IBM Resilient

Intelligent Orchestration

Battling Complex Cyberattacks with the Next Generation of Incident Response and Security Operations

Table of Contents

Abstract

Security leaders across all industries face mounting challenges. Cyberattacks are continually growing in volume, complexity, and sophistication, and incident response (IR) teams are pushed to the limit of their time, skill, and resources. Additionally, the average Security Operation Center (SOC) uses more than 75 different security tools – making full visibility nearly impossible and integrating those tools challenging as well.

This is why, in the last decade, security teams have sought new ways to optimize their ability to respond to and resolve incidents faster, more accurately, and more efficiently.

Recent research from Gartner[1] reveals its Security Operations and Response (SOAR) model as having three essential components: Security Orchestration and Automation, Security Incident Response Platforms, and Threat Intelligence Platforms. We believe the Intelligent Orchestration (IO) model is similar as it blends all three elements – incident response, intelligence (both human and machine-based), and orchestration and automation – to drive improved security operations and incident response.

The key in the IO model is that it is human-centered; the human sits in the center and is core to the strategic decision making. By combining human intelligence and machine-based intelligence, Intelligent Orchestration weaves together people, process, and technology seamlessly to drive down response times.

Figure 1. SOAR Types

ID: 325580

Source: Gartner (February 2018)

Evolution of Incident Response

Today, the next generation of incident response is emerging: Intelligent Orchestration. Intelligent Orchestration goes well beyond standard orchestration and automation efforts by combining machine intelligence – which includes threat intelligence, incident context, and artificial intelligence – with human context. This enables even faster and more accurate decision making. Intelligent orchestration combines this intelligence with an organization's knowledge and procedures, integrating across all of its SOC tools to deliver a guided response. "Guided response" enables the right analyst or executive to receive the right information at the right time. This focuses the response process and empowers security teams to outsmart, outpace, and outmaneuver cyberattacks.

In addition to guiding analysts through the response process, Intelligent Orchestration allows teams to enrich incidents with human and technological intelligence. As a result, analysts can punch well above their weight, slashing the time taken to upskill new recruits, and minimizing reliance on individuals.

Intelligent Orchestration provides documented, repeatable workflows that are infused with expertise from across the organization – including veteran security analysts and HR, legal, and marketing teams – and provides a foundation for continual improvement and maturity. Taking the time to consistently refine and codify the actions of your most experienced analysts — and find new opportunities to orchestrate and automate processes — can yield significant results. IBM Resilient customers have seen their median time to resolution drop from over an hour to just a few minutes.

This white paper will show security leaders how to plan, develop, and maintain an Intelligent Orchestration function within their organization, irrespective of their starting point. It will help educate and guide you as you assess new technologies and platforms on the bigger picture.

Overview

Preparing for and responding to cyberattacks is a top challenge to organizations of all types and sizes. When it comes to incident response, five major challenges have emerged:

The skills gap is widening – with no end in sight

The highly publicized cyber security skills gap has grown consistently wider over the past decade. In 2015, Frost & Sullivan predicted a skills gap of 1.5 million workers by 2022, but revised the estimate to 1.8 million workers in the most recent version of their Global Information Security Workforce Study .

The skills gap poses grave issues for any organization under increased pressure to ensure the security of sensitive data. Security budgets have crept up over the past decade, but as yet there has been no corresponding increase in the availability of human capital. A recent study by The Ponemon Institute also shows that response continues to be underfunded in relation to other areas in security. This reality is driving the need for a force multiplier technology to help analysts do more, work faster and more effectively.

The volume and sophistication of cyberattacks is skyrocketing

While organizations struggle to cope with current security demands, the threat landscape is far from static. According to the Ponemon Institute Cost of Malware Containment report, the average SOC logs almost 17,000 malware alerts in a typical week. As a result, a SOC could spend 21,000 hours each year chasing down false positives, at an estimated cost of $1.3 million.

At the same time any one of those alerts could cause substantial disruption to business operations. The damage caused by a successful cyberattack can take days or weeks to resolve, and the additional fallout of reputational damage, data leaks, and potential fines often lasts for months or years.

Security environments are more complex than ever

As organizations increasingly invest in cyber security and build out robust SOCs, the average number of security technologies an organization deploys has grown to a staggering 75 tools.

Managing and maintaining these tools is a burden. Gaining visibility across their SOC and into their effectiveness and value is difficult, and analysts need to constantly move between various tools during a response – taking up significant amounts of valuable time.

Analysts are overwhelmed, slowing median time to detection (MTTD) and resolution (MTTR)

To add to the challenges, the widening skills gap and rapidly increasing volume of threats is overwhelming security teams and, in some cases, contributing to employee burnout.

The average security analyst receives far more alerts per day than they can realistically cope with. As a result, time to resolution for security incidents is consistently poor across all industries and geographic locations.

Analysis of source data[6] from Verizon's 2017 Data Breach Investigations Report (DBIR) tells a bleak story. While median time to incident detection is quite low at four hours, median time to resolution is more than four calendar days. Threat actors have no such constraints — once an initial foothold has been obtained within a target network, time to compromise can typically be measured in minutes.

Data breach notification regulations are getting more complicated, and GDPR is going to change the requirements for incident response

Global, national, and local privacy breach requirements are more complex than ever before – and continually evolving. Privacy and legal teams can spend days working to meet regulatory obligations after an incident and still not be 100 percent confident they've fulfilled their requirements. As a result, privacy breach response today is lengthy, tedious, and expensive.

Perhaps the biggest challenge is the implementation of the European Union's General Data Protection Regulation (GDPR). The act brings new challenges for organizations dealing with personal data and information loss of EU citizens. It also creates many complexities around how an organization will be required to respond to a data breach. In particular, any organization globally that collects personal data from EU citizens – whether the company is based in the EU or not – will have 72 hours to notify authorities of a breach. Otherwise, the company risks being fined €20m or up to four percent of annual revenues.

The Intelligent, Next-Generation Response

While it is true that there are massive challenges finding cyber talent and managing a complicated SOC environment, new advancements offer tangible hope by arming teams with the technology and intelligence they require to triage, investigate, and resolve cyber threats in a faster and more efficient manner.

Intelligent Orchestration (IO) is a powerful security capability that uniquely addresses the challenges described above. By combining human and machine intelligence with orchestration and automation, IO dramatically accelerates and sharpens response to cyberattacks. By definition, it takes the complexity of incident response across people, process, and technologies and simplifies it making it accessible to organizations with a quick time to value.

IO is supported by an incident response platform (IRP), which provides security teams with a central hub to process, track, and resolve incidents. Powerful IRPs seamlessly integrate with security technologies such as SIEM and EDR, and enrich incidents using threat intelligence. The resulting benefits for security personnel can have a significant impact on time to detection and resolution.

Addressing Security Challenges with Intelligent Orchestration

Incident response is a highly complex part of SOC operations. At its best, it is a living process – proactive and reactive – involving dozens of both interlinked and disparate technologies, complex IT and business processes, and personnel from across the organization. With Intelligent Orchestration, organizations can empower their security teams to outsmart, outpace, and outmaneuver cyberattacks.

Outsmart cyber threats with the unique combination of human and artificial intelligence

Intelligent Orchestration combines artificial intelligence with human context, enabling faster and more accurate decision making. On the human side, Intelligent Orchestration unlocks and codifies the expertise of employees – such as veteran analysts and the HR, legal, and marketing teams – into IR processes. As a result, junior analysts can take the same steps as your expert staff.

Additionally, Intelligent Orchestration enables teams to integrate with third-party solutions to provide analysts with the information they need when they need it – enabling better decision making.

By providing expert-level processes and technological intelligence, Intelligent Orchestration enables "guided response." This ensures they have the right information at the right time.

> "Resilient's integration into Splunk has... enabled us to identify and fix process gaps, reducing response effort times from a matter of days to less than several hours on average."
>
> **Incident Response Manager,**
> Penn State Health & College of Medicine

Outpace cyberattacks through orchestration and automation across SOC tools

Intelligent Orchestration enables security teams to automate tasks where it makes the most sense in the response processes. For example, teams can automate repetitive and time-consuming triage and orchestrate enrichment tasks, allowing analysts to focus more on making critical decisions faster. And once the best course of action has been determined, Intelligent Orchestration allows analysts to quickly take the steps needed to close out incidents.

As a result, analysts can more quickly prioritize the increasing volume of alerts and attacks, accurately identify critical incidents, and take the right steps to fully and accurately investigate and stop the attack.

"With Resilient, our time to respond to an emerging threat went from 84 minutes to under 2 minutes."

Director of Cyber Security for a global pharmaceutical company

Outmaneuver cyberattackers with agile and adaptive Dynamic Playbooks and guided response

Security incidents rarely emerge fully formed. That means IR playbooks need to adapt as new details about an incident are uncovered. Dynamic Playbooks, a key component of Intelligent Orchestration, automatically adjust the IR playbook during the course of an investigation, ensuring that analysts are working with the most up-to-date information and processes.

Additionally, with orchestrated enrichment through integrated threat intelligence, SIEM, and EDR tools, analysts can rapidly discern an attacker's tactics, techniques, and procedures and take immediate action to combat it.

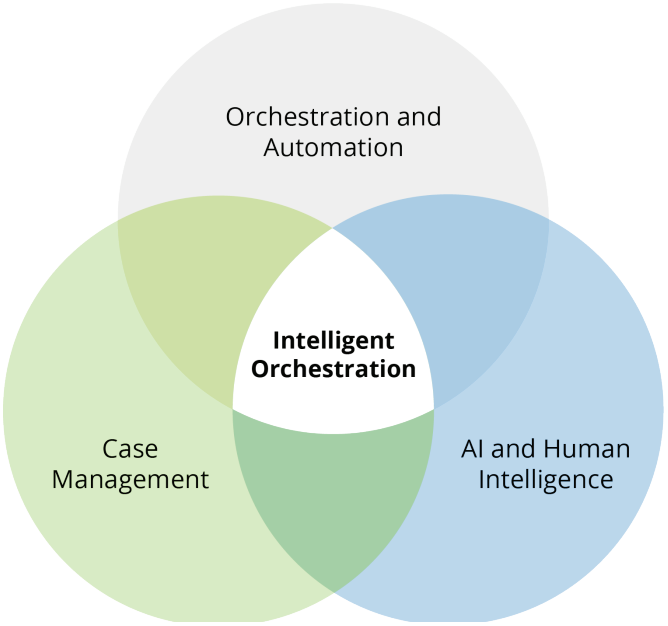
"Resilient's IRP was the only choice that was capable and customizable enough to help me build a modern incident response practice. Our mean time to discover, recovery, and closure dramatically improved using the Resilient IRP."

Head of Cyber Security Incident Response for a leading medical center and research facility

What is Intelligent Orchestration

As explained earlier, Intelligent Orchestration is the combination of human and technological intelligence. On the human front, Intelligent Orchestration distills the knowledge and experience of your most seasoned security personnel into an easily repeatable process. Technologically, Intelligent Orchestration transfers the burden of procedural "heavy lifting" to machines, providing intelligence to analysts and freeing time to focus on higher-value activities.

Put another way, the purpose of IO is to guide analysts through response workflows in fast and agile manner. And while technology and automation play a critical role in this endeavor, a strong groundwork of people and processes must be laid first.



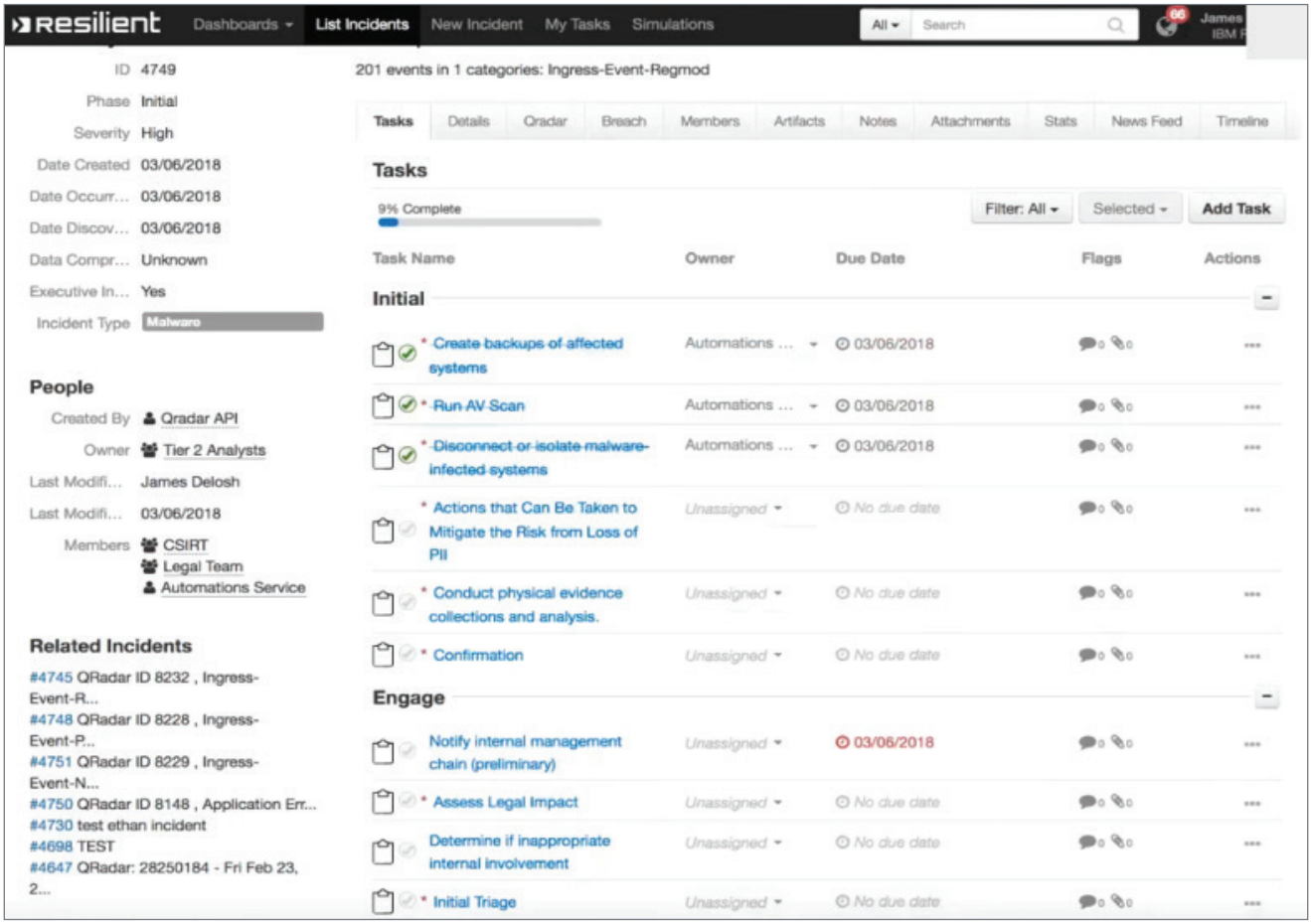
Intelligent Orchestration seamlessly blends three pillars of incident response management.

People ↦ Process ↦ Technology

People and Processes

The task here is to unlock tribal knowledge and refine and codify the practices of your most experienced security personnel into a set of solid, repeatable processes that can be followed by even the newest of recruits. This helps lessen organizations' reliance on individuals and the time needed to train new analysts – very important in the face of the skills challenge – and helps ensure that real-world practices become far more consistent. This is a business-first approach to IR – and has tremendous continuity benefits.

In the image below, taken from Resilient IRP, each stage of the response process for this ransomware attack have been clearly laid out for analysts to follow. In the planning stages, once this process has been codified and refined, analysts know precisely what action they should take at each stage in order to resolve the incident promptly and thoroughly.



Intelligent Orchestration guides analysts step-by-step through a proven and repeatable response process.

Responding to a ransomware attack — or any security incident — requires a series of distinct actions, some of which will be performed by IR personnel and others which must be passed to other teams. Some actions are good candidates for automation, while others will always require human intervention. The practice of designing and formalizing your IR processes will inevitably highlight these factors, putting you in a strong position to maximize the efficiency of your IR function.

Technology: Orchestrate First to Drive More Powerful, Human-Centric Automation

IR automation has a tremendous value proposition. By taking the burden of time-consuming and repetitive tasks away from human analysts, automation addresses all three of the top challenges discussed in section two. However, automation works best within the context of an Intelligent Orchestration strategy – because not everything can be automated. But once processes are in place, security teams should begin strategically employing automation to streamline critical steps and quickly get incident information to analysts.

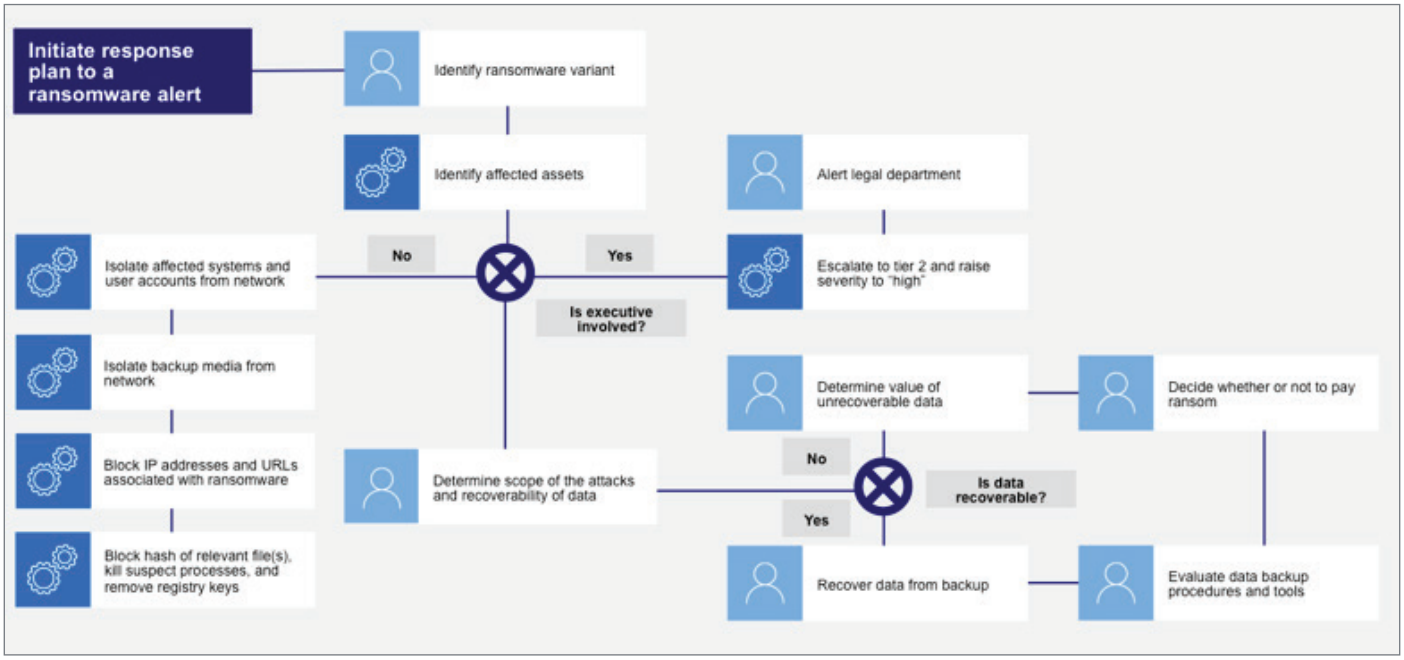
By integrating an IRP with existing technologies such as SIEM, EDR, ticketing systems, and other IT and security tools, a huge amount of purely administrative time can be saved — the full force of your technologies can be brought to bear without the need for constant screen switching and manual data transfer.

For example, one of the most time-consuming phases of incident response is triage, and threat intelligence tools can play a vital role here. The challenge, however, is that many security teams are forced to manually search for potentially malicious events, and then spend time searching through threat feeds to confirm their suspicions. This could take several minutes or more per event, wasting valuable time over the course of a day.

With Intelligent Orchestration, indicators of compromise (IOCs) or other artifacts are automatically delivered to an IRP via integrations with detective controls (such as SIEM or EDR) and integrated threat intelligence feeds are automatically deployed to enrich security incidents with vital context based on attached artifacts. This saves a significant amount of time for security personnel, who no longer need to manually access threat feeds, while also cutting out the potential for human error.

To start to identify suitable tasks for automation, look for simple, repetitive tasks such as incident triage, updating firewall or filter rules, and banning malicious hashes. Playbooks will be punctuated with human decision points, and automation should be used to progress response efforts up to and following these points.

Consider the diagram below — a simple process for responding to ransomware attacks:



Intelligent Orchestration features Dynamic Playbooks, which adjust response plans in real time as information about the incident is uncovered.

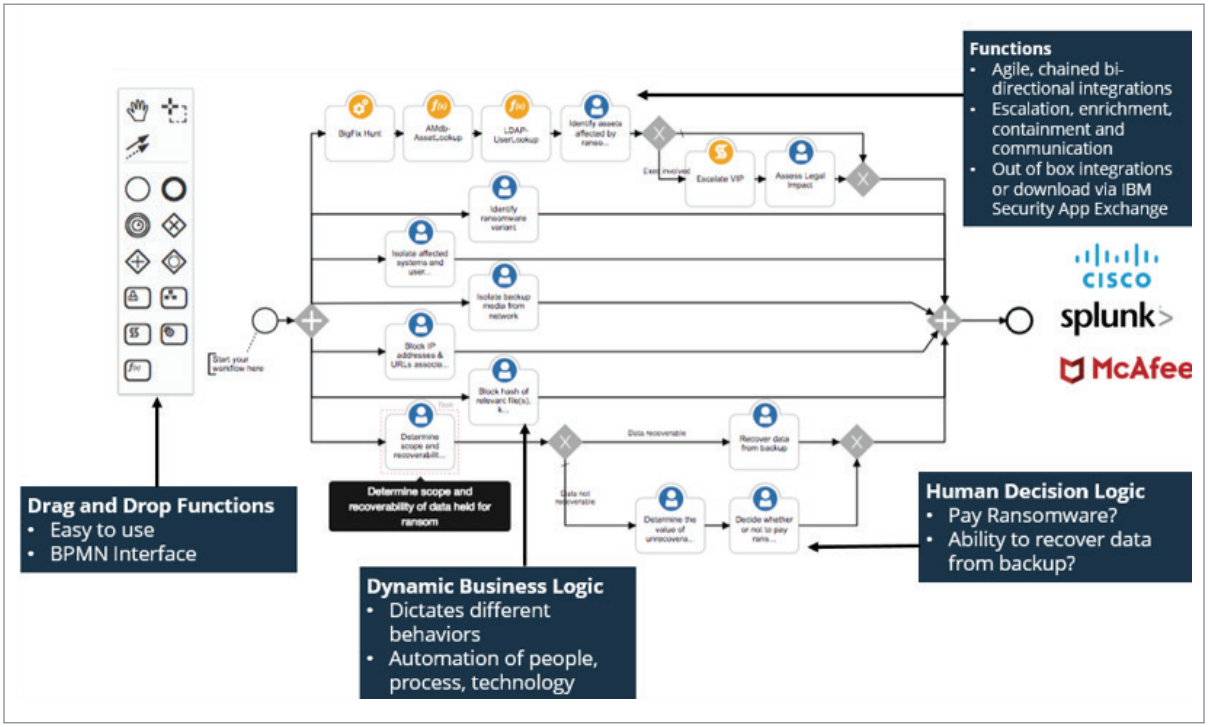
Certain tasks, such as identifying malware variants and determining the scope of an attack, require heavy input from human analysts. Technology can accelerate these processes and provide input but relying exclusively on automation in these areas would be extremely risky. On the other hand, tasks that result from those human decision points can often be automated based on the decisions made . Once a malware variant has been identified, banning associated hashes and blocking IP addresses can be performed automatically with the click of a button.

Technology in Intelligent Orchestration should guide human analysts through the process of responding to an incident, taking care of those aspects of the process that don't require human input, and providing the information and context necessary for critical decision making.

Accelerated Integrations and Automation with Intelligent Orchestration

With Intelligent Orchestration, the process of creating and maintaining integrations and automated playbooks is highly simplified, as an IRP with Intelligent Orchestration enables teams to build and manage playbooks and integrations without coding and scripting.

That is because Intelligent Orchestration relies on enterprise-grade integrations that can be applied and reused across multiple playbooks. Security teams can design these playbooks with a simple drag-and-drop interface based on industry-standard business process management notation (BPMN). Additionally, Intelligent Orchestration features the componentized ability to string functions together in a nested/modular fashion. In this way, organizations can define components once but piece them together as needed. For example, if a team needs to update its malware process based on new tools and/or improved standard operating procedures, it can simply update the malware workflow. All workflows that call on it (e.g. ransomware) will call on the new version.



With Intelligent Orchestration, security teams can quickly and easily build robust IR workflows that combine people, processes, and integrations with a visual drag-and-drop editor.

With this simple yet powerful interface, security teams can quickly build robust IR processes that seamlessly blend human tasks and decision making with technological integrations and automations. These powerful and complex workflows are known as Dynamic Playbooks.

Dynamic Playbooks

With Intelligent Orchestration, people, processes, and technologies can be codified into playbooks that dynamically adapt within a powerful IRP. These "Dynamic Playbooks" guide security analysts through the process of resolving incidents, tracking progress, and facilitating the assignment of tasks to teams or individuals throughout the organization.

Dynamic Playbooks standardize the response process by ensuring incidents are responded to uniformly, based on codified actions, so that each response is handled as if it were prescribed by your most experienced analysts. Dynamic Playbooks also adapt in real time, adding, removing, or editing steps in the IR process as the attack changes or details about the incident are uncovered through enrichment activities.

For example, if, during the investigation of a malware outbreak, it is determined that an executive's laptop is infected, it changes the nature of the response The incident should be escalated to a higher priority, and the legal team may need to be notified that sensitive information is at risk. With Dynamic Playbooks, these steps are automatically added to the response playbook in real time, ensuring that the analyst can deliver a complete, expert-level resolution to the incident. In this way, Dynamic Playbooks enable "guided response," leading analysts to a fast and efficient resolution.

Benefits of Intelligent Orchestration in Practice

To understand how Intelligent Orchestration works in a real security environment, consider a simple use case.

First, your EDR identifies a suspect process, which is attempting to connect to an external server. To investigate this incident manually, the analyst would need to:

- Write and run a SIEM query, pulling all relevant events into a .csv file
- Identify an MD5 hash for the suspect process and research it in the appropriate threat intelligence feeds
- If the process is confirmed as malicious, create a backup of the endpoint, isolate it from the rest of the network, and run an AV scan
- Update the incident record, attaching all relevant log files, notes, etc.

This process could take an analyst 30 minutes – and potentially much longer. With Intelligent Orchestration, many of the steps in this process would be streamlined, and the analyst would quickly be armed with the insight they need to fully resolve the incident.

- EDR identifies a suspect process, and automatically generates an incident in the IRP
- SIEM is automatically queried, and relevant information is appended to the incident
- IOCs from the incident are compared with threat feeds and confirmed as malicious
- Based on this intelligence, the incident is labeled a malware attack, and the relevant Dynamic Playbook is applied
- Standard processes start automatically: Creating backups, isolating endpoints, and running AV scans
- An audit trail of all steps is kept automatically

If the analyst needs to perform additional queries or take further action, they can do so without ever needing to switch windows, keep manual records, or perform cumbersome manual tasks. This alone could save 15-30 minutes per incident.

> "The key enabler for CISOs... is to get visibility across their security infrastructure to make better decisions during security incidents. This visibility will enable them to have a more strategic and risk-based conversation with their board of directors, CFO and CEO about the direction of their security program."
>
> **Lawrence Pingree, Research VP at Gartner[7]**

Use Case: Reducing Average Response Time by More than 97 Percent

Global pharmaceutical organization slashes time to resolution from 84 minutes to under 2 minutes with Intelligent Orchestration

The Challenge

A market-leading global pharmaceutical organization approached IBM Resilient with a problem: It had four security teams spread across the globe, each using their own processes and technologies, battling a combined 5,000 incidents per year. The organization lacked a centralized platform for incident response, and key decision makers struggled to stay abreast of emerging threats.

"Collaboration, communication, and record-keeping was difficult. None of [the teams' technologies] communicated with each other, and collaborating meant documenting actions in three different systems, which was three times the work," said the organization's senior manager of global information security.

One situation in particular brought things to a head: A privacy incident occurred and was responded to simultaneously by all four security teams. Each team reached its own conclusion and made a different suggestion. Ultimately, lacking proper communication, the IT team was instructed to delete the data which only exacerbated the situation and necessitated additional work to recover the files.

All told, the organization faced three major challenges:

1) High incident volume — more than 5,000 per year

2) Disjointed and inconsistent response teams/ processes

3) Lack of communication, visibility, and audit trail

The Solution

In order to address these challenges, it was clear the disparate security teams would need to be brought into alignment, along with their technologies and processes. An Intelligent Orchestration approach to the problem would empower the teams to quickly take action on new incidents, eliminate confusion and miscommunication, and facilitate a collaborative, consistent approach to IR and related documentation.

"For us, orchestration was a way to stay coordinated even as we got faster and more agile," explained the senior manager. "We sought to ensure that every detail, from roles and responsibilities to how data was recorded, was standardized and understood by all," said the security professional.

Resilient IRP was deployed as the central hub for IR across the organization. Using Resilient IRP, the organization was able to:

- Coordinate response activities in a central location, with an automatically generated audit trail and total visibility for analysts and executives
- Develop and codify standardized IR processes, enabling security teams to work together and respond to incidents powerfully and consistently
- Eliminate duplication of effort by assigning tasks to individuals and teams across the organization
- Integrate existing security technologies into the response process while automating repetitive, time consuming, and manual tasks

"[With Resilient IRP] our team works together as a well-oiled machine, with less confusion and less time wasted," said the senior manager. *"When we respond to an incident, 60 percent of analyst actions can be completed through Resilient. We no longer need to waste time going to five or six other tools."*

The Results

With Resilient IRP in place, the organization noticed substantial improvements in collaboration between security teams. Visibility into the response process was greatly improved, while new and junior analysts quickly grasped what was required of them as they up-skilled.

Via two-way integration with over a dozen security technologies, analysts had access to almost everything they required without needing to switch windows or complete manual transfers. Resilient IRP also enabled the organization to run IR simulations across all four teams, allowing them to practice resolving incidents that had previously caused issues.

"For our long-term commitment to better IR, Resilient was the right tool for us," said the senior manager. "With this platform, we're able to train our staff and practice workflows with tabletop exercises. As a result, all four of our security teams are performing effectively together."

Ultimately, the most obvious benefit came to the fore: Time savings. The combination of improved processes, seamless integrations, and automation enabled the organization to slash time taken to resolve common incidents. The organization's senior manager of global information security concluded:

"With Resilient, our time to respond to an emerging threat fell from 84 minutes to under two minutes."

Summary

To help security teams battle today's top security challenges, Intelligent Orchestration provides a game-changing platform for transforming incident response – and empowering teams to outsmart, outpace, and outmaneuver cyberattacks.

Intelligent Orchestration provides:

- Guided Response That Delivers the Right Information to the Right People at the Right Time
- The Speed of Artificial Intelligence Combined with Human Decision Making and Context
- Instant Visibility Across the SOC
- Faster Time to Value Through
- Agile, Re-Usable Playbook Components

A Buyer's Guide to Intelligent Orchestration Platforms

The incident response platform industry has continued to mature, with many vendors offering solutions across an increasingly varied range of automation and case management capabilities. While many offer tools that help with specific areas within incident response, few offer the full combination of case management, orchestration and automation, and intelligence.

When assessing vendors, here are nine questions you can ask to ensure you're investing money wisely:

1. Does the platform facilitate development of people and processes?

The orchestration of people and processes are essential to successful IR. Functionality such as Dynamic Playbooks and visual process mapping will help you refine IR processes and develop the skills of your analysts.

2. Does it enable automation to enable faster and more efficient incident response?

Analyst overwhelm is a huge challenge in the security world, and nowhere is it felt more keenly than in IR. A powerful Intelligent Orchestration platform should reduce the burden of repetitive tasks and window switching via integrations and automation. Additionally, it should guide junior personnel through your IR processes, and empower them to take on responsibilities beyond what they could cope with alone.

3. Does it provide a system for tracking and measuring the efficacy of your IR program?

Reporting and analytics are essential to a healthy security function — they provide evidence of ROI, highlight areas for improvement, and inform risk management strategies. An Intelligent Orchestration platform should provide instant access to a wide range of reporting options at a granular level, including comprehensive pre-set templates and the option to create your own.

4. Is there a rules-based system for escalation to the legal, HR, marketing, or executive teams if an incident warrants their involvement?

Some incident types warrant the immediate involvement of legal or senior executives. When these incidents are identified, the platform should automatically inform these parties, and provide them with a detailed account of the incident without delay.

5. Does it integrate with existing security and IT tools?

To maximize value for the IR function, an Intelligent Orchestration platform must fit into the "orchestration ecosystem," which could include a variety of third party and community-built applications.

As an example, one of the biggest challenges for IR analysts is the need to constantly switch between and transfer data between security technologies. An Intelligent Orchestration platform that integrates fully with your orchestration ecosystem can alleviate this issue and enable analysts to focus their time and energy on strategic activities.

As a starting point, the platform should integrate with common security tools such as EDR and SIEM. Beyond this, you should consider the specific needs of your IR function, and procure a platform that will integrate with all of your existing security technologies without the need for substantial development.

6. Does it enable teams to build IR workflows that combine human tasks, integrations, and automation?

IR processes should be constantly evolving and improving. An Intelligent Orchestration platform should facilitate this process by enabling individual tasks to be automated or allocated to relevant personnel.

7. Does it utilize relevant, contextualized threat intelligence?

Threat intelligence is a huge boon for IR, where it helps analysts prioritize the most urgent incidents and provides insight into the best ways to combat different types of threat. An Intelligent Orchestration platform should ingest TI directly and use it to automatically enrich incidents, saving analysts the time it would take to manually parse threat feeds.

8. Can it be updated or customized quickly and easily?

As mentioned earlier, continual improvement is key to long-term incident response success. An IRP that can be administrated by the security team and updated as your IR program evolves can go a long away in ensuring that these improvements are captured. This includes updating

roles, responsibilities, and owners, IR playbooks, reporting dashboards, and automated workflows.

9. Does it facilitate cross-organizational collaboration?

IR is not a closed loop. Not only is it beneficial to work alongside other parts of the organization, such as legal, HR, and marketing, it's also often necessary to pass incidents back and forth between IR and the IT helpdesk. Integration with helpdesk software is highly valuable for this reason.

10. Does the platform include privacy regulations and data breach notification workflows?

Data breach notification regulations are continually evolving globally, making tracking and complying with them more complex than ever before. Privacy and legal teams can spend days working to meet regulatory obligations after an incident and still not be 100 percent confident they've fulfilled their requirements. And with the arrival of the EU General Data Protection Regulation (GDPR), the stakes and complexities are greater than ever.

An IRP can take the complexity out of fulfilling data breach notification requirements by providing response plans that instantly map to the latest regulations, as well as automated notification of new regulations, providing context of an organization's ongoing regulatory status.

11. Does the vendor offer value as a business partner? Do they have a strong track record?

The IR software market is still relatively young, and it pays to do your homework on potential vendors before making your decision. If you're considering a vendor, try to speak with some of their clients before moving forward to avoid unpleasant surprises.

Register for a demonstration of the Resilient IRP to learn how Intelligent Orchestration from IBM Resilient can help your organization outsmart, outpace, and outmaneuver cyberattacks.

Orchestrate your response and empower your security team to act faster and more intelligently.

Schedule your demonstration of the Resilient Incident Response Platform today at:
http://info.resilientsystems.com/incident-response-platform-schedule-a-demo

---

Sources

1 "Preparing Your Security Operations for Orchestration and Automation Tools." – Gartner Research, Feb. 2018

2 "Global Information Security Workforce Study - Center for Cyber Safety ...." https://iamcybersafe.org/gisws/. Accessed 8 Mar. 2018.

3 "IT budget research 2018: Funding and spending ... - Tech Pro Research." http://www.techproresearch.com/downloads/2018-it-budgets/. Accessed 8 Mar. 2018.

4 "The Third Annual Study on the Cyber Resilient Organization" – Ponemon Institute, March 2018

5 "The Cost of Malware Containment - Ponemon Institute." 26 Jan. 2015, https://www.ponemon.org/blog/the-cost-of-malware-containment. Accessed 27 Mar. 2018.

6 "Incident discovery and containment: Average is over. | Verizon Insights ...." 21 Jul. 2017, http://www.verizonenterprise.com/verizon-insights-lab/VES/incident-discovery-and-containment-average-is-over-. Accessed 8 Mar. 2018.

7 "Gartner Press Release, Gartner Says Detection and Response is Top Security Priority for Organizations in 2017" 14 Mar. 2017, https://www.gartner.com/newsroom/id/3638017. Accessed 12 Mar. 2018.

ABOUT IBM RESILIENT

IBM Resilient is the industry's leader in helping organizations thrive in the face of any cyberattack or business crisis. IBM Resilient's proven Incident Response Platform (IRP) empowers security teams to analyze, respond to, and mitigate incidents faster, more intelligently, and more efficiently. The Resilient IRP is the industry's only platform with Intelligent Orchestration, enabling teams to integrate and automate people, processes, and technologies in a single, open incident response hub. With Resilient, security teams can have best-in-class response capabilities. IBM Resilient has 300 global customers, including 60 of the Fortune 500, and hundreds of partners globally. Learn more at www.resilientsystems.com.