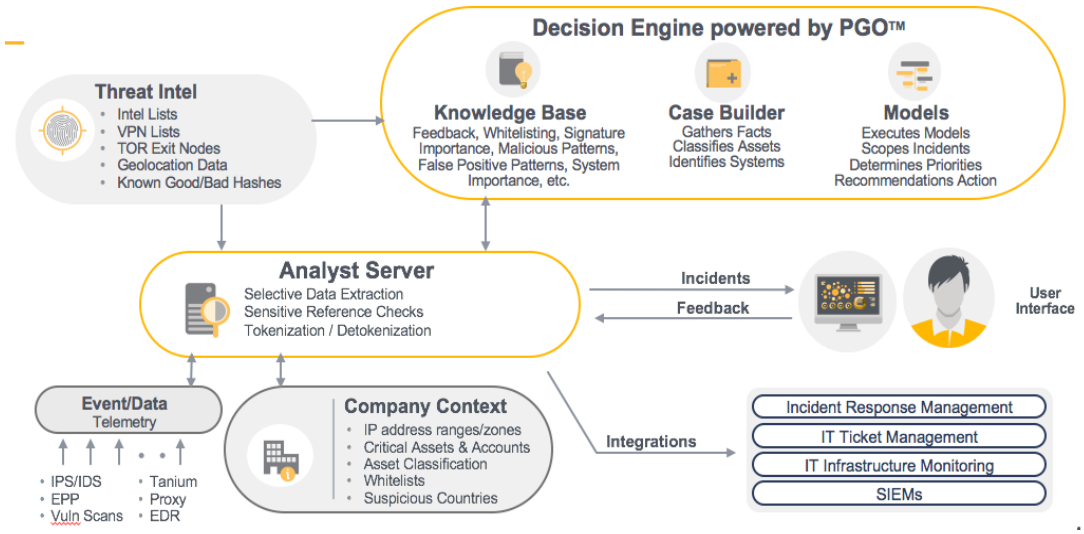
Respond Analyst is designed to process every event detected*, not just alerts labeled "critical," and perform extensive checks on each and every security event. There is no need to filter events from the source data to accommodate the human analysts' Events Per Analyst Hour (EPAH) capability –Respond Analyst scales horizontally to handle all events. The result is a greater depth of coverage and increased consistency in the analysis of high value and difficult to analyze security telemetry that contains important and relevant evidence of potential threats. As a security expert decision system, Respond Analyst is scalable and transparent, handling large volumes of streaming security events and creating detailed and vetted security incidents (cases) that require response from security or IT.

Designed to easily integrate into any security infrastructure, 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 content to maintain.

Currently, Respond Analyst is trained in to handle two telemetries - Network Intrusion and Malware Activity. Additional Analysis will be available later in 2018.

ARCHITECTED FOR SCALABILITY

Respond Analyst was built to support the exponential growth in security-important data and the many different types of infrastructures in today's security environments. Respond Analyst has two components – the Analyst Server, which can be run on-premise or in the cloud, and the Decision Engine, which is a cloud application. Customers can choose the implementation that matches their business need.

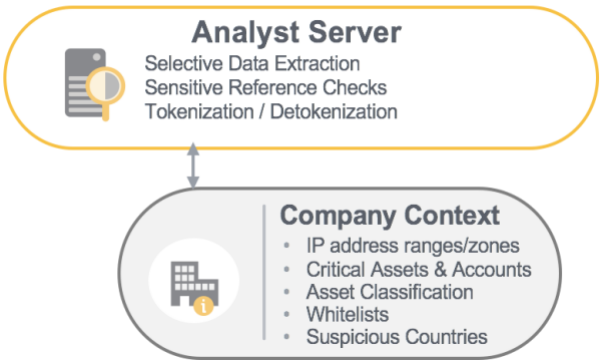


Respond Analyst leverages existing security event collection infrastructure, extracting and securing the data the Respond Analyst needs onsite, tokenizing sensitive information and completing deeper analysis with the Decision Engine.

ANALYST SERVER

The Analyst Server extracts specific event information from existing security detection sensors, company context about the IT environment, and global threat intelligence.

If the Analyst Server is hosted on-premise, sensitive reference checks of identifying event fields are performed, for example, a lookup of an internal IP address or hostname to check if it is on the critical asset list. Identifying fields are tokenized and the annotated and anonymized event is sent to the clients' dedicated Decision Engine tenant for processing.

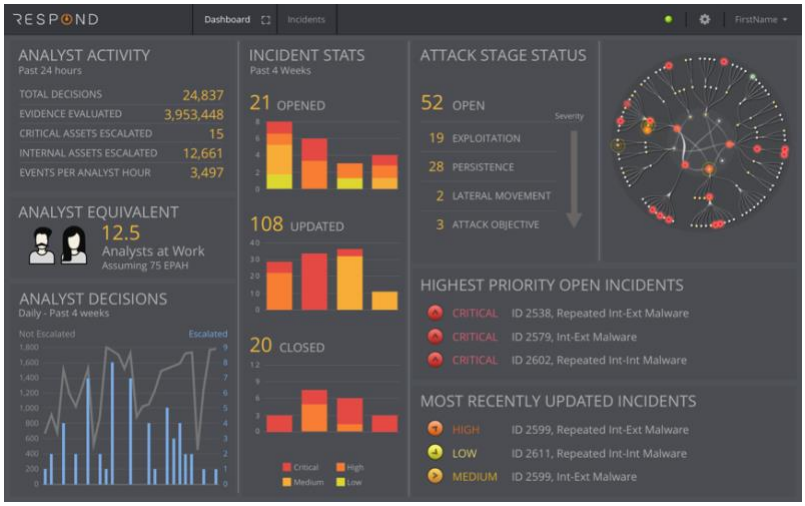


The Decision Engine comes pre-structured with expert judgment and adapts while maintaining "tribal" knowledge 24x7x365 to perform without fatigue, loss of attention or staff attrition. This mix of expert judgment and self–adaption enables Respond Analyst to immediately produce high-fidelity results and improve quickly as it works with a security team.

ANALYST SERVER - EVENTS & CONTEXT

During onboarding, the administrator of the Analyst Server is asked to provide important context about the IT environment through Respond Analyst's management dashboard interface -- information about the company's publicly-owned IP space, critical assets and accounts, security and network infrastructure such as vulnerability scanners and load balancers, network IDS/IPS signatures of high or low importance to the organization, and asset vulnerability information. Not all context is required for 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 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 that include Hadoop, Splunk, and SIEM forwarders and connectors from products such as Micro Focus ArcSight and IBM QRadar. The Analyst Server will also accept streaming events directly from the network IPS management and endpoint protection platform consoles themselves. Unlisted event sources are also possible since the Onsite Analyst Server listens for events on TCP-6060, UDP-514, and HTTP-6080.



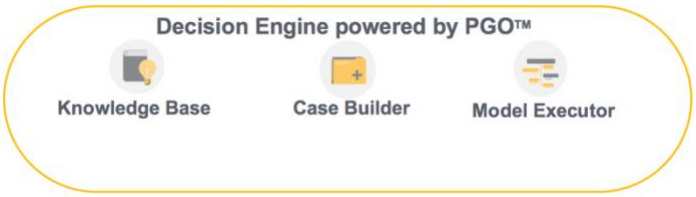
If the Analyst Server is installed on premise, the server can be physical or virtualized, and requires at least 8 cores, 64 GB of RAM with a minimum 48 GB free RAM, and 512GB disk space.

ANALYST SERVER: EVENT PROCESSING

As the Analyst Server receives events, it checks IP addresses and hostnames against sensitive contextual references such as the critical asset list, critical account list, file name checks, geolocation information, and vulnerability data. The events are annotated with the results of these checks and translated into a proprietary event format.

If the Analyst Server is installed on-premises, sensitive fields like IP addresses, hostname, account and domain name, file name, and sensor IDs are tokenized and a mapping of the tokens to original values is embedded in a database on the on-premises Analyst Server. Batches of events are then sent securely to the Respond Software Cloud.

DECISION ENGINE



Decision Engine has three features that codify the foundational knowledge, complex decision-making process and ongoing learnings of a highly skilled security analyst – Knowledge Base, Case Builder and Model Executor.

What is PGO?
At the core of the Respond Analyst is Probabilistic Graphical Optimization (PGO). PGO was developed by Respond's security experts and data scientists to analyze all network events, equate malicious attacks and determine which incidents should be investigated. PGO utilizes the most critical variables a SOC analyst considers relevant and decides if an event is malicious and actionable.

PGO is a patent-pending, multi-layered technology developed at the unique intersection of applied mathematics, security expertise and knowledge, and proprietary algorithms. With machine-level scalability, PGO 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, PGO 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. PGO is foundational the Respond Analyst decision models, delivering efficient and effective security

KNOWLEDGE BASE

Knowledge Base
Feedback, Whitelisting, Signature Importance, Malicious Patterns, False Positive Patterns, System Importance, etc.

Events from the Analyst Server 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 Analysis Module, 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 Analysis Module, Respond Analyst keeps a record of attributes shared across systems the organization, and leverages this knowledge base to look for patterns indicating malware may be spreading or isolated within the environment.

Additionally, Respond Analyst keeps track of repeat offending systems and accounts, corroborating suspicious garnered from the Network Intrusion Module within the Malware Event Analysis Module.
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 exit nodes lists.

CASE BUILDER

The Case Builder evaluates if the systems, 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.

This feature gathers the information required for Respond Analyst to answer a series of analytical questions for every event.

MODEL EXECUTOR

The Respond Analyst executes Analysis Modules, which are created to support the growing number of telemetry that the Respond Analyst evaluates. The Respond Analyst is skilled in Network Intrusion Analysis and Malware Event Analysis. For more specifics on these models, see the section below.

Just like a front-line security analyst, the Respond Analyst decides to either:
- Escalate the case, with the recommendation that incident response should perform containment and remediation actions
- Escalate the case, with the recommendation the system(s) evaluated should be reimaged and reissued, not requiring incident response
- 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.

ANALYSIS MODULES

Analysis Modules are delivered, pre-built with Analyst Server and Decision Engine content Two Analysis Modules are available with additional modules becoming available throughout 2018.

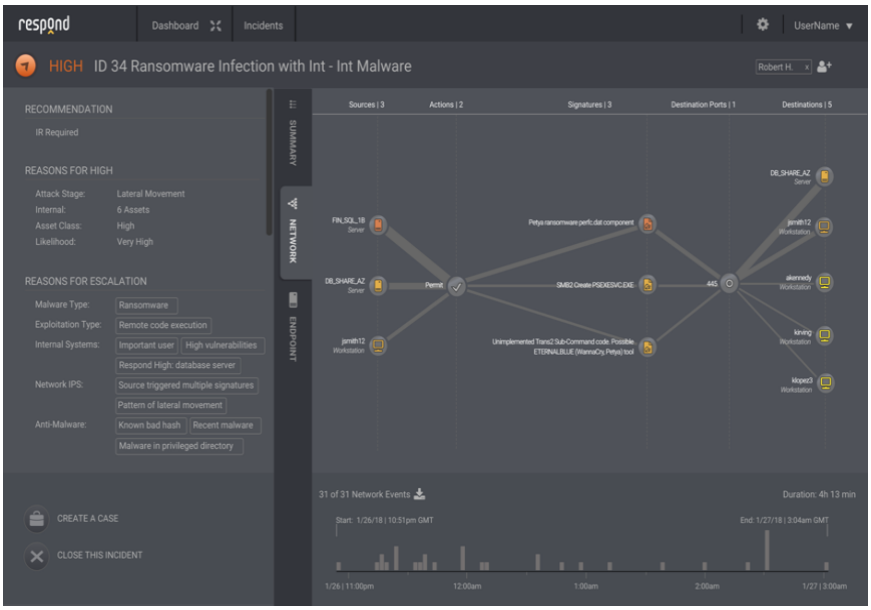
The Network Intrusion Analysis Module receives Network Intrusion Detection & Prevention Systems (IDS/IPS) data
With 58+ checks, the Network Intrusion Module provides automated decision on incidents that are malicious and actionable and provides visibility across a broad range of attacks, such as but not limited to **damaging inbound and lateral exploitation**, **command and control communications, internal reconnaissance, and spreading malware across the network.**

The Malware Event Analysis Module receiving Endpoint Protection Platforms (EPP) data
With 25+ checks, the Malware Event Analysis module provides automated decisions on incidents based on whether malware is spreading, the value of the system in question, how dangerous the malware is, how it output that enables rapid, efficient and effective incident response.

WORKING WITH THE RESPOND ANALYST

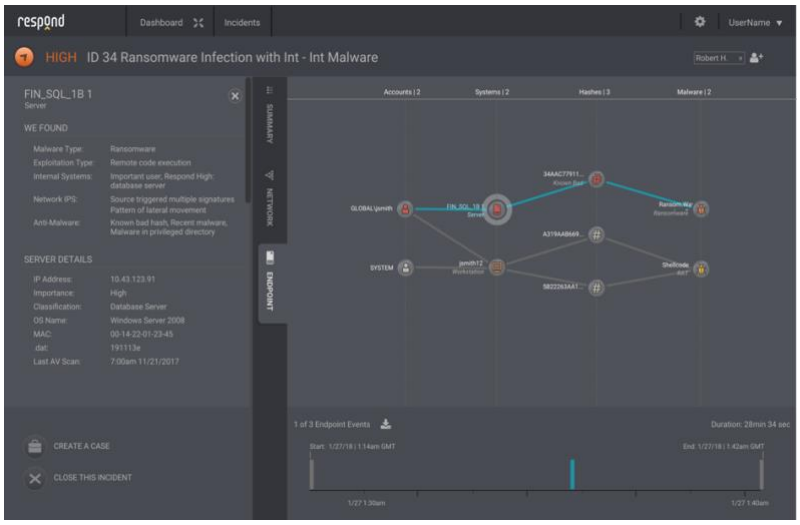
INCIDENT RESPONSE

Upon completing its processing, the Decision Engine securely returns scoped and prioritized incidents to the Analyst Server which de-tokenizes the sensitive information and presents the incidents to the security team. If configured, security personnel will receive notification of a newly escalated incident via an email notification. Integration with notification systems, such as PagerDuty, is also available.



The Respond Analyst interface is specifically designed to present the evidence that led to an escalation as well as the reason for its priority and a graphical representation of the incident, including time-based analysis, to further clarify and support its escalation decision.

If Respond Analyst decides the incident requires an incident response, escalations from both network IPS and endpoint protection telemetries and future Respond Analyst Modules can be scoped together into a single incident based on common systems, attacks, or hashes. Within the interface, the incident can also be assigned to a user and/or sent to a configurable case management solution.

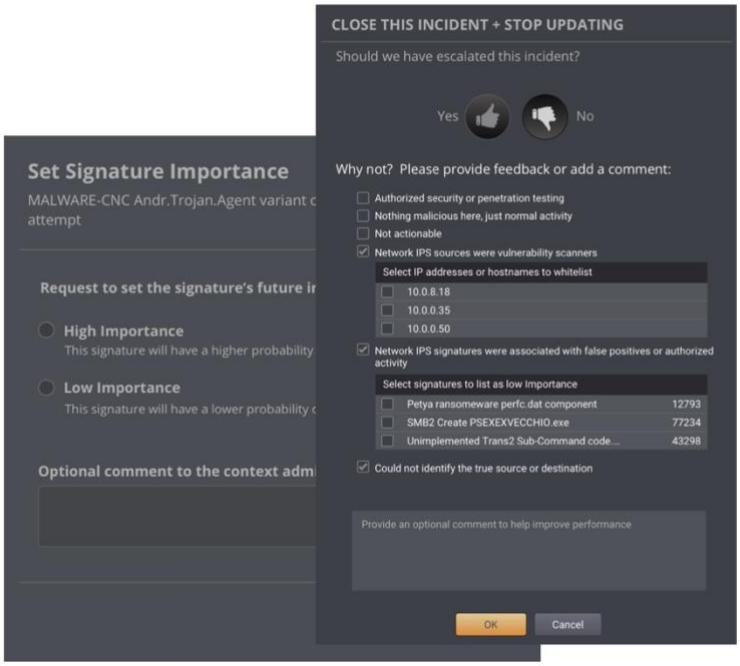


Respond Analyst decides that incident response is not required but recommends the system being escalated should be reimaged and re-issued, the user is presented with the interface of an Infected system. Within the interface, the incident can also be assigned to a user and/or sent to a configurable IT ticket management solution. The user can also configure Respond Analyst to output escalations in syslog, which could be used for ingestion back into a SIEM.

PROVIDING INCIDENT RESPONSE FEEDBACK

Although the Respond Analyst is operational and effective on implementation, ongoing feedback is important in order to improve results and adapt to changes in an IT environment.

Respond Analyst is an interactive tool that allows users to request adjustments to the criticality of assets and the importance of specific signatures directly in the reporting interface. These requests are collected and made available to the administrator in the Respond Analyst management interface where they can be quickly reviewed and accepted or rejected.



When an incident responder closes incidents in Respond Analyst, they are asked to provide feedback. If the outcome is a “good” escalated incident (thumbs-up), incident cases with similar evidence will have a higher probability of escalating, if the outcome is a “bad” escalated incident (thumbs-down), incident cases with similar evidence will have a lower probability. In the negative case, Respond Analyst collects additional qualitative reasons to improve the Knowledge Base. For example, the incident responder can give feedback to Respond Analyst that the escalated incident was a result of an internal vulnerability scanner. Or the incident responder may want to lower the importance of an observed network IDS/IPS signature because it generates false positives within the organization’s environment.
As incident responders provide feedback, the Decision Engine optimizes its models and updates the Respond Knowledge Base, ensuring that future decisions take into account up-to-date context, malicious patterns, anomalous behavior, and changes in environment and attacker approach.

SUPPORTED TECHNOLOGIES

Network IDS/IPS

- Cisco FirePower
- Fortinet FortiGate
- Palo Alto Networks
- Suricata
- Snort
- Trend Micro TippingPoint

Endpoint Protection Platforms

- Symantec Endpoint Protection

Event repositories/connectors

- SIEM Platforms (e.g. Splunk, ArcSight, QRadar)
- ELK, Hadoop
- Direct from end product

Company Context

- Internal Assets, Whitelisted Assets, and Critical Assets
- Critical Accounts
- Vulnerability Scanners (e.g. Qualys, Rapid7)
- Inferred Asset Classification (Tanium, Symantec)
- High Importance and Low Importance Network IPS Signatures
- DNS Servers

Threat Intelligence

- IP Address Reputation
- IP Anonymization (e.g. Public VPNs, TOR Exit Nodes)
- IP Geolocation
- Known Bad Hashes
- STIX/TAXII Integration

Operations Management

- Email
- IBM Resilient
- ServiceNow
- PagerDuty

Respond Software redefines Security Operations with the first security expert system, the Respond Analyst. Driven by its patent-pending Probabilistic Graphics Optimization (PGO) technology, Respond Analyst emulates the decision-making of an expert security analyst, effectively becoming a SOC team member that specializes in high-volume, low signal use cases while it applies, adapts and maintains an organization's tribal knowledge 7x24x365. Respond Software was founded by security operations veterans and world-class product technologists to serve its customers across multiple industries