Accelerating Security Incident Response

Abstract

It’s virtually impossible for today’s typical security teams and Security Operation Centers (SOCs) to quickly and accurately respond to the massive volume of threat-related events encountered across their networks and systems. This holds true despite their existing investments in threat detection software and infrastructure. Furthermore, expanding headcount to address the problem is not feasible. Not only is there a limited supply of highly skilled security personnel, but security teams and SOCs are also challenged by how quickly they can optimize people, processes and technology to respond and resolve security events; most SOCs today lack the ability to automatically validate, triage, classify and respond to the growing mountain of threats. What automation does exist in security incident response is also largely home grown, with substantial labor costs and designed to specifically address a single problem within a very specific context. Expensive and scarce talent thrown at limited and ad hoc processes does not scale. Without the ability to automate efficiently and to leverage limited resources, organizations will remain unable to adequately respond to threats, leaving enterprises exposed.

In reality, many of the automation challenges facing modern SOCs are quite similar to those encountered by IT and Network Operations Centers (NOCs) with respect to how they respond to and resolve the huge volume of network-facing incidents encountered on a daily basis. NOCs and SOCs both need be able to automate the validation of events and to quickly collect relevant contextual data in order to investigate, contain and remediate issues with a consistent and repeatable process. This is equally true for security and non-security related incidents, as are the corollary objectives of maximizing the productivity of highly skilled resources and resolving incidents as quickly and efficiently as possible.

This whitepaper discusses the challenges of scaling a security incident response team and the critical role that a best-in-class security incident response and automation platform can play in accomplishing this objective. To this end, this paper introduces Resolve Systems’ unique human-guided automation and how the Resolve® software platform enables SOCs to extract additional value from existing threat detection investments by providing the same end-user experience that has enabled large multi-national organizations and telecommunication companies to accelerate incident response.

Today's SOC is Inherently at Risk

The trajectory of many security operations today is unsustainable. Investments predominantly in prevention and detection systems may result in improved identification of potential or actual security threats, but this improved detection comes with a continually increasing volume of security events and "alert fatigue" in the SOC, that takes a toll on personnel that have to be processed by humans. Alert fatigue is itself a very real concern: In retrospect, it often proves to be the root cause of many high-profile security disasters that have cost many enterprises literally hundreds of millions of dollars in losses, along with significant reputational damage. Simply adding headcount is not a tenable solution; most security organizations are resource constrained, with limited budgets and even with budget for hiring, there is a limited pool of qualified candidates. But even if hiring were feasible, increasing the number of people responding to security events is, at best, a short-term patch, as doing so does not solve the underlying issue, which is the need to resolve security events in an efficient, repeatable and scalable manner.

In response, leading industry analysts and top organizations are beginning to realize that shifting the focus from threat detection towards improving incident response is long overdue and are now in search of solutions to enable this.

Security Incident Response and Automation

Most security operations have developed some form of incident response processes and procedures. Many are cobbled together from a variety of disparate point solutions including ticketing systems, SharePoint, wikis, shared folders, Word documents and individual scripting tools, to name a few. This patchwork of solutions lacks process consistency, workflow, and audit trails and relies heavily on an individual's skill level and focus. This approach is highly inefficient and does not scale effectively in comparison to automated incident response, which enables personnel to respond through a defined, completely tracked and auditable process. The effort to streamline the incident response process with automation has led to the development of "Human-Guided Automation" capabilities that are unique to Resolve's incident resolution platform.

At its essence, a Security Incident Response and Automation platform should automate and guide the user through the steps required to properly manage a security incident end-to-end. Key capabilities include:

- Ensure that security incidents are quickly diagnosed, tracked and acted upon, including taking protective measures and capturing the timeline of events, along with identifying and preserving evidence and artifacts, all in a secure and reliable manner.
- Ensure that the response to security incidents follows a consistent, repeatable process that can be executed quickly through a combination of automation, guided procedures and knowledge by more readily available, lower-cost resources, while increasing the productivity of more expensive and scarce expert resources.
- Orchestrate and execute cross-functional activities required to manage security incidents at the enterprise level using rules based procedures.

> Simply describing "what to do" to a security analyst is not sufficient. Automating many of the steps so the analyst does not have to do it manually provides value and drives adoption of incident response playbooks.

Traditionally, Incident Response platforms have focused on orchestration of human activity based on playbooks. This approach is inherently limited as most playbooks consist of rudimentary static documents or wiki pages, that provide instructions on how to handle a specific security incident and lack dynamic guidance and therefore do not allow the individual responding to the incident to apply knowledge and process consistently. Over time these static playbooks face the same fate as IT knowledge base articles; they become stale, unreliable and ultimately are ignored, thereby exacerbating a SOCs ability to properly respond. The more efficient and effective approach is Resolve Systems' "Human-Guided Automation"—the orchestration of human activity through playbooks AND automation, in combination with contextually relevant knowledge and guided procedures, which enables the user to quickly and reliably accelerate the threat response and resolution process.

The Resolve platform provides the best-in-class approach to Security Incident Response and Automation by enabling:

1. **Workflow orchestration** to coordinate the execution of activities within and across teams. The activities are necessarily linked with Resolve, supporting multiple assignments and effectively tracking response statuses every step of the way.
2. **Security-specific process guidance,** dynamically driven by the nature of the threat, which in turn provides detailed, repeatable response, replacing rudimentary playbooks and ad hoc responses with Human-Guided Automation.
3. **Automations that are embedded directly within the playbook** procedure itself, enabling security analysts to execute, examine and capture automation results directly into the Investigation Record. This eliminates the inefficiencies of manual processes and minimizes the "swivel chair" between tools, scripts, copy & pasting

of evidence, updating of tickets and a myriad of other menial, repeatable activities that accompany each incident response. Automations become a tool to aid in the process of threat incident response and an integral part of the threat resolution process.

4. **Abstracting lower-tiered operations personnel from the core systems and infrastructure** thereby enabling lower cost, more available resources to work incidents that are automatically classified to fit within their competency level and more importantly, when warranted by the threat evaluation data, to automatically escalate more complex incidents to more knowledgeable personnel. This automatically driven process is key to ensuring that all threats receive an immediate response in the most cost-effective manner.

Playbooks and Human-Guided Automation

Regardless of skill level, it is essential to have a well thought out and documented playbook that is regularly updated to ensure a consistent approach to security incident response. Security analysts often claim that security incidents are complex and that attackers are constantly adapting their approach and therefore playbooks cannot be sufficiently defined, let alone automated. It is true that certain incidents can be too complex to be handled by a full end-to-end automation; however, the vast majority of common security incidents can be clearly defined and the response can therefore be fully or semi-automated and managed by lower-skilled security personnel, enabled with Resolve.

Resolve's Incident Response and Automation platform tightly integrates automation with playbooks by leveraging our unique Human-Guided Automation to provide the process guidance necessary to maximize the productivity of security analysts at every tier and experience level. Resolve's incident response and automation platform can play a significant role in scaling even the most complex security operation.

Table 1: Common Security Tasks

Routine (Operational in Nature)	Non routine (Artisan in Nature)
Asset Inventory	Security architecture to protect assets
Data identification	Threat analysis
Vulnerability assessment and patch management	Policy creation based on risks/environment
Policy deployment (like firewall or antivirus rule changes)	Breach investigation
Virus identification and removal	
Ticketing and incident workflow	
User access rights changes	

Source: Gartner (September 2015)

> The playbook and automation provides the structure needed to achieve consistent results and avoid "cowboys" going off-roading due to overconfidence in their abilities.

Integration and Collaboration with IT Matters

Security teams cannot operate in silos. The effectiveness of SOC teams is largely determined by their ability to integrate and to collaborate with their IT counterparts. Having an incident response automation platform that clearly defines, orchestrates and tracks activities broadly across IT systems and processes is essential to achievement of this objective.

Whether data gathering for triage, blocking a phishing website, or moving a compromised server into an isolated VLAN, these activities can clearly benefit from automation that spans across security and IT operations. Whereas, previously, the security team would need to submit a request to the network team to block a bad website, an automation can be developed in conjunction with the network team and embedded directly within a Resolve playbook that eliminates this time consuming step, thereby reducing security incident response risk. More importantly, junior security analysts that may not have the necessary networking training or experience to independently respond to complex security incidents can be empowered by Resolve's Human-Guided Automation to accurately and reliably execute commands that previously required both security and IT experts.

Practical Considerations for Security Incident Response Automation

There are several key elements to take into consideration when planning a security incident response automation program. These include:

1. **Identifying Playbooks that will help SOC personnel respond and resolve security incidents:** Identify, understand and define how to respond to security incidents; particularly to repetitive incidents and/or repetitive parts of particular incidents in order to enable entry level security analysts or IT personnel.
2. **Leveraging automation wherever practical:** Automate as many steps of the playbook as possible. Automating the entire end-to-end process is not necessarily where the

untapped value resides; partial or semi-automation for individual steps of a larger playbook have been proven to provide tremendous value.

3. **Developing an "Adapt & Maintain" mentality**: Keeping the playbooks current with changes to environment, tools and incident response strategies is essential. Resolve enables the collaboration within and across necessary teams to drive content collaboration.

To get started, the SOC needs to identify which incidents merit the time needed to create playbooks and automation. A good way to qualify relative value is to examine ticket and event data to determine:

- What type of incidents occur most frequently?
    - How is a security incident identified and validated?
    - Can this incident be fully automated?
    - Can this incident benefit from Human-Guided Automation?
- How complex is the response to the security incident?
    - Is it something that could be addressed by lower-skilled analysts if proper process guidance and systems access issues could be properly managed?
    - Is this incident fairly deterministic and therefore does not require deep security expertise?

A valuable place to start is often in the area of event validation and investigation. Is this really a security incident? How can the available data be used to automatically enrich the case for a faster and more complete understanding of the true nature of the threat? What is the threat classification and therefore the response plan? Leveraging automation to drive validation and information gathering has been proven to enable security teams to respond faster, increase overall SOC productivity and reduce dangerous alert fatigue that comes with a large volume of repetitive tasks.

Investigation information gathering and assessment are commonly manual, time consuming activities. Resolve's Human-Guided Automation drives these tasks in an efficient manner. Resolve's playbooks are an easy to consume combination of automation, guided procedures and decision support tools that speed the security analysts through the various activities that must be performed to properly respond and contain the security incident, including the automated capture of key artifacts.

> "Automate whenever feasible… seek "automatability" - the capability of being automated as higher levels of confidence are achieved"
>
> **- Oliver Rochford, Gartner**

When planning for incident response automation, it is important to understand which incident types are best suited for full automation and which require a security analyst involved in the process. Based on the type and the risk profile of the event, an immediate automatic response, without any human intervention, may be required. Actions may include isolating systems, containment and taking additional steps to thwart additional damage from the attack.

On the other hand, there are incident types that require human intervention by a security analyst. For these incident types full automation may not be desired, but semi-automation or automation triggered and executed by the security analyst as a part of the overall response process (i.e., Human-Guided Automation) can provide substantial value by abstracting away complexities of underlying systems and the manual execution of actions, while still providing required control over the response process.

Resolve provides both full automation and Human-Guided Automation, along with the capabilities necessary to ensure that all automation tasks, whether machine or human driven, are fully tracked and auditable.

Lastly, incident-related communication and collaboration are important elements that should be captured along with the security incident investigation record. Unlike point collaboration tools, Resolve's platform integrates with instant messaging and mailing lists and can be configured so messages sent to a specific group or channel are automatically preserved along with the Investigation Record.

Activity	Benefits
Identify what incident types to automate	Analyze ticket and event history to determine which incident types will deliver value and build trust
Automate validation and information gathering	Look for opportunities to reduce unnecessary work
Incident Response orchestration	Streamline execution of complex and repetitive incidents. Clearly define responsibilities and interaction with IT teams
Containment and Remediation automation	Empower junior security analysts to take on more responsibility and increase the overall productivity of the team
IT workflow / process integration and collaboration	Avoid creating a security silo. Leverage existing IT teams, tools and processes.

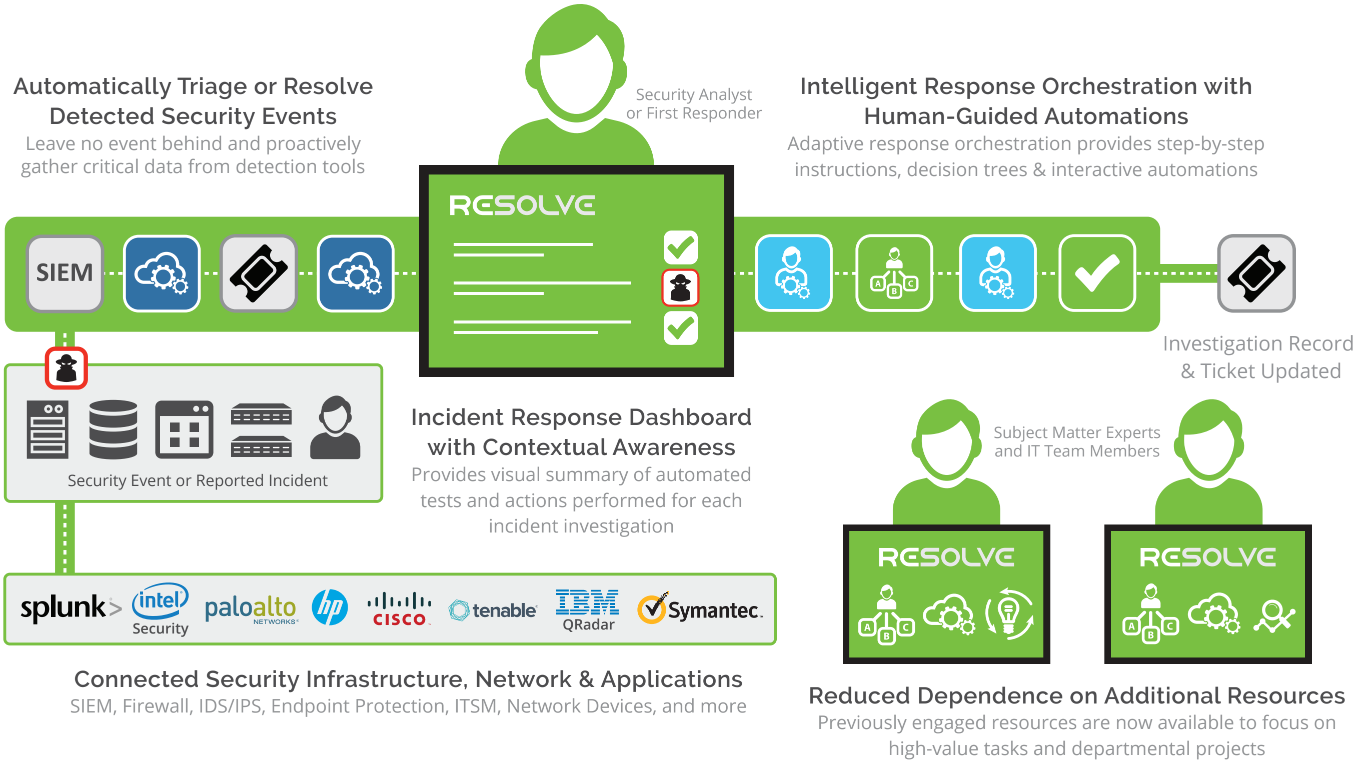
Resolve Capabilities Make It Easier

Resolve's Security Incident Response Automation platform is a unique, enterprise solution that drives process efficiency for both security and IT incident response with:

- Process workflow orchestration
- Playbook process guidance
- Human-guided and full automation
- Extensive library of pre-built playbooks and automations
- Broad Security and IT connectivity and integrations
- Visual drag-and-drop, no-code "Automation Builder"

Resolve enables security teams to:

- **Identify real and actionable alarms –** Resolve easily integrates via prebuilt connectors to your existing IT ecosystem to proactively and reactively run automations to assess, validate and resolve threats, thereby reducing time spent on false alarms and missing real threats
- **Rapidly isolate compromised systems –** Limit damage due to a security breach by leveraging validation and diagnostic automations that can shutdown applications or access.
- **Accelerate time-sensitive remediation processes –** Analyze and resolve security incidents with embedded automations as part of an interactive resolution guidance that provides step-by-step instructions via Human-Guided Automation, without direct access to underlying systems.
- **Leverage security experts' knowledge –** IT Security experts are valuable and expensive; scale by leveraging their knowledge by imbuing it into Human-Guided Automations and decision trees that enable lesser skilled resources.
- **Standardize response procedures –** Resolve enables full and Human-Guided Automation to be standardized and tracked. Automated logging enforces compliance and evidence preservation for each and every incident.



Automatically Triage or Resolve Detected Security Events

Leave no event behind and proactively gather critical data from detection tools

Security Analyst or First Responder

Intelligent Response Orchestration with Human-Guided Automations

Adaptive response orchestration provides step-by-step instructions, decision trees & interactive automations

Investigation Record & Ticket Updated

Incident Response Dashboard with Contextual Awareness

Provides visual summary of automated tests and actions performed for each incident investigation

Subject Matter Experts and IT Team Members

Connected Security Infrastructure, Network & Applications

SIEM, Firewall, IDS/IPS, Endpoint Protection, ITSM, Network Devices, and more

Reduced Dependence on Additional Resources

Previously engaged resources are now available to focus on high-value tasks and departmental projects

Features	Benefits
Process orchestration workflow	
Flexible workflow orchestration with multiple activity streams / assignments	Not all incidents are the same. Different incidents may require different activities, assignments and workflows.
Support for automated mapping of workflow templates for various incident response scenarios	As the number of playbooks and automations grow, it is important to be able to easily map SIEM and IT Incidents to security playbooks and allow the playbooks to be directly integrated into the SIEM and ticketing systems.
Active playbooks and collaboration	
Support for templated playbooks / process guidance that can be dynamically adapted to the specific incidents	Allow playbook templates to be flagged for updates and reviews or directly updated to more accurately represent the changing security and IT environments.

Features	Benefits
Active playbooks and collaboration	
"Active-Playbooks" – steps of the playbooks can be easily automated and embedded within the procedure to accelerate manual activities. Results are automatically captured in the incident.	Allows analysts to more efficiently execute the steps of the playbook through automation. Encourage and promotes the use of the playbook by analysts as they save the analyst's time/avoid waiting for IT to perform certain tasks.
Integration with instant messaging systems to automatically capture collaboration	Ensure valuable collaboration interactions are automatically captured.
Machine-assisted decision support	
Ability to enable lower-skilled support and security analysts to do initial validation and assessment through automation	Allowing the validation and data collection activities to be extended to entry-level analysts and IT support teams. The use of automated assessment allows inexperienced users to make the correct process decisions.
Easy-to-build automation without any development skills	
Flexible, extensible and programmable	Ensures that the automation platform can be extended to support custom environments, systems, integrations and use cases. Not limited to specific vendor APIs and content libraries.
Visual automation design and definition	Allows the automation to be developed visually like a process flow diagram. Automation tasks are based on intuitive configuration and visual data parsing. No coding required.
Scalable, reliable and secure	
Enterprise and carrier-class scalability and reliability	Scale from small pilots to extremely large global environments. Used in production by many global enterprises, communication service providers and MSPs
High availability, load balancing, clustering and site-to-site data redundancy	Built-in application clustering and load balancing. Support for geographic site-to-site redundancy
Secure and encrypted at rest and in-transit for evidence and artifacts	Ensure integrity of collected data and evidence
Broad set of integration to both Security and IT systems and infrastructure	
Network Security Infrastructure: Firewalls, IDS, IPS, Web Proxy, Secure Email Gateways, DLP, etc.	Broad integration with IT processes, systems, devices and tools
Endpoint Security: Anti-malware, HIDS, HIPS, endpoint encryption, DLP, etc.	Broad integration with Security processes, systems, devices and tools
SIEM, Threat Intelligence, and other intel sources	Integration with many event and incident sources
IT solutions: ITSM, CMDB, MOM, Directory Services, Systems Management, Patch Management, etc.	Integration with many IT services
Extensive library of Security and IT playbooks and automations	
Immediate time-to-value with pre-built playbooks and automations	Large library of security and IT content to provide immediate value

1216-04

About Resolve

Resolve Systems is a software company based out of Irvine, California with the most widely deployed Enterprise Security and IT Incident Response Automation platform. Resolve fundamentally reduces the amount of time that it takes organizations to investigate, respond to and resolve security and IT incidents and is used by many Fortune 500 enterprises, CSPs and MSPs / MSSPs to scale and accelerate their Security and IT operations productivity.

North American Headquarters
2302 Martin Street
Suite 225
Irvine, CA 92612
T: +1.949.325.0120

EMEA Headquarters
60 Cannon St
London EC4N 6NP
United Kingdom
T: +44 (20) 3743 2123