

Security Incident Response Reaches Beyond the SOC to Achieve Resolution

Security operations leaders have begun to realize the need for a scalable enterprise-wide approach to security incident response.

Security operations teams demand a platform to drive high-speed working partnerships with other technology teams (e.g., IT, network, service desk, etc.) via packaged, sharable knowledge and adaptive automation.

Contents

1-2

State of Security Operations

3

Technology-Fortified
Cross-Team Collaboration

4-6

Benefits of Enterprise-wide
Security Incident Response

6-8

Enterprise-wide
Orchestration in Action

8

Key Functionality

10

How Does Your SOC Stack Up?

11

References & About Us

Executive Summary

Current approaches to security incident response remain insufficient against the escalating volume and severity of security incidents. Organizations are beginning to discuss in earnest a question: *Can the security operations team continue to succeed with only informal, ad hoc support from other technical teams?*

Partnership between various operations teams such as security, IT, network, and service desk is critical for security incident response success, and an “enterprise-wide” incident response strategy benefits all involved teams, corporate leadership, and the broader organization.

Security incident response strategy requires enablement by technology, and this paper examines specific platform requirements. Major themes include interactive automated guidance (aka adaptive automation), data continuity, context preservation, shared toolkits, progress visibility, and reliability. This paper also explores the results achieved and an exemplar use case enabled by such a platform.

The State of Security Operations and Response

Businesses today experience security incidents at unprecedented rate and scale. The volume of data stolen by cybercriminals doubles year over year, and the cost of cyberattacks overall is increasing.¹ Deeply damaging attacks (in which >USD\$1M is lost per attack) constitute a growing proportion of all cyberattacks as well.² A security incident’s direct and indirect costs come from many sides. For example, attacks causing network downtime cost, on average, more than USD\$100,000 per down hour and, aside from a lack of availability, costs also stem from indirect factors such as legal liability, customer alienation, and violation of government regulations.³

Recent security incidents have caused affected businesses historic damage, and even threatened entire industry landscapes. For example, a recent malware attack cut FedEx's profits by USD\$300M *in a single quarter*.⁴ At greater scale, the ramifications of Equifax's massive breach of US consumers' personal data resulted in multiple C-suite forced removals and many federal and state-level hearings and investigations.⁵ The severity of the Equifax breach in particular may trigger new, restrictive legislation and even destabilize the US credit industry.⁶

Prevention-only strategies have proven insufficient, and as a result security teams have increased focus on incident response. In the wake of recent corporate security catastrophes, security incident response practices have gained media attention and public awareness. Yet current approaches to security incident response are ineffective against the escalating volume and severity of attacks.⁷ Many well known factors act against the security team in incident response, including:

- » The arms race nature of cybersecurity
- » Friction between finite staff and evergrowing incident volume⁸
- » Skills shortage
- » Crime-fighting administration due to the potential legal ramifications of an incident*

Equally important but less well publicized factors

SOC Slowdown Factor	Impact
Manual Processes	Manual processes slow incident detection and response as they scale poorly and are prone to human error. ⁹
Reliance on a Disparate Toolset	Security has limited effectiveness when the team depends on multiple independent point tools. Pivoting between platforms wastes staff bandwidth and valuable details fall into the cracks. ¹⁰
Lack of Visibility into Remediation Progress	Without appropriate visibility into response progress, the SOC has difficulty tracking security incident lifecycle and confirming identified security deficiencies have been remediated. ¹¹
Cross-team Incident Handling Challenges	<i>Collaboration difficulties between security, IT, and other technical groups choke incident response progress.</i> ¹²

All of the above hamper incident response speed and efficacy, increasing the risk of damage and slowing containment of significant breaches.¹³

These challenges have been difficult to address with products available to security teams today, as most vendors see security incident response and resolution as primarily a problem for the security operations team. Addressing the issues enumerated above, however, requires the participation of multiple technical teams across the entire enterprise; thus, security incident response must be examined enterprise-wide.

*These topics are explored further in [Security Incident Response Needs A Unified Platform](#). White paper. Resolve Systems, 2017.

The SOC Needs Technology-Fortified Cross-Team Collaboration

Many enterprise organizations are discussing an important question:

Can the security operations team succeed with only informal, ad hoc support from other technical teams?

Research indicates security leaders share a growing recognition of the need for cross-team response, and many industry-leading organizations have instituted a Cybersecurity Incident Response Team (CSIRT).¹⁴ CSIRTs demonstrate successful security incident response requires multiple technical teams to come together. It's worthwhile to explore why teams must assure these connections in security incident response. Once understood, it becomes clear how a product guaranteeing these collaborations creates immense value.

When responding to a security incident, security team members need to affect various systems to gather investigative data and/or take remediation actions. However, the security team often lacks authority over many internal systems; most belong to IT, network, and other technical owners. For example, IT operations teams must manage enterprise IT systems carefully, as even the smallest inadvertent change could have a *catastrophic* impact on business-critical applications.

How then can a security analyst interact safely with these systems?



Network



Servers & Workstations



Endpoint Protection



Firewall



Email



Operations teams share automation, orchestration, and knowledge in a unified incident response platform.

The analyst *must* partner with system administrators in the relevant/affected technical team during security incident response, however, the network and IT teams experience pressure to keep business-impacting applications and services available, which may be at odds with security incident remediation.¹⁵ Thus, the teams often find themselves at cross-purposes in the midst of a security incident. This further heightens the need for cross-team collaboration in incident response.¹⁶

Additionally, the service desk team can support security incident response via its engagement in both detection and remediation. It is often the first team to become aware of security incidents, both in obvious user-reported attack types (e.g., phishing) and in subtler user-side warning signs of significant breaches. For example, corrupted or deleted data, unexplained user account lockouts, and performance degradation from unusual usage or traffic suggests a deeper security incursion may be in progress.¹⁷ On the remediation side, service desk is in regular contact with end users and acts as a valuable channel to communicate essential security messages. In many businesses today, service desk is unable to investigate and diagnose these incidents to solve the issue independently. Much opportunity exists to let service desk teams drive solutions and work more closely with security teams.

Better Incident Response is Enterprise-wide

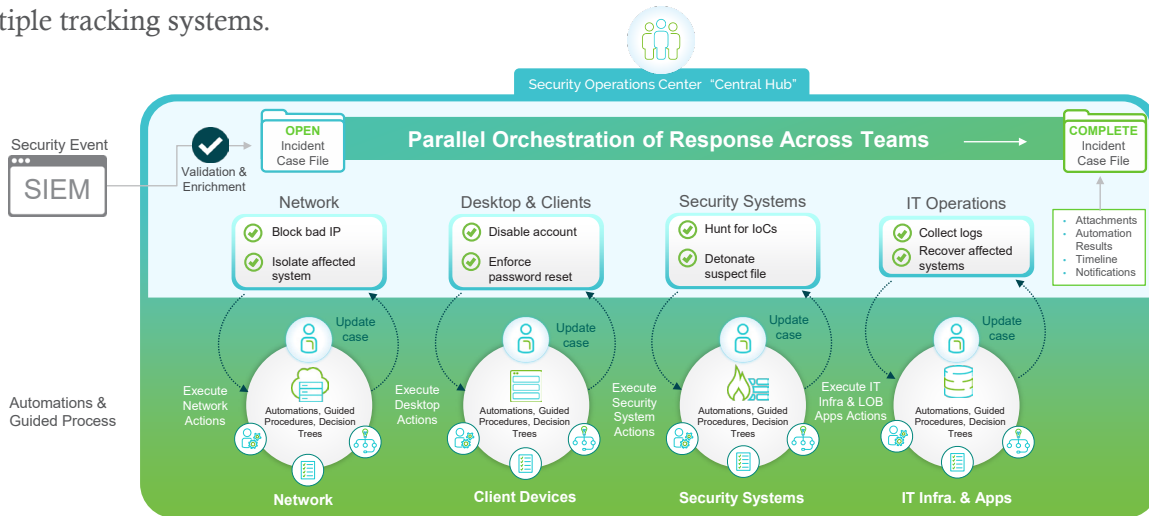
Based on these partnerships' importance in security incident response, it's crucial to look at how to realize them. The approach of empowering the security team to handle incidents by spearheading work across IT, network, service desk, and other technical teams is *"enterprise-wide" security incident response orchestration*.

Several critical components power enterprise-wide orchestration for security incident response: *A unified platform that works across teams and the automated processes underpinning it*. Even organizations with an existing CSIRT need this technology to scale successfully. To ensure streamlined task handoff and proper visibility, the platform must:

- » Help avoid remediation delays
- » Ensure prompt, correct remediation actions
- » Capture a continuous audit trail of all human and automation-driven activities
- » Manage the security incident no matter which team (security, IT, etc.) works on it

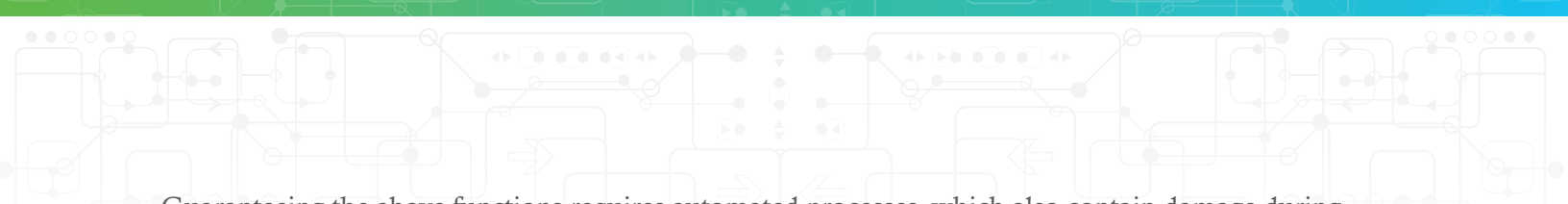
Empowering the security team to handle incidents by spearheading work across IT, network, service desk, and other technical teams is "enterprise-wide" security incident response orchestration.

To speed response, avoid information fragmentation, and create the audit trail forensics and compliance require, the platform must manage the security incident through its *entire* lifecycle, and thus *must support all technical teams involved in the response*. The platform must help avoid remediation delays by *preserving crucial incident context* for supporting technical teams and allow the SOC to share critical insights on the incident without the typical constraints and signal loss associated with transferring data manually across multiple tracking systems.



Synchronized cross-group response for security incidents

Assurance that supporting technical teams execute quick and correct remediation actions is possible only with a platform providing respective teams *prescriptive, context-specific procedures and guidance*. This is a *crucial* element, as incident response procedures are often non-obvious and known only to Subject Matter Experts (SMEs). However, IT, network, and service desk SMEs are rare and overloaded resources, so level 1 (L1) agents will most likely handle requested incident response actions. As L1 agents are less trained and less knowledgeable than SMEs, avoiding errors requires clear guidance without reliance on individual judgment.



Guaranteeing the above functions requires automated processes, which also contain damage during incident response, thereby reducing risk, and help frontline security analysts to do more without escalation. Automation is often called a “force multiplier,” as it maximizes scarce security staff’s focus on investigation versus menial and repetitive tasks. However, automation needs standards-based security incident response procedures to ensure optimal response and consistency.

Indeed, a true force multiplier would be greater than automation alone. It would also be a strategy that empowers frontline security analysts to do more without escalation.

Called “left shifting,” the power of SME-approved procedures and automations to lead frontline security analysts to correct actions and decisions increases the entire security team’s efficacy. Such a strategy benefits the security incident remediation work done by network, IT, and service desk teams as well. As an added benefit, giving these teams improved visibility and inclusion in security incident response processes fosters better understanding of cybersecurity, how it affects other teams’ responsibilities, and how it applies to their day-to-day work. A superior enterprise-wide security incident response platform also drives efficiencies across teams and enables further security operations empowerment over time.

A platform that:

- » Helps security and other technical teams share processes and tools creates multiplying efficiencies—greater speed and lower cost in incident response
- » Creates a path to package IT and network activities and approve security to execute them, and vice versa, builds unprecedented cross-team enablement. In addition, packaged automations can be pushed to frontline agents like service desk

It also extends reach to drive the highest-velocity incident response possible.

Gains from Enterprise-wide Security Incident Response Orchestration

The previous section examined how technology fortifies partnerships between security and the IT, network, and service desk teams. Also key to explore is how these technology-enabled partnerships benefit all involved groups, corporate leadership, and the entire organization.

An enterprise-wide approach to security incident response benefits the security operations team by offering faster response and reduced risk, as well as improved visibility, forensics, and compliance.

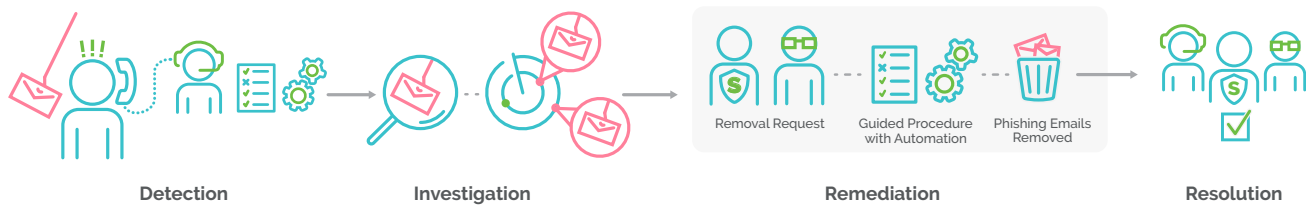
Accelerated response and remediation becomes possible when necessary **knowledge and automation get packaged and pushed closer to where the security incident is first detected.**

Once IT and network teams develop confidence with simpler use cases, they can package automations and procedures and give them to security to execute. So, for example, security can take approved actions on the network upon noticing an anomaly, without having to engage the network team. Automated actions maximize security and other technical staff’s effect by tackling basic tasks, allowing the team to focus on investigation and containment. With SME-approved guided procedures, frontline security analysts can do more without slowdown from escalation. Remediation activities outside the SOC happen faster because other technical teams share the same efficiencies and can access crucial incident context.

Security enjoys *reduced risk in response* with the help of automations and procedures designed to contain damage during incident response. Guided response procedures ensure other technical teams take prompt and correct remediative actions without inadvertently adding damage. Security also receives increased visibility into incident remediation progress with a continuous audit trail of all actions taken by both humans and automation, which the SOC can query on demand, resulting in improved forensics and compliance from complete evidence capture and activity recording.

The security team is far from the sole beneficiary of an enterprise-wide approach to security incident response orchestration, as significant gains exist for the network operations team, the IT operations team, the service desk team, corporate leadership, and the broader organization as well. Both the network and IT operations teams experience significant *time savings*, as well as *optimal network availability and maximum systems uptime*, respectively. The service desk team reaps time savings as well, and new problem-solving capabilities bring improved customer satisfaction and first-call resolution rates. Finally, leadership and the broader organization experience rewards like cost avoidance and reputation protection.

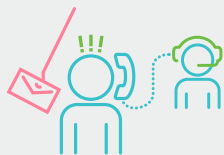
Enterprise-wide Security Incident Response Orchestration in Action



An example security incident illustrates the improved response delivered by an enterprise-wide approach. Consider the phish, a common attack type, sees investigation, remediation, and resolution with unprecedented speed, efficiency, and documentation via enterprise-wide orchestration technology. The benefits begin even at the point of detection: the service desk team.

Detection

An employee reports to service desk he received an unusual email prompting him to enter his corporate credentials into a strange-looking login portal, which then loaded a blank page. This employee has become a phishing email victim, and his corporate credentials have been compromised. With an enterprise-wide security incident response platform in place, the L1 service desk agent who receives the employee's report engages the platform and follows a guided procedure that helps identify the issue and walks the agent through issue-appropriate steps. The procedure zips the L1 agent to an approved IT automation that performs an immediate password reset for the employee, thereby preventing further damage (e.g., data exfiltration, malware introduction, etc.) to the employee's account and associated corporate systems. Finally, the procedure guides the L1 agent to create a new security incident in the enterprise-wide security incident response platform for the security operations team to investigate further.



Observations

The platform enabled the L1 service desk agent to accomplish "first call" issue resolution for the employee, and it's helped the agent take immediate incident containment steps.

Security Team Engages

A L1 security analyst receives the incident via the platform/service desk, complete with a log of all steps taken by the L1 service desk agent. The platform gives the L1 security analyst a guided procedure and IT-approved automation to quickly search the corporate mail servers for similar phishing emails sent to other employees. Finding several, the L1 security analyst assigns, through the same platform, email removals and spam filter updates to the IT operations team.



Observations

*The L1 security analyst has received the incident with full context from service desk, and the platform guided the agent to tackle **the most risk-critical incident response activities first** (i.e., completing full containment) as well as engage the required IT resources as soon as possible.*

Investigation

The guided procedure continues to lead the L1 security analyst to identify this particular phish as a credential harvester. The enterprise-wide security incident response platform provides adaptive automations to quickly find employees who have opened the message and clicked the malicious links. Discovering several compromised employees, the L1 security analyst receives another IT-approved automation to execute immediate password resets for the additional affected employees. As it does for all users, the platform automatically captures the L1 security analyst's notes and actions, as well as all relevant data on the affected employees and automations executed within the incident.



Observations

The L1 security analyst has quickly investigated the phish's full scope via adaptive automations and guided procedures. The enterprise-wide security incident response platform helped execute critical response actions without escalation or hand-off delay, thus preventing further damage to compromised entities.

Remediation

Meanwhile, the platform sends a L1 IT operations agent the L1 security analyst's request to remove the specified "phishing messages and update the spam filter. The request comes complete with a log of all steps taken by the L1 security analyst and the L1 service desk agent. The L1 IT operations agent is guided through procedures and uses the platform's adaptive automations to quickly find all instances of the phishing email on the mail server, remove them, and update the spam filter to screen out related phishing messages moving forward. Finally, the enterprise-wide security incident response platform guides the L1 IT operations agent to send all affected employees (those people for whom the L1 security analyst had reset credentials) a message with a templated explanation of the incident.



Observations

The L1 IT operations agent received the request with full context from both security and service desk, and avoids wasting time going back and forth between teams to understand steps already taken. The platform led him to best practice remediation and communication procedures, and adaptive automations accelerated his actions. The incident had the least possible impact on the IT operations team, as the L1 IT operations agent was only asked to do the least activity required by the team's specific ownership areas (i.e., deleting email messages, changing the spam filter, and communicating with employees about IT matters), and the enterprise-wide security incident response platform ensured seamless transitions without escalation. Indeed, **the incident has been fully remediated without requiring escalation within any involved team!**

Resolution

The incident is resolved when the L1 IT operations agent sends affected employees the templated message and closes the request, while the L1 security analyst receives notification from the platform that all required IT operations steps are complete. The security analyst checks the notes and actions taken by the other respective parties in the enterprise-wide platform's log, and can rest assured forensic and compliance experts will have all necessary incident documentation for post-hoc analysis. The L1 security analyst closes the incident, and the L1 service desk agent receives notification from the platform that the incident is fully remediated.



Observations

All incident stakeholders have maintained visibility into the incident resolution's progress without having to take proactive measures or update one another manually. The security operations team retained a complete audit trail of all incident activities, including actions executed by both the service desk and IT operations teams. The enterprise-wide security incident response platform enabled investigation, containment, and full remediation of the phish with unprecedented speed, efficiency, and visibility. The risk presented by the phish was minimized, while all engaged teams maintained optimal productivity.

Key Functionality to Power Enterprise-wide Orchestration of Security Incident Resolution

The superior results of an enterprise-wide orchestration approach to security incident resolution can be achieved only via technology offering specific, key functionality. A platform that can follow security incidents across all technical teams, from open to close, speeding response and preventing information fragmentation must offer:



Interactive Guidance



Data Continuity



Context Preservation



A Shareable Toolkit



Progress Visibility



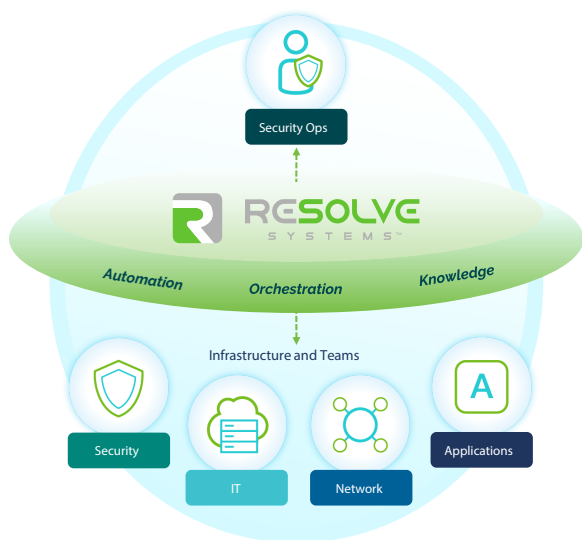
High Reliability

Only with these offerings can an organization create a new enterprise-wide approach to security incident response orchestration or enable a successful CSIRT strategy.

Speeding response and cutting remediation risk requires interactive guidance—prescriptive, context-specific procedures for all technical teams engaged in the incident response. This guidance reduces reliance on overloaded SMEs and integrates human-directed activities and decisions with machine automation. For example, automation can perform system validations at machine speed, saving significant time and ensuring an analyst or frontline agent enters a resolution procedure armed with required information. In addition, automation-enhanced procedures guarantee security analysts and frontline agents make correct decisions in complex technical scenarios, as such procedures summarize results in non-technical terms, while preserving a complete data set for security engineers.

Critical security functions such as preventing incomplete, scattered records and preserving crucial evidence depend on **data continuity**—the enterprise-wide security incident response platform’s ability to capture a continuous audit trail of actions taken by humans and automations in incident response. Capitalizing on its direct involvement in all incident response steps, the platform retains results of all activities, automations, and authorization requests, thus enabling security, legal, compliance, and forensics teams post-hoc. It also avoids unreliable cross-system data transfer methods, such as copy/paste to move information between ticketing and other incident response platforms. It can even note deviations for retrospective process improvement, training, and other automation opportunities.

Reducing delay in cross-team response and remediation activity is possible with **context preservation**, which provides supporting technical teams with instant access to critical insights from the SOC on the incident. The success of identifying, retaining, and sharing crucial incident details with teams outside the SOC is assured programmatically and no longer at the mercy of available ticketing fields or an individual’s writing skills and focus. The incident’s IT- or network-side recipient is no longer tasked with having to track down and interview the requesting security analyst to identify affected systems, incident criticality, or previous actions.



A **shareable toolkit** containing standardized, cross-team processes and automations drives response speed and efficiency. IT and network experts can package specific actions as adaptive automations and approve them for execution by security team members. Security experts can do the same for IT, network, and service desk teams. This approach extends the security team’s reach in both investigation and remediation.

Finally, **progress visibility**, which lets the SOC view the incident while it’s remediated by other technical teams, and platform **reliability**, which any operations-grade product should offer, round out a successful solution. Maintaining the SOC’s visibility throughout the incident response lifecycle allows the security team to give advisory support and added threat context proactively, should an incident

require difficult decisions in other teams. Reliability requires a platform with a scalable and redundant architecture, supporting the best deployment method for the specific organization served (e.g., on premise or SaaS) as well as demonstrating proven success in the most complex and largest global enterprises.



How Does Your SOC Stack Up?

Visionary SOCs across the world are laying the technology foundation for greater security empowerment and improved cross-team incident response. It's clear leaders see enterprise-wide security incident response orchestration as a growing priority, and many seek the right platform to serve this critical strategy. The preceding sections have examined the challenges, approaches, and technology requirements for success in enterprise-wide security incident response orchestration, and have also discussed the rewards following from adoption of an enterprise-wide security incident response platform.

Leading organizations today are setting a new bar in risk reduction and response speed thanks to enterprise-wide incident response technology and a forward-thinking approach.

Is your SOC ready to join today's top enterprise-wide security forces?

References

1. Leyden, John . "More data lost or stolen in first half of 2017 than the whole of last year." The Register® - Biting the hand that feeds IT. Situation Publishing, 20 Sept. 2017. Web. 12 Oct. 2017.
2. Chickowski, Ericka. The Impact of a Security Breach 2017. Rep. DARKReading Reports with Guidance Software, June 2017. Web. 9 Oct. 2017.
3. IBID
4. Kovacs, Eduard. "FedEx Profit Takes \$300 Million Hit After Malware Attack." Information Security News, IT Security News & Expert Insights: SecurityWeek.Com. Wired Business Media, 20 Sept. 2017. Web. 12 Oct. 2017.
5. United States. Cong. House. Energy and Commerce Committee. Hearing on Oversight of the Equifax Data Breach: Answers for Consumers Oct. 3, 2017. 115th Cong. 1st sess. Washington: GPO, 2017 (statement of Richard F. Smith, former CEO, Equifax).
6. Cox, Jeff. "Regulators to crack down on credit firms after Equifax hack, CFPB director says." CNBC, CNBC LLC, 27 Sept. 2017. Web. 16 Oct. 2017.
7. Oltsik, Jon. Cybersecurity Analytics and Operations in Transition. Rep. Enterprise Strategy Group, July 2017. Web. 05 Oct. 2017.
8. Monahan, David. InfoBrief: A Day in the Life of a Cyber Security Pro. Issue brief. Enterprise Management Associates, 17 May 2017. Web. 26 July 2017.
9. Oltsik, Cybersecurity Analytics
10. Oltsik, Jon. "Cybersecurity pros reveal what they think about their organizations." CSO Online. IDG Communications, Inc., 5 Sept. 2017. Web. 16 Oct. 2017.
11. Oltsik, Cybersecurity Analytics
12. Chuvakin, Anton, and Augusto Barros. How to Plan and Execute Modern Security Incident Response. Research Note. Gartner, 7 Apr. 2016. Web. 27 Sept. 2017.
13. The State of Malware Detection & Prevention. Rep. Ponemon Institute, LLC with Cyphort, Mar. 2016. Web. 12 Oct. 2017.
14. Oltsik, Cybersecurity Analytics
15. Chickowski, Ericka . "Bringing Network And Security Teams Together." Network Computing: Connecting the Infrastructure Community. UBM Tech, 16 July 2015. Web. 12 Oct. 2017.
16. Oltsik, Jon. "People, process and technology challenges with security operations." CSO Online. IDG Communications, Inc., 11 Apr. 2017. Web. 12 Oct. 2017.
17. Rance, Stuart. "5 Reasons the Service Desk Should Care About Information Security." SysAid Blog. SysAid, 8 Oct. 2015. Web. 12 Oct. 2017.

About Resolve Systems

Resolve Systems is the global leader in providing a single platform for enterprise-wide incident response, automation and process orchestration for Security Operations, IT Operations, Network Operations and service desk teams.

Resolve accelerates incident response and resolution by supplying engineers with partially or fully customized human-guided automations, powerful real-time incident collaboration and the omnipresence to orchestrate existing systems, across silos.

Headquartered in Irvine, California, USA with operations in EMEA and APAC, **Resolve Systems** works with nearly 100 of the largest global firms and is majority owned by funds affiliated with Insight Venture Partners, a leading global private equity and venture capital firm investing in high-growth technology and software companies

About Insight Venture Partners

Insight Venture Partners is a leading global venture capital and private equity firm investing in high-growth technology and software companies that are driving transformative change in their industries. Founded in 1995, Insight has raised more than \$13 billion and invested in nearly 300 companies worldwide. Our mission is to find, fund and work successfully with visionary executives, providing them with practical, hands-on growth expertise to foster long-term success.

For more information on Insight and all of its investments, visit www.insightpartners.com or follow us on [Twitter](#).



resolvesystems.com

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

EMEA Headquarters
60 Cannon St
Suite 119
London EC4N 6LY, UK
T: +44 (20) 37432123

Asia Pacific Headquarters
1 Fullerton Road
#02-01, One Fullerton
Singapore 049213
T: +65 6832 5513