Technical Review

Respond Analyst: The Virtual Security Analyst

Date: February 2020 **Author:** Jack Poller, Senior Analyst

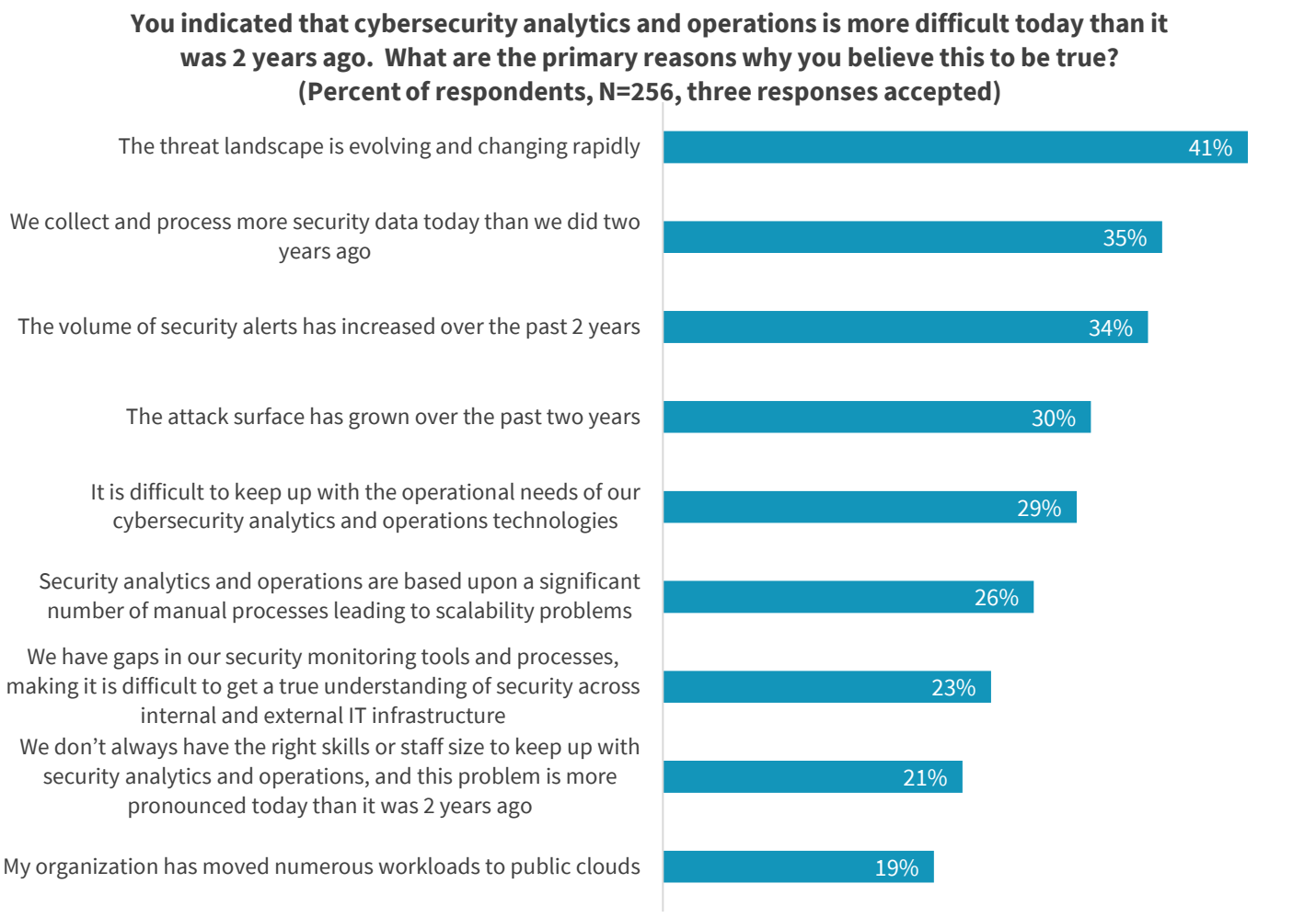
Abstract

This ESG Technical Review of Respond Analyst focuses on how the solution functions as a virtual cybersecurity analyst, analyzing cybersecurity telemetry, aggregating many events and alerts into security incidents, and efficiently and effectively presenting incidents to the security team for investigation and remediation.

The Challenges

According to ESG research, 63% of organizations say that cybersecurity analytics and operations is more difficult today than it was two years ago. These organizations most frequently cite the rapidly evolving threat landscape, the increasing volume of cybersecurity telemetry data, and the increasing volume of alerts as contributing factors (see Figure 1).[1]

Figure 1. Changing Threat Landscape and Security Operations Model



Source: Enterprise Strategy Group

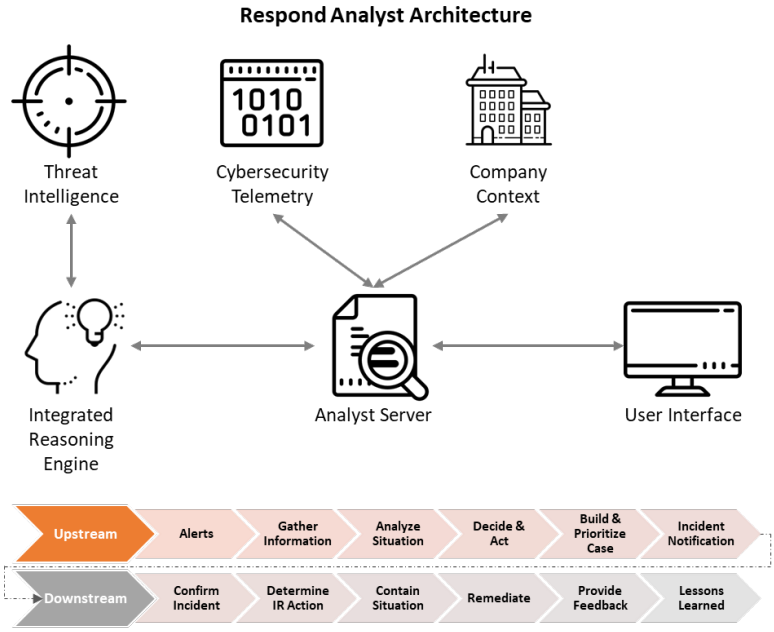
[1] Source: Master Survey Results, *Cloud-scale Security Analytics Survey*, December 2019.

Organizations are collecting and analyzing data from a wide range of telemetry covering endpoint, network, threat intelligence, vulnerability management systems, and more. More than three-quarters of ESG research respondents (77%) use ten or more security analytics and operations tools and these organizations say that two of their top challenges are monitoring security across a growing attack surface (27%) and keeping up with the volume of security alerts (23%).[2]

The Solution: Respond Analyst

Respond Software developed the Respond Analyst as a decision automation system for cybersecurity. Using Robotic Decision Automation (RDA), the Respond Analyst software provides automated reasoning and decision-making skills, ingesting large volumes of data and automatically triaging and investigating security events—escalating only fully scoped security incidents that require human action. Organizations can quickly deploy and leverage the automation that delivers the immediate scale and rapid ROI inherent in cloud-based solutions.

The Respond Analyst employs probabilistic mathematics and patented techniques incorporating the knowledge and expert judgement of human security analysts to monitor security telemetry, automating human analysis of security alerts and enrichment data. The software reduces false positives and prioritizes actionable alerts, providing the security team with all relevant data to investigate and remediate an incident.



The Respond Analyst automates the upstream process, gathering telemetry data, analyzing the situation, and building and prioritizing an incident. The software also automates the downstream process, helping the security analyst to confirm the incident, determine the appropriate response to remediate the incident, and gather and incorporate feedback into the decision-making process. The built-in automation learns from the local environment, aggregates data from all Respond Analyst deployments, and obviates the need for the security team to develop their own playbooks or rulesets.

Organizations deploying the Respond Analyst benefit from:

- Immediate escalation of actionable security incidents, resulting in the reduction of false positives.
- Reduction in the total number of incidents requiring security analyst review, enabling analysts to focus on high priority activities such as incident response and threat hunting.
- Reduction or elimination of human bias or fatigue through consistent, continuous, real-time monitoring and evaluation of important cybersecurity events and alerts.
- Integration of organizational context in the evaluation process, triangulating assets, users, and threats.
- Consideration of real-time threat intelligence and vulnerability scanning in the decision-making process.
- Faster and better decision making with reasoning based upon all available data sources.
- Aggregation of events and alerts into incidents based on common attacker tactics, techniques, and procedures (TTPs), leading to automated decisions and actions based on context.
- Incident prioritization considering asset criticality, attack stage progression, and likelihood of attack.
- Rescoping and reprioritization of incidents in real time as the Respond Analyst discovers and evaluates new evidence.

[2] Source: Master Survey Results, *Cloud-scale Security Analytics Survey*, December 2019.

- Incident summaries with instant access to all available evidence of malicious activity, accelerating incident confirmation and remediation.
- Integration of user feedback into automated analyses and decision making, improving accuracy and fidelity.
- Workflow integration with alert systems, SIEM, SOAR, ticketing, and case management solutions.
- Cloud-based software with fast deployment and rapid return on investment.
- Speed, scalability, and consistency inherent in modern software-as-a-service (SaaS) solutions.

ESG Tested

ESG engaged with the Respond Analyst dashboard, which provides a summary of the Respond virtual analyst activity. As shown in Figure 2, the left side provides a summary of the event telemetry tracked by sensor type, analyst activity, and the incidents over the last seven days. The dashboard conveniently translates these metrics into the number of human analysts theoretically added by the Respond virtual analyst, using the assumption that a human can evaluate and investigate 75 security events per hour. These metrics show the volume of evidence and events systematically evaluated by the Respond Analyst, bringing machine scale and consistency to every alert, not just those investigated by the security analyst team. Using this information, CISOs and security managers can better understand how the Respond Analyst reduces the time and effort expended by security analysts, enabling those analysts to focus on high priority tasks.

The center of the dashboard displays the attack stage status for all open incidents. The colors indicate the severity of the incident, with yellow indicating the lowest severity (severity 4), then amber (severity 3), orange (severity 2), and red for severity 1, the highest severity.

The right side of the dashboard displays summary of incidents based on the progression through the MITRE ATT&CK framework attack stages, and a list of the top-three highest severity open incidents and the top-three most recently updated incidents.

The dashboard also includes an animation that represents how the Respond Analyst decision models work: an event comes into the system and the virtual analyst virtually asks a series of questions (the outer ring of dots). The Respond Analyst uses mathematical models to "connect the dots" and decide, based on what is currently known, whether the events and evidence indicate a security incident.

Respond Software designed the dashboard to mimic the dashboards used by traditional security operations centers (SOCs) to provide at-a-glance understanding of the progression of detected attacks and the efficiency and effectiveness of both the Respond virtual analyst and the human analysts. The dashboard helps CISOs, security managers, and security analysts to understand the risk of successful attacks and data compromise and improves response prioritization.

Figure 2. Respond Analyst Dashboard

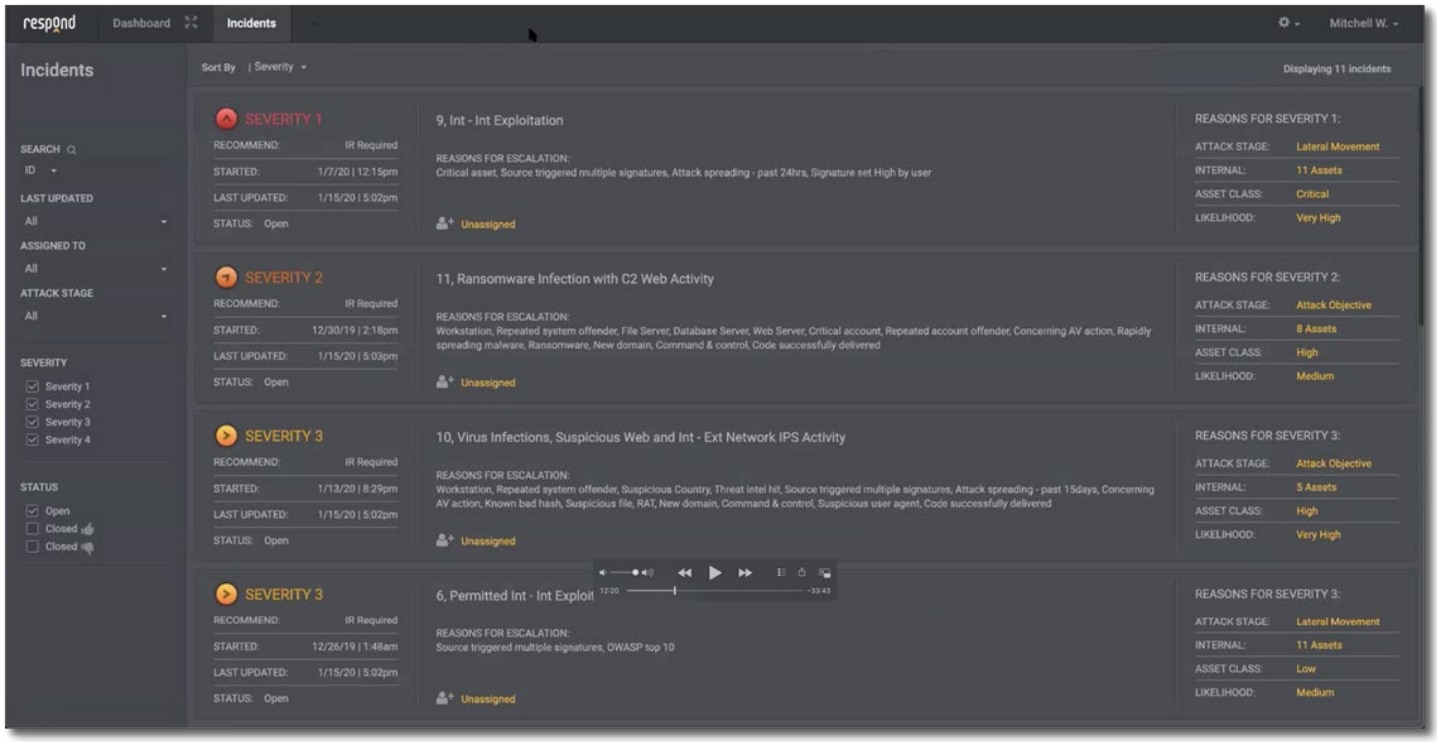
Source: Enterprise Strategy Group

Next, ESG selected ***Incidents*** from the top tab selection, which brought up the Incident queue, as shown in Figure 3.

Each incident in the queue is represented by a card providing key information, including severity (the most important data), recommended action, key dates, status, description, and the reason for escalation. The left side of the incident queue displays a set of quick filters, enabling the security analyst to search and filter based on numerous criteria including last updated, assigned to, attack stage, severity, and status.

Respond Software designed the incident queue to be the main interface used by security analysts and managers. The incident queue enables the security team to triage, prioritize, assign, and process incidents quickly and efficiently.

Figure 3. Incident Queue



Source: Enterprise Strategy Group

Security analysts typically are notified via email, pager (through integration with PagerDuty or other services), or a case management system. The link in the notification brings the user to the incident details page. This page can also be accessed directly from the incident queue by clicking on an incident. The incident page provides three views of an incident: the endpoint view, the web filter view, and the systems view.

ESG, acting as an incident responder investigating an incident, clicked on incident 11, Ransomware Infection with C2 Web Activity, which brought up the endpoint view of the incident details page, as shown in Figure 4. The left side of the incident details page provides additional information, including the reason that Respond Analyst classified the incident as severity 2 (accounting for attack stage, affected assets and asset class, and likelihood of impacting the organization), the reasons for escalation (malware type, affected systems, and anti-malware and web filtering coverage), and status.

The right side of the page presents the endpoint view of the incident. This view is a graphical representation of the typical EPP/AV contextual data: accounts, systems, hashes, and malware names (if known) and types. The bottom of the page contains the timeline of events, with a button to download the raw event details and evidence the virtual analyst collected. Clicking on a date in the timeline enables the analyst to play out the incident; events for that time are highlighted in blue in the visualization. The bottom of the page presents a daily bar graph showing the number of events each day that are part of the incident. Using this view, we rapidly understood how the users, accounts, systems, and malware are tied together. We were able to quickly judge the impact and dwell time of the malware and the level of effort necessary to remediate the attack.

Figure 4. Incident Details – Endpoint View

Source: Enterprise Strategy Group

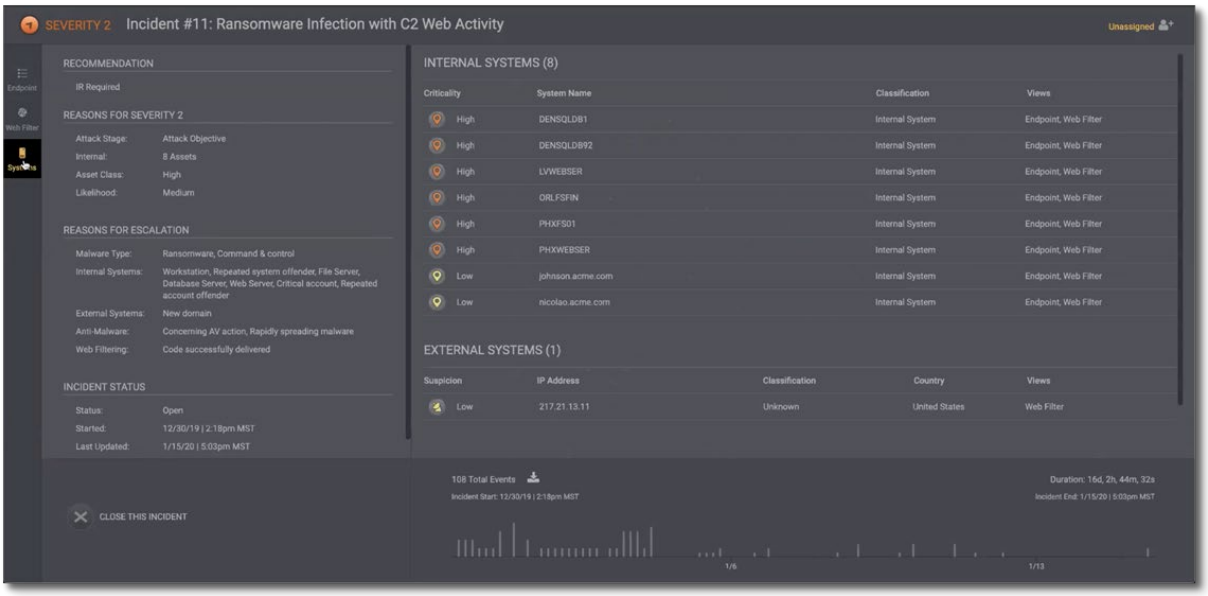
Next, we selected the ***Web Filter*** view from the left side tabs, which updated the right side with a graphical representation of the network activity associated with the incident, as shown in Figure 5. We compared the timelines between the endpoint and web filter views and noted that the endpoint view showed events at the beginning of the incident, representing the initial compromise, and the web filter view showed events later in the progression, which typically represents attempts to contact command and control servers.

Figure 5. Incident Details – Web Filter View

Source: Enterprise Strategy Group

As the last step in investigating this incident, we selected the systems view, which updated the right side with a list of affected systems, as shown in Figure 6. Respond Analyst used local contextual information to automatically rank affected systems based on criticality, enabling us to prioritize our remediation efforts.

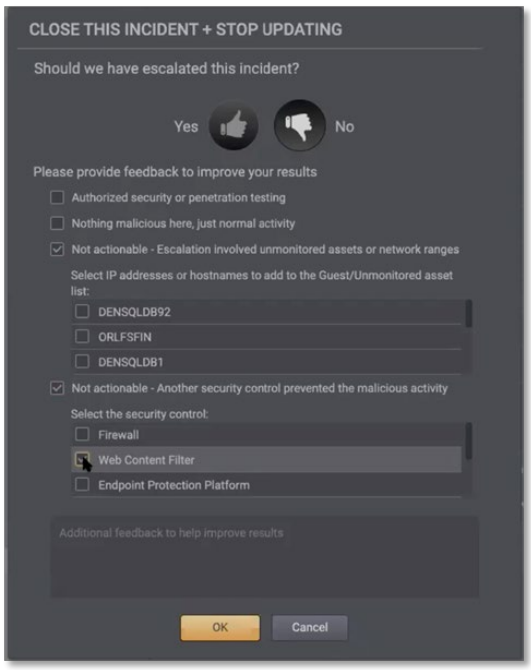
Figure 6. Incident Details – Systems View



Source: Enterprise Strategy Group

Acting as an incident responder, ESG clicked on ***CLOSE THIS INCIDENT***. As shown in Figure 7, Respond Analyst asked for detailed feedback information, which it uses to update the Robotic Decision Automation models for increased accuracy and fidelity. Information collected includes whether the incident should have been escalated, whether the incident was an actual malicious act, and which security control prevented the malicious activity.

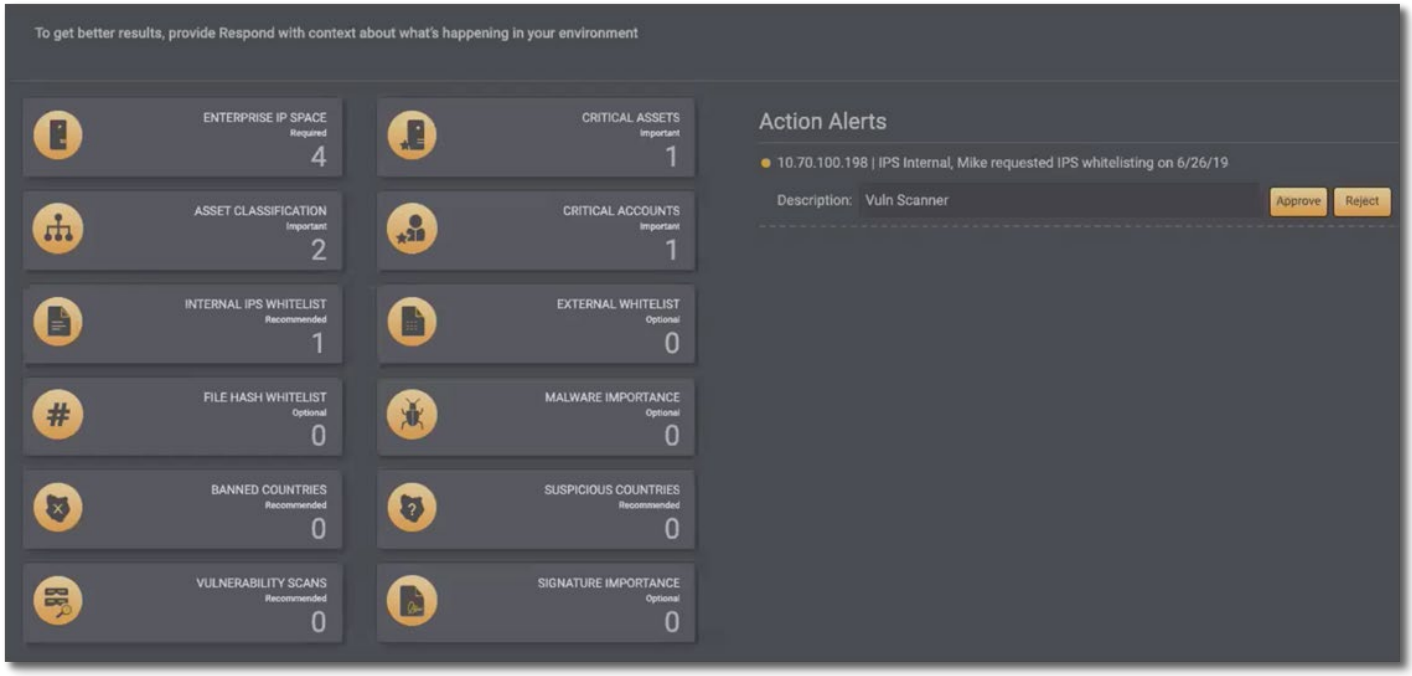
Figure 7. Virtual Analyst Feedback



Source: Enterprise Strategy Group

As the last step in the evaluation, ESG clicked on the gear icon at the top right to update the Respond Analyst configuration. We selected Context to provide additional contextual information to the models. The more context the system has, the better decisions it can make, improving the accuracy of identifying malware and improving the priority and severity classifications. Contextual information includes IP address space, banned countries, asset and user classifications, IPS whitelists, file hash whitelists, vulnerability scans, and critical accounts.

Figure 8. Context Configuration



Source: Enterprise Strategy Group

Why This Matters

Higher data volumes, the changing cybersecurity landscape, and new data security and privacy regulations are key IT complexity drivers—and why nearly two-thirds (64%) of organizations say IT *still* isn't getting easier. The cybersecurity skill shortage—44% say they have a problematic shortage of skills in that area—exacerbates the IT complexity issue.[3]

ESG validated that Respond Analyst functions as a virtual security analyst, potentially augmenting human analysts for less experienced and understaffed organizations. Respond Analyst applied a variety of automated decision models to analyze cybersecurity telemetry events and alerts, organizational contextual information, and common TTPs. The real-time analyses reduced millions of events into a few incidents representing potential malicious activity. Incidents were presented in cards that were easily consumed. We found that we rapidly developed an understanding of the overall state of the environment and were able to quickly investigate incidents. Respond Analyst presented the relevant contextual information, enabling us to decide upon the correct remediation action. We were then able to provide feedback to the system to improve fidelity and accuracy, reducing the likelihood of false positives.

[3] Source: ESG Master Survey Results, *2020 Technology Spending Intentions Survey*, January 2020.

The Bigger Truth

The ever-increasing volume, velocity, and sophistication of threats and attacks, combined with the ever-increasing volume, velocity, and variety of organizations' devices, data, and access methods is forcing organizations to deploy more cybersecurity controls, resulting in an ever-increasing volume of cybersecurity telemetry. Thus, security teams are deploying a multitude of security analytics tools—more than three quarters (77%) of organizations use ten or more analytics tools.[4]

An increase in the number of tools utilized increases security operations and analytics complexity and requires an increase in personnel. Yet nearly three-quarters (70%) say it is difficult to recruit and hire additional SOC staff. This is driving organizations to search for alternatives, including advanced analytics and machine learning, and 71% say their organization is planning to deploy or deploying machine learning technologies for cybersecurity operations and analytics.[5]

ESG validated that the Respond Analyst uses multiple machine learning models to analyze millions of cybersecurity telemetry events and alerts in real time. Using Robotic Decision Automation, the Respond Analyst behaves as a virtual analyst, and has the potential to replace or augment human analysts. Testing revealed:

- The Respond Analyst simplifies and accelerates cybersecurity telemetry event and alert processing, triage, and prioritization, combining multiple events and alerts into a single incident.
- The Respond Analyst dashboard provides a high-level SOC dashboard experience, enabling at-a-glance understanding of the current state of incident processing for CISOs and security team managers.
- The Respond Analyst incident queue enables rapid triage, prioritization, and assignment of incidents to responders.
- The Respond Analyst provides all relevant contextual data for an incident with network, endpoint, web filter, and system views, enabling incident responders to investigate incidents and follow suggested remediation steps quickly and efficiently.
- The Respond Analyst automatically requests and incorporates feedback into the decision models, improving fidelity and accuracy.
- The Respond Analyst leverages user-provided contextual information—IP addresses, user and system information, whitelists, and more—into the decision models, improving the ability to differentiate between valid user activity and malicious activity, decreasing false positives.

Organizations in need of advanced analytics and Robotic Decision Automation should thoroughly test the efficacy, functionality, and operational capabilities before purchasing or deploying any security operations and analytics solution.

If your organization is looking to streamline cybersecurity operations and analytics, then ESG believes that you should consider the effectiveness, efficiency, and potential ability to augment human cybersecurity analysts with the virtual analyst capabilities of the Respond Analyst from Respond Software.

[4] Source: Master Survey Results, *Cloud-scale Security Analytics Survey*, December 2019.
[5] ibid.