ESG Lab First Look

Resolve Systems: Accelerating Security Incident Response

Date: December 2017 **Author:** Tony Palmer, Senior Validation Analyst

Cybersecurity Challenges

72% The percentage of respondents who consider *cybersecurity analytics/operations* to be **somewhat or significantly** more difficult today than it was two years ago.[1]

45% The percentage **who believe** *cybersecurity is the area in which their IT organization* has **the most significant shortage of skills**.[2]

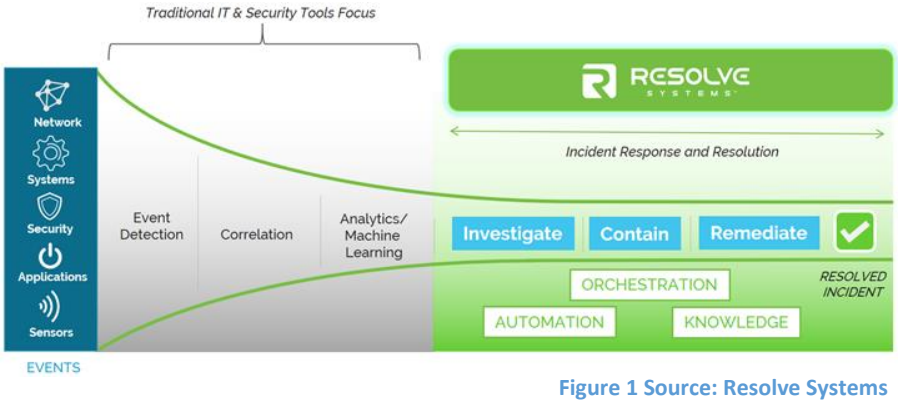

Figure 1 Source: Resolve Systems

Research from ESG and the Information Systems Security Association (ISSA) reveals that 70% of cybersecurity professionals believe that the global cybersecurity skills shortage has impacted their organizations.[3] Based upon this research, it's clear that most organizations don't have enough cybersecurity staffers, don't have some necessary cybersecurity skills, or both—a daunting situation. Meanwhile, the number of security incidents that businesses have to investigate and respond to has grown exponentially; the proliferation of new systems and applications is creating more security incident scenarios and better detection tools are generating more alarms. Considering the manual and ad hoc processes and actions commonly used to investigate and respond to incidents, along with the lack of collaborative tools between security operations and other IT teams, it's no wonder that organizations' mean time to response (MTTR) for security incidents is on the rise. It's not prudent or feasible to respond to the security challenge by simply adding more personnel. If your security analysts and investigators don't have the best incident response tools, investigation and resolution of security events will take longer, increasing the prospect of a damaging data breach.

Resolve Systems' Enterprise IT and Security Incident Response, Orchestration, and Automation Platform

Traditional cybersecurity solutions have focused on prevention and detection. In today's cybersecurity environment, this has translated into an overwhelming increase in alerts and incidents. Organizations need to be able to respond to incidents quickly and effectively. Resolve provides a unified security incident response (SIR) platform designed to connect responders across the enterprise using process and technology. The platform provides both case management functionality to manage the lifecycle and artifacts of incident response while adaptive automation capabilities ensure that the platform can be optimized for any incident types in any organization. The integrated platform ensures that the response process follows security incidents across teams, providing an audit trail and avoiding the data fragmentation that occurs with point solutions. With Resolve, security teams and responders across the enterprise are given access to standards-based playbooks, process guidance, and options for human-guided and closed-loop automation for security incident response.

Resolve captures all incident-related activities in a complete investigation record for compliance, forensics, evidence preservation, and reporting.

[1] Source: ESG Research Report, *Cybersecurity Analytics and Operations in Transition*, July 2017.
[2] Source: ESG Research Report, *2017 IT Spending Intentions Survey*, March 2017.
[3] Source: ESG Research Report, *ESG/ISSA Research Report: The Life and Times of Cybersecurity Professionals*, November 2017.

ESG Lab Demo Highlights

ESG Lab performed hands-on testing of Resolve Systems, triaging and resolving complex security incidents on a live production network.

Enterprise Security Incident Response

- ESG Lab started in the Splunk Enterprise Security dashboard, looking at a notable event that indicated a potential email phishing attack. We opened Splunk's ***Custom Actions Menu***, and selected ***Resolve Guided Resolution***. This took us to the ***Secops.Phishing*** playbook, which is an interactive procedure inside Resolve using a combination of a set of instructions with embedded automation and a larger process that guides the SecOps analyst through a decision tree construct.
- As SecOps works through the guided process, they can address and respond to the incident. Remediation involves multiple actions across many disciplines that Resolve can execute automatically as prescribed by subject matter experts across domains per best practices.

Figure 2 Source: Resolve Systems

- In less than five minutes, ESG Lab was able to walk completely through the guided resolution process. We quickly determined that the threat reported by Splunk was a real phishing attack, triggered the appropriate procedures to automatically block the outside sender and the bad URLs, and informed all affected internal users of the attack.
- Resolve provides a SecOps case management system that integrates with existing IT case management systems.
- When a case is created, SecOps can select a playbook template. Numerous templates are provided, based on the NIST Computer Security Incident Handling Guide. Playbooks are customizable without requiring coding of any kind.
- ESG Lab customized a playbook with just a few clicks. The playbook is represented as a visual flowchart; to create or edit a playbook or action task, users drag and drop elements into and out of the playbook in the Resolve Systems GUI.

First Impressions

ESG research reveals that the cybersecurity landscape is becoming increasingly difficult to manage. Organizations' critical assets, including intellectual property, customer information, financial data, and more are increasingly at risk of compromise. Repercussions from a breach are severe, including financial penalties, impact to brand and company valuation, and lawsuits. Organizations need a sophisticated incident response strategy in order to respond to incidents with agility and minimize risks.

Resolve Systems demonstrated a deep understanding of enterprise environments, providing cross-domain orchestration paired with adaptive, customizable automation. Resolve owns the resolution process from beginning to end, feeding results into the dashboard to drive resolution actions. Resolve is designed to enhance and augment existing solutions, providing a mix of manual and automated actions, seamlessly integrated into a guided resolution process. Automation development is robust and code-free, with the overall solutions enabling organizations to respond effectively and quickly to security incidents, threats, and breaches.

Resolve enables a security organization to discover, investigate, and manage responses to events from a single interface, while enabling other IT domains to use the tools they are comfortable with to address incidents completely, taking swift, focused, confident action.