# The Respond Analyst™ | an XDR Engine

## 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 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 25 percent of their time chasing false positives.

To address these issues, Respond Software offers the Respond Analyst, an XDR Engine. The Respond Analyst intelligently connects disparate SOC evidence by applying patented, probabilistic mathematics and Integrated Reasoning to determine the likelihood that events are malicious, actionable and important enough to escalate to security personnel. The Respond Analyst augments security operations teams by significantly reducing the need to chase false positives resulting in more time for threat hunting.

### An Open Architecture

The Respond Analyst integrates with the broadest range of vendors, telemetries and threat intelligence, so you can choose best-of-breed solutions to modernize your sensor grid. Or keep your existing tools without the need to rip and replace them. The Respond Analyst works with over 65 vendor offerings across important categories such as Endpoint Detection and Response (EDR), Enpdoint Protection Platforms (EPP), Incident Detection and Prevention Systems (IDS/IPS), Web Filtering, Security Information and Event Management (SIEM), Vulnerability Scanning, Authentication, and more.

The Respond Analyst integrates directly with Security Orchestration Automation and Remediation (SOAR) platforms to reduce attacker dwell time. The Respond Analyst saves you time and effort because you are not responding to false positives – only actionable incidents are escalated by the Respond Analyst.

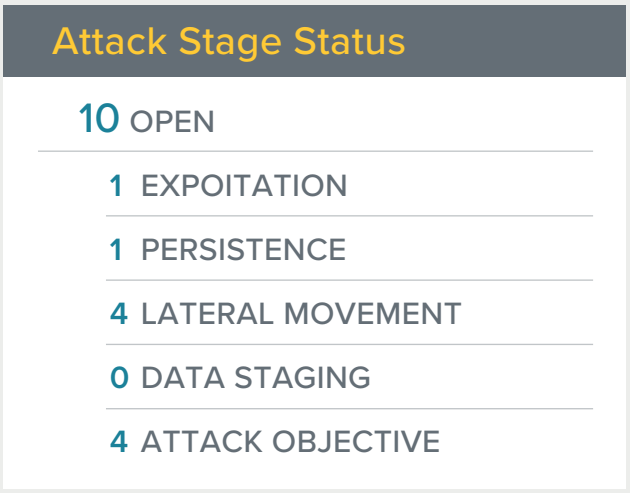
### Key Benefits

- Provides an open architecture allowing choice for best-of-breed technologies
- Built-in intelligence that does not require playbooks, rules or scripts saving time and cost
- Automates monitoring, detection, triage and escalation of well vetted incidents
- Installs in hours providing a quick time-to-value
- Integrates with the leading SOAR products for quicker remediation and reduced attacker dwell time

## Automated Security Investigations

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
- Provides detailed cases in an intuitive incident summary with all available evidence of malicious activity
- Notifies incident response team via email/ PagerDuty, re-notifies if priority is upgraded



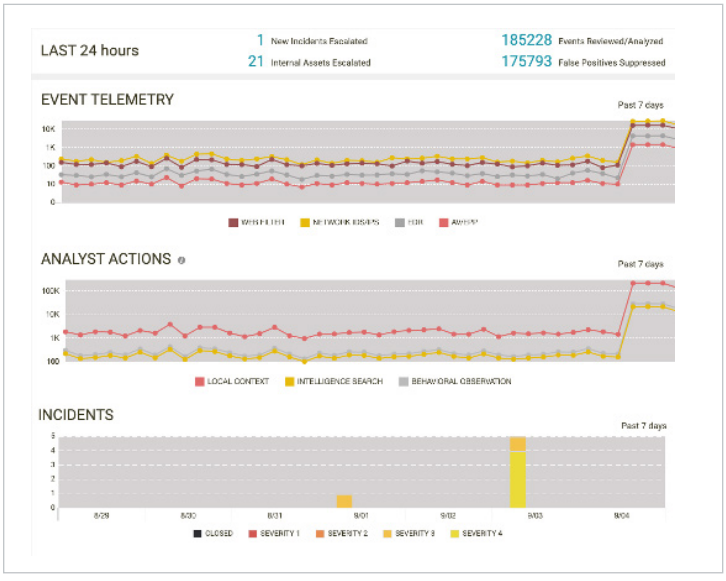

*Evaluates all alerts and performs extensive checks on each.*

- Learns from customer feedback and integrates with SIEM, Big Data, SOAR, ticketing and case management platforms to reduce attacker dwell time
- Incidents are presented and mapped to the stages of the MITRE ATT&CK™ framework
- For Managed Security Service Providers (MSSP), the Respond Analyst includes multi-tenancy capability for easy customer management
- Exposes the quantity of alerts that are monitored, analyzed and escalated (if necessary) including false positives

## Speed, Scale and Consistency of Software

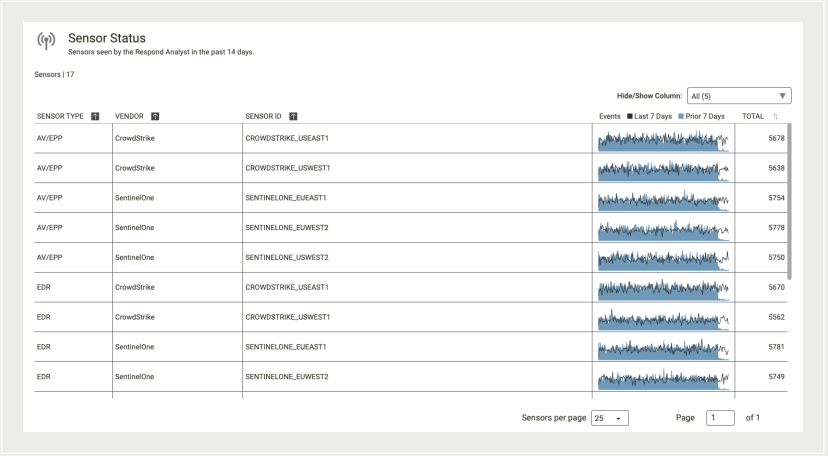
The Respond Analyst runs 24x7x365 and scales to the largest enterprises. It integrates with existing security infrastructure including SIEM and SOAR platforms, and removes the need to filter, tune-down or ignore security events to match the monitoring capacity of human analysis. Because the Respond Analyst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

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 streams and is evaluated, the Respond Analyst dynamically rescopes and reinterprets the attack stage. If necessary, the Respond Analyst will reprioritize the incident.*

The Respond Analyst includes a complete checklist of security sensors in the environment.




# Supported Technologies and Vendors - GA

## Network Intrusion Detection & Prevention

- Check Point SmartDefense
- Cisco Firepower NGIPS (Sourcefire)
- Fortinet FortiGate NIDS
- Gigamon Insight (ICEBERG)
- McAfee Network Security Platform
- Palo Alto Networks NGFW IPS
- Snort NIDS & IPS
- Suricata IDS
- Trend Micro TippingPoint

## Endpoint Detection & Response

- VMware Carbon Black EDR
- Crowdstrike Falcon Insight: EDR
- SentinelOne EDR

## Threat Intel Info

- IP Reputation, IP Anonymization (e.g. Public VPN & TOR Nodes), Geolocation, Known Bad Hashes

## Industrial Control Systems

- Forescout Security Matters

## Context Integrations

- DHCP (Windows, UNIX, Fortigate, Infoblox)
- Microsoft AD
- Vulnerability Scanners (Tenable Nessus, Tenable Security Center, Qualys, Rapid7)
- Tanium Asset
- VMware Carbon Black Response

## Endpoint Protection Platforms

- BlackBerry Protect (CylancePROTECT)
- Broadcom Symantec Endpoint Protection
- Crowdstrike Falcon Prevent: NGAV
- Fortinet FortiClient NGEPP
- McAfee Endpoint Security
- McAfee VirusScan
- Microsoft Windows Defender
- Palo Alto Networks Traps
- Palo Alto Networks Cortex XDR
- SenitnelOne EPP
- Sophos Endpoint Protection
- Trend Micro Apex One
- Trend Micro OfficeScan
- Trend Micro Deep Security

## Threat Intel Integrations

- VirusTotal
- Open Threat Exchange (OTX)
- Maxmind
- DShield
- WHOIS
- STIX/TAXII (Supporting most commercial vendors, e.g. Anomali and OASIS)

## Customer Info

- Critical Systems, IP space, DNS servers, Critical Accounts, Internal/ External Safe List, Malware importance, Guest/Unmonitored networks, Filehash Safel List, Banned/Suspicious Countries, Signature Importance

## URL/Web Filtering

- Check Point URL Filtering
- Cisco Firepower URL Filtering
- Cisco Umbrella / Umbrella DNS WF
- Forcepoint Web Security
- Fortinet FortiGate Web Filtering
- Fortinet FortiClient Web Filtering
- iBoss Secure Cloud Gateway
- McAfee Web Gateway
- Broadcom Symantec Web Filter (Blue Coat ProxySG)
- Palo Alto Networks NGFW URL Filtering
- Websense
- Zscaler Secure Web Gateways

## Event Repository Integrations

- SIEM (e.g. AlienVault, ArcSight , QRadar, Splunk, Sumo Logic)
- ELK, Hadoop
- Google Cloud Storage
- Palo Alto Networks Cortex
- Direct from security event product

## Operations Management

- Automated Communication Platforms (e.g. PagerDuty, Email)
- ServiceNow
- IBM Resilient SOAR
- Palo Alto Networks Cortex XSOAR (Demisto)
- Splunk Phantom




© 2020 Respond Software. All rights reserved.