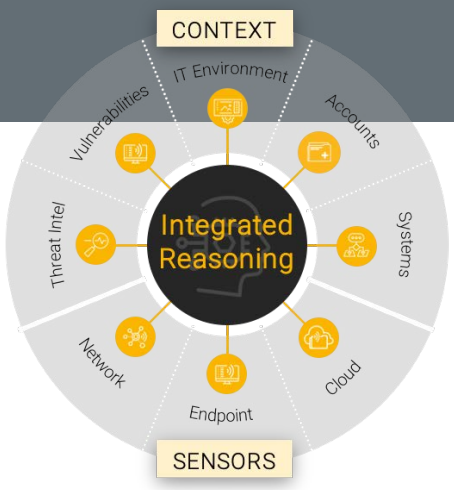
Respond Software | at-a-Glance



Automated Alert Investigation: Fast, Consistent, Cost Effective

The Respond Analyst, an agnostic XDR engine, integrates with the broadest range of vendors, telemetries and threat intelligence, so your customers can choose best-of breed solutions without the need to rip and replace existing tools.

The Respond Analyst XDR Engine deploys in hours and constantly learns without tuning, coding or content writing. It is cloud-native, so there is no infrastructure to manage.

The Respond Analyst XDR Engine has been hard at work across the customer base. Year-to-date, the Respond Analyst has reviewed more than 1 trillion security events -- diagnosing impact, removing false positives, and escalating just over 5000 incidents. Known for its ability to scale, at a typical large-scale customer, the Respond Analyst processes over 700 million events and alerts per week, and escalates roughly 25 well-vetted, likely security incidents.

The Respond Analyst XDR Engine intelligently connects disparate SOC evidence. It does this by applying patented, probabilistic mathematics and a unique Integrated Reasoning engine to determine the likelihood that events are malicious, actionable and important enough to escalate to security personnel. The capacity to stream data in real-time, execute automated response playbooks via simple “right-click” actions or directly feed SOAR platforms, significantly reduces attack dwell-time.

Key Features

Visibility and Understanding (aka Sensors & Context)

- Uses multiple perspectives; network sensors, host-based sensors and security control points, to monitor in-bound, out-bound and lateral movement of potential attackers
- Monitors high-volume, low-signal security sensors that are challenging for humans
- Uses APIs and inferences to gather and infer context (assets, users, vulnerabilities, threats)

Expert Judgment in Software

- Makes a fully informed, rational and consistent decision in near real time
- Subject matter expert judgment is captured into mathematical decision models. The Respond Team has built more than 35 SOCs over the last 25 years and that expertise is captured in Respond Software’s models.
- Reasons to the most likely explanation using deeper analysis than human SOC analysts have time for; considering 40-60 relevant factors per decision model
- Integrated reasoning corroborates decisions using all supporting evidence

Automated Learning

- Learns from customer feedback
- Aggregates lessons from all customers to provide an awareness of the global security situation
- Tribal knowledge and local context are collected and maintained

Streaming Analytics

- Delivered through the cloud (or hybrid if you prefer) for security, scalability and efficiency
- Simple operational integrations via plugins and REST APIs
- Data lake and logging infrastructure agnostic - all major vendors supported

Respond Software | at-a-Glance

How Your Cybersecurity Team Benefits

Analyst

Get a cheat code for finding the bad guys

- Makes job fun again
- Discovers incidents faster
- Covers more alerts, in more depth
- Reduces the drudgery of console monitoring
- Pivots, swivels and correlates for you, automatically
- Reduces time wasted chasing false positives

SOC Tech

Empower your security analysts to respond faster

- Weaves together silos of data
- Reduces noise/false positives
- Accelerates time-to-value with complex logic built-in
- Wrangles data out-of-the-box
- Integrates seamlessly with SIEM / SOAR and other tech
- Gets real time sensor health data

SOC Leader

Improve team productivity, consistency and predictability

- Expands coverage while reducing unattended alerts
- Frees up people and resources
- Reduces night/weekend on-call burdens
- Increases analyst job satisfaction/reduce turnover
- Future-proofs your investigation capabilities

CISO

Reduce risk and optimize your budget

- Future-proofs your investigation capabilities
- Frees up people and resources
- Builds confidence we are finding everything
- Reduces hiring/training/managing pain

---

kyriba™

Case Study - FinTech leader builds world-class security

When protection from fraud and cybercrime and improved safeguards for financial data are among the key value propositions a business offers its customers, it's only logical that maintaining world-class cybersecurity operations is high on that company's priority list. Kyriba, a leader in FinTech, built an enterprise- grade security program that massively extends the SecOps team's capabilities. "We have seen that if there are more than about 75 events over an hour, it's just too many alerts," says Eric Adams, CISO at Kyriba.

"In our case, Respond Software covers Levels 1 and 2 alerts and can take actions based on a playbook, and escalate only those that need personal attention, so our personnel only look at those qualified alerts, determine whether they are valid or a false positive, and provide feedback into the Respond tooling." Powered by the intelligent decision-making skills of Respond Software their security program meets the strictest compliance standards and maximizes security operations efficiencies. Respond Software monitored 269M events, escalating just 4 incidents in a one-month period. That is the equivalent of 5,000 human analysts working 24×7 to cover 269M events in one month. "The automated nature of this solution helps reduce alert fatigue and frees analysts up to work on other tasks."

respond

Take a quick tour of the Respond Analyst
https://respond-software.com/respond-analyst

www.respond-software.com. For more information, email info@respond-software.com.