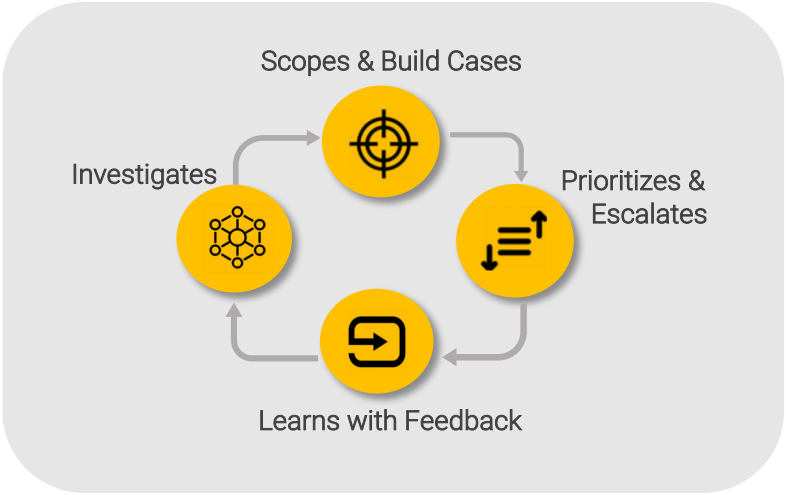
Respond Analyst

Power Your Security Team With Automated Monitoring and Triage

Respond Analyst is the first decision automation system for cybersecurity.
With the speed, scale and consistency of modern software,
Respond Analyst is ready to go to work, out-of-the-box.



- Evaluates every alert with consistency and speed
- Considers relevant contextual information to make better-informed decisions and identify real threats
- Groups related events into actionable security incidents
- Builds detailed cases with decision-making transparency
- Reprioritizes escalations as new information develops
- Builds and maintains tribal knowledge for future investigations

Autonomous Decision Making

Respond Analyst is pre-built with years of security expertise – no programming or long learn modes to achieve results – and adapts based on feedback and contextual input.

Escalates Actionable Incidents for Response

Based on layered analysis across gathered evidence, Respond Analyst escalates vetted and actionable security incidents. The breadth and depth of the analysis ensures high accuracy rates making efficient use of analyst time.

Consistent, 24x7 Coverage

Respond Analyst looks at all events, all the time without taking short-cuts or human bias. Since all security data may contain hidden clues, Respond Analyst evaluates all data without tuning or filtering down sensors based on static rules.

Easy to Install, Fast Results

Respond Analyst is easy to install and works with most security technologies. With a straightforward installation process, Respond Analyst can be on the job and delivering results from day one.

Intelligent Decision Engine based on PGO®

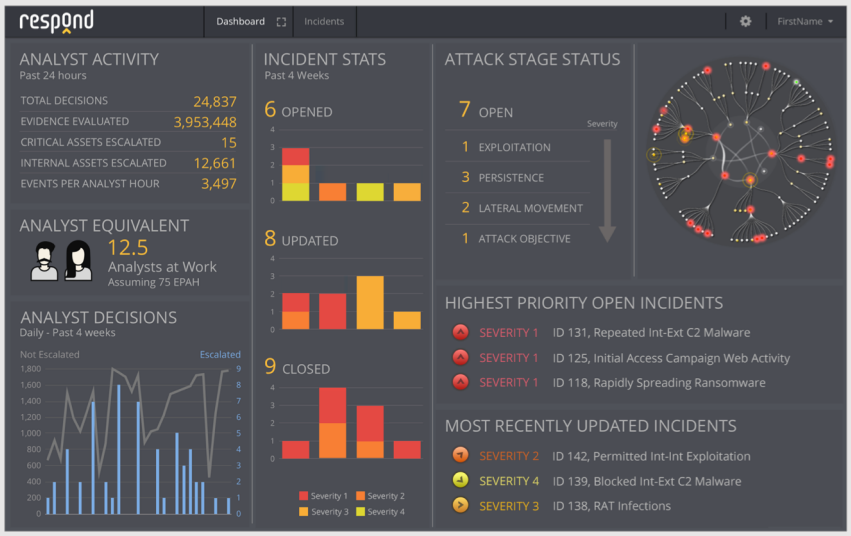
Probabilistic Graphical Optimization (PGO) is a patent-pending technology that uses to model human judgment, decision-making and learning. PGO leverages advanced modeling principles and techniques to analyze and reason security events and alerts across dozens of dimensions to ultimately come to a conclusion about the likelihood that the activity is malicious and actionable.

Respond Analyst Dashboard View

Respond Analyst tracks its progress for metrics and KPI reporting.

Operates at the capacity of a team of analysts

Evaluates all alerts, and performs extensive checks on each.



Dynamically rescopes and prioritizes incidents as new, related information is streamed and evaluated.

Presents evidence-based escalations detailing why alerts were escalated and the context behind them.

Respond Analyst provides in-depth analysis for a broad range of security use cases with a growing number of analysis modules.

Network Intrusion Analysis

- Dangerous network exploitation both inbound and laterally
- Command & Control communications
- Internal reconnaissance
- Spreading malware across the network

Malware Event Analysis

- Propagating malware between hosts
- Destructive or modern malware, such as Ransomware
- Infections on sensitive or critical systems

Web Filter Analysis

- Discovery of targeted campaigns
- Identification of client-side exploitation
- Analyze Command & Control traffic
- Identify data exfiltration

Supported Technologies

Network Intrusion Detection & Prevention
- Cisco FirePower
- Fortinet FortiGate
- McAfee
- Palo Alto Networks
- Snort
- Suricata
- Trend Micro TippingPoint

Endpoint Protection Platforms
- Microsoft SCEP
- Symantec Endpoint Protection

Industrial Control Systems
- Security Matters

Web Proxy & URL Filtering
- Palo Alto Networks
- Symantec ProxySG

Event & Alert Sources
- Direct from end product
- ELK, Hadoop
- SIEMs (e.g. ArcSight, QRadar, Splunk)

Company Context
- Active Directory
- Internal, whitelisted, and critical assets
- Critical accounts
- Inferred asset classification (Symantec, Tanium)
- Important accounts
- Vulnerability (e.g. Qualys, Rapid7, Tenable)

External Context
- IP Reputation
- IP Anonymization (e.g. Public VPN & TOR Nodes)
- Geolocation
- Known Bad Hashes
- STIX/TAXII Integration
- Threat intel lists
- WHOIS

Operations Management
- Demisto
- Email
- IBM Resilient
- PagerDuty
- ServiceNow

For more information, contact Respond Software at info@respond-software.com
or go to: www.respond-software.com

1002-10 2018

Gartner Cool Vendor 2018

respond SOFTWARE