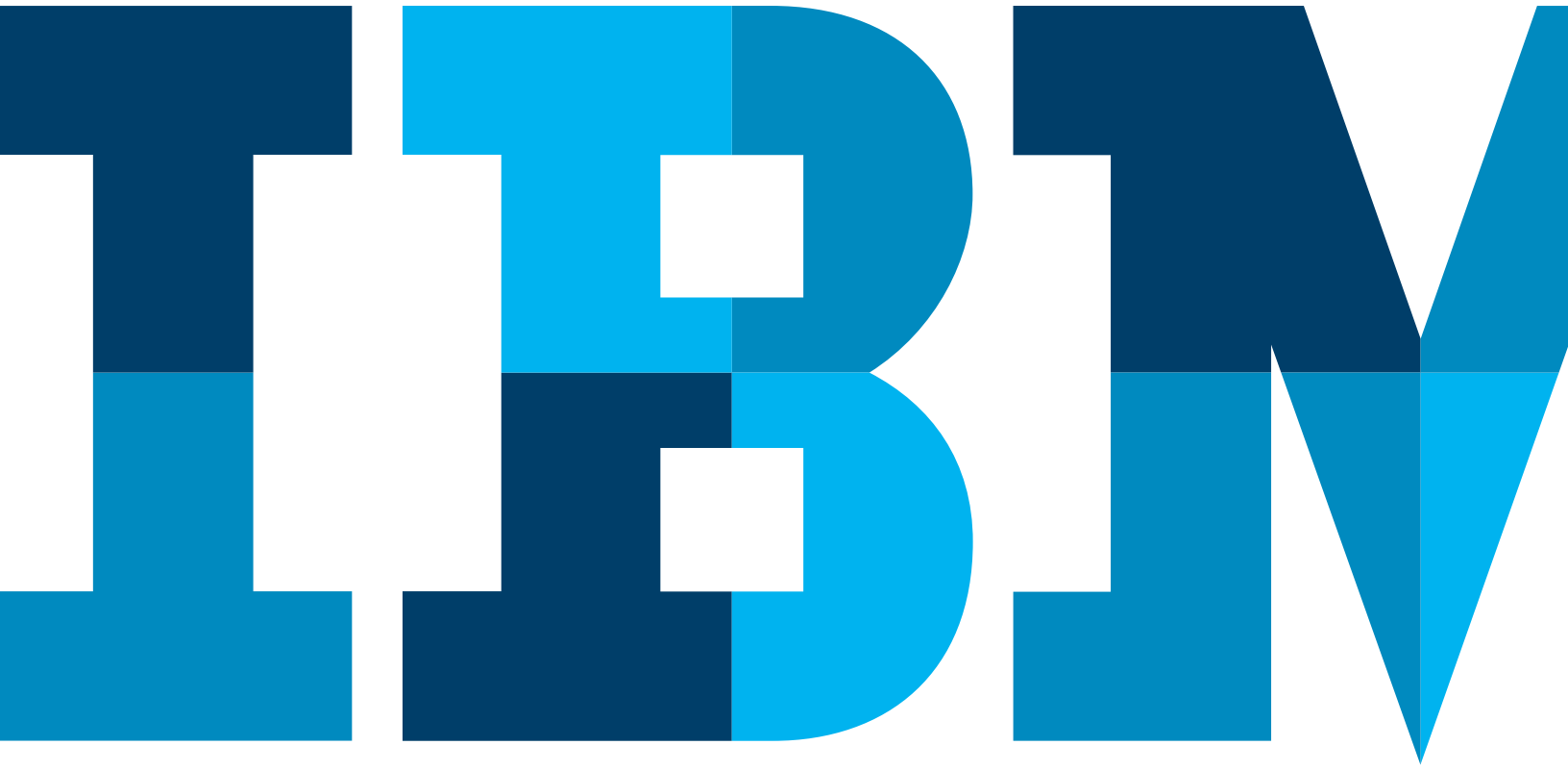
**IBM Security**
White paper

# Six steps for building a robust incident response function

*The incident response challenge*



IBM

## Contents



## Introduction: This is the decade of incident response

Organizations globally realize that working only to prevent and detect cyberattacks will not protect them against cyber security threats. That is why IBM Resilient® was developed: to arm security teams with a platform for managing, coordinating, and streamlining incident response (IR) processes.

IBM Security has had the privilege of working with organizations of all sizes and across all industries as they implement Resilient solutions to develop more sophisticated and robust incident response functions. These organizations build IR processes that are consistent, repeatable, and measurable, rather than ad hoc. They make communication, coordination, and collaboration an organization-wide priority. They leverage technology that empowers the response team to do their job faster and more accurately.

To go beyond the content in this white paper and learn more about how IBM Resilient can empower your security teams, please visit: https://www.ibm.com/security/intelligent-orchestration/resilient.

But there are challenges to building and managing a more robust IR program. Three challenges in particular stand out:

1. **The volume of cyber security incidents is increasing**
   Forty-two percent of cyber security professionals say their organization ignores a significant number of security alerts because they can't keep up with the volume, according to Enterprise Strategy Group[1].
2. **Security teams are struggling to fill open positions**
   200,000 cyber security jobs remain unfilled across the industry as of 2016, according to CyberSeek[2].
3. **Organizations are too complex and underprepared for effective response**
   Insufficient planning and preparedness and complexity of IT and business processes are the top barriers to responding to cyberattacks[3].

To solve these challenges, many IBM Resilient customers are striving to align their people, process, and technology so that IR analysts understand who is responsible for which tasks, when tasks need to be done, and how to do them. This emerging concept is known as incident response orchestration.

Incident response orchestration empowers security analysts by putting IR processes and tools right at their fingertips. They can access important incident information in an instant, make accurate decisions, and take decisive action. It leverages automation to increase the productivity of security analysts and technologies—alleviating the skills gap and the volume of alerts.

But IR orchestration is a process, not a product. It requires strong foundational blocks—trained people, proven processes, and integrated technologies. Orchestration is built on these core elements, and the effectiveness of an organization's orchestration efforts lies entirely on the quality of these fundamental pieces.

## Mapping your IR maturity

Over the years, IBM Resilient customers have increased their IR sophistication at various levels across a spectrum of maturity. Maturity levels are often necessitated by industry, available resources, or experience, but most IBM Resilient customers continually look to evolve their IR function into a more advanced phase.

With the help of these customers, IBM Security's Resilient team has developed an incident response maturity model.

This model maps the journey from an ad hoc and insufficient incident response function to one that is fully coordinated, integrated, and primed for continuous improvement and optimization.

The road to orchestrated incident response starts with developing people, process, and technology. That is the purpose of this guide: to show you the primary key steps in the process of building a robust IR function.

| **Maturity level** | | **Ad hoc** | | **Maturing** | | **Strategic** |
|---|---|---|---|---|---|---|
| **Existing capabilities** | | **As needed** | **Dedicated part-time** | **Full-time** | **SOC/IR+** | **Fusion** |
| | **People** | • 0–1 | • 1–3<br>• specialization | • 2–5<br>• Formal roles | • ~10<br>• Shifts (possible 24x7) | • 15+<br>• Intel, SOC, and IR teams |
| | **Process** | • Chaotic and relying on individual heroics reactive<br>• General purpose run book<br>• Tribal knowledge | • Situational run books; some consistency<br>• Email-based processes | • Requirements and workflows documented as standard business process<br>• Some improvement over time | • Process is measured via metrics<br>• Minimal threat sharing<br>• Shift turnover<br>• SLAs | • Processes are constantly improved and optimized<br>• Broad threat sharing<br>• Hunt teams |
| | **Technology** | | • SIEM<br>• Sandboxing | • Continuous monitoring<br>• Endpoint forensics<br>• Tactical intelligence | • Malware analysis<br>• Additional intelligence<br>• IT operations | • Intel+IR drives security program<br>• Strategic intelligence<br>• Coordination with physical security |
| **CMM equivalent** | | **Initial** | **Repeatable** | **Defined** | **Managed** | **Optimized** |

*Table 1*: Incident Response Maturity Model

## Step 1: Understand threats, both external and internal

Every organization faces a unique threat landscape, and the first step in building out your incident response function is to develop a detailed understanding of this landscape.

Part of your threat landscape is the nature of the cyberattacks your organization will contend with. That may include specific threats that your organization has addressed in the past (for example, malware infections or phishing attacks), as well as threats that are known to affect your industry broadly (such as ransomware attacks on healthcare organizations, or DDoS attacks on internet infrastructure companies).

Additionally, a robust threat model should consider all possible actors and incidents. For example, a recent survey of a dozen healthcare organizations found that many struggle with an "inadequate threat model" and focus "almost exclusively on the protection of patient health records."[4] The survey found that rather than developing a holistic view of their IT environment and possible threats, staff at healthcare organizations rarely venture beyond the narrow focus of regulations like the US HIPAA law. More serious threats that didn't directly affect patient health information—such as ransomware that targets healthcare devices—lurked in organizational blind spots.

The spectrum of possible cyber incidents your organization may face is broad, and each will warrant its own IR process. To get started, among the questions you might ask are

- What kinds of attacks or adverse incidents has our organization experienced in the past?
- Have we sustained a malware infection in the recent past? If so, what kind of malware (botnet, theft of data, ransom)? When and for how long did the incident last and how was it resolved?
- Have our employees been the victims of targeted phishing email scams designed to steal employee credentials? If so, which employees?
- Has our organization been the subject of criticism in popular online forums or by *hacktivist* groups or other online personalities?
- Has our organization been specifically targeted by a denial-of-service attack or other form of intentional online disruption?

In attempting to understand the threats facing your organization, consider what types of attacks your competitors, business partners, and peer companies have encountered. Have you seen similar attacks?

## Preparing for privacy breaches

While cyberattacks themselves can be enormously damaging, the potential for regulatory fines can be equally if not more damaging to an organization. It's essential for security teams to assess what regulations will apply to them in the event of a breach-based on your industry and the data you hold that may be targeted—and how they can be best prepared to ensure compliance. Questions to ask include:

- What are your privacy obligations—including industry regulations, state/federal data breach laws, and contractual agreements?
- When do you need to provide notification of privacy breaches (factors often include breach size and whether the data was encrypted—but vary across geographies and industries)?
- Who needs to be notified, and how (customers, attorney general's office, others)?
- What is the time limit for notification?

Privacy obligations are already a major concern for security and privacy professionals, and it's likely to increase with the EU's incoming General Data Protection Regulation, or GDPR, which goes into effect in May 2018.

*"GDPR is one of the biggest developments in privacy in decades. For most organizations, fulfilling data breach notification requirements is already a significant challenge. GDPR adds another complex layer to that sentiment"*

— Dr. Larry Ponemon, Chairman and Founder of the Ponemon Institute

The GDPR is a globally focused privacy law that introduces steep, sweeping changes. It applies to any organization globally that does business with EU citizens or organizations, includes a 72-hour window for data breach notification (which is much tighter than most current laws in the US), and can impose potentially enormous fines for non-compliance (20 million euros, or four percent of an organization's annual revenue). Organizations should take steps and set roles, responsibilities, and processes for complying with GDPR now.

## Assessing your organization

Additionally, your threat landscape is not just the external factors and risks that may impact you, but also your internal challenges and shortcomings. As described earlier, the cybersecurity skills gap looks to be a challenge that our industry will need to manage for the foreseeable future—and organizations should assess how it impacts them today and work to manage it.

To identify your internal skills gap, evaluate the current skills you have versus the skills you'll need to effectively combat and manage the external threats you face. Performance metrics such as time-to-completion on individual tasks and workload balance are good indictors of the skills you have today and where the gaps are. And by using tabletop exercises and analysis, you can further validate your assessment and find additional gaps you may have overlooked.

Finally, your threat landscape—the attacks you face, the regulations you're beholden to, and your organizational skills shortage—is a continually evolving assessment. As the cybercrime market, privacy regulations, and other industry trends shift, your landscape will too. Be sure to set regular intervals to review and update your threat landscape accordingly.

**Case Study:**
**Top 10 European Bank**

One IBM Resilient customer faced a unique challenge: they had three security teams around the world who managed incidents with their own specific processes. This led to valuable threat information becoming siloed, a lack of central management and oversight, and no dependable way to test and improve IR processes.

The organization's security leadership knew it had to standardize IR plans across the organization and enable centralized incident management and oversight.

The plan: the security leadership team brought the groups together to collectively develop combined, standardized response plans for specific incident types—incorporating the most effective and proven processes from across the three groups. Additionally, the organization implemented a single incident response platform (IRP) for the three groups to:

- Centrally manage incidents across the organization
- Enable better context gathering and collaboration
- Provide better visibility to management
- Create a feedback loop that ensures new IR plans, tests, and improvements are shared across the organization

With this new strategy, the organization's security teams can continually gain value from the organization's experience and intelligence collectively.

## Step 2: Build a standardized, documented, and repeatable incident response plan

Surveys indicate that insufficient planning and preparedness is still the single biggest barrier to cyber resilience today. It is, perhaps, not surprising then that most organizations don't have a proper incident response plan in place. According to the 2016 Cyber Resilient Organization study from the Ponemon Institute, only 25 percent of organizations have a cyber security incident response plan (CSIRP) in place and applied consistently across the organization. The remaining 75 percent either don't have a plan at all, follow informal, ad hoc processes, or don't have their plan applied across the organization.

As a result, many IR functions are slow, inefficient, and ineffective–which increases the likelihood of a costly, damaging cyberattack, increases employee dissatisfaction and burnout, and puts security leadership's jobs at risk. However, having a standardized, documented, and repeatable IR plan addresses these risks and ensures your team knows exactly what to do, and when and how to do it. It also provides a platform for continual improvement, enabling your organization to stay ahead of ever-evolving cyber threats.

The challenge: creating a proper IR plan is time-consuming and requires a dedicated, organization-wide effort. To that end, security leadership needs to work to make incident planning a priority. An incident response planning workshop can ensure that all your team's stakeholders come together to develop consistent, documented, and standardized response plans.

Your team should engage with executives and even the board of directors to ensure they understand the risks and let other relevant leaders know that they'll be expected to contribute. This includes marketing, HR, legal, IT, and other business units.

During the workshop, your teams (with security leadership's guidance) can come together to walk through specific incident scenarios and:

- Map out specific steps that need to be taken to resolve an incident throughout its lifecycle
- Determine roles and responsibilities
- Identify the key technologies and channels of communications to be leveraged during a response
- Build processes around permissions and escalations

Resources like NIST, SANS, and CERT can provide great frameworks for these conversations and plans—but, ultimately, your IR plans will need to be specific to your organization. Therefore, it's important to involve all contributors across the organization. You will need to tap the know-how and experience of your existing IT and security teams, key stakeholders within your organization, as well as executives, and legal and compliance officers. External third party entities like business partners and suppliers can also be part of the conversation.

By the end of these exercises and conversations, your team should have well-thought-out, repeatable, and documented plans that can be centralized, followed by anyone on your team, and continually improved upon over time.

**Case Study: Fortune 100 Technology Company**

One IBM Resilient customer had made major technological investments in their SOC, and needed to ensure their people and processes were equally developed. Their plan: use simulations to test processes and develop SLAs and executive reporting.

This customer established regular, quarterly simulations that focused specifically on complex and unlikely events—ensuring they wouldn't be caught off-guard by most severe threats. To gain organizational support, the security leadership developed incident response SLAs. These metrics were grouped by incident types and severity, and provided a standard for the incident response team to strive for. Additionally, the SLAs enabled the CISO to demonstrate performance to the board—and set budget accordingly. Today, this customer continues to experience hundreds of incidents daily—but their well-trained team can manage and resolve them in a streamlined, effective manner.

## Step 3: Proactively test and improve IR processes

Cyber adversaries are continually striving to gain new advantages. Cyber security teams need to make staying ahead a priority.

One of the most effective ways to keep IR capabilities driving forward is running simulations—and doing them in a dedicated, results-driven manner.

IR simulations provide a useful method for overcoming the "insufficient planning and preparation" barrier. Simulations ensure that your entire IR function—people, processes, and technology—are primed and ready for real-world incidents, while also uncovering opportunities for future improvements.

The key for security leaders is to ensure that their simulations are effective, and there are specific steps your team can take to ensure your team is making improvements and making them stick.

To start, security leaders should plan upfront to make the simulation meaningful. Do you want to practice a commonly seen incident, or prepare for something unexpected? Both types are valid to explore.

Security leaders should also build specific, thoughtful simulations that include important details your analysts will need to search for. In other words, make your team think critically about the simulation and ensure it's more than just a check-the-box exercise.

Additionally, make your simulations measurable. Set goals and track key metrics such as time-to-completion and level of completeness. And replay simulations to measure improvements (or regressions).

Finally, make IR simulations an organization-wide event. Include participants from HR, legal, marketing, and other groups to ensure they will be ready to play their parts when a real incident hits. Similarly, share the results of your post-mortem analysis across the organization. This will help keep your team honest and educate leadership on where and what resources are needed.

## Step 4: Leverage threat intelligence

Cyber criminals are working together—collaborating and sharing information across the dark web. Security professionals should be working together, too.

As part of the 2016 Cyber Resilient Organization study, the Ponemon Institute compared high-performing respondents (those whose cyber resilience had increased in the last year) to average organizations to identify key differences. One of the many findings: high-performing organizations are more likely to participate in a threat-sharing program (70 percent versus only 53 percent of average organizations).

The threat intelligence (TI) industry has seen increasing buzz in recent years, and for good reason: security teams are seeking better insight and awareness into the activity in their environments.

Leveraging threat intelligence is a big part of becoming more aware. But there are challenges to implementing it. Security teams often need to navigate countless feeds of varying quality, as well as manage the signal-to-noise problem.

Fortunately, many IBM Resilient customers have years of experience implementing and experimenting with a variety of threat intelligence feeds. Based on their combined experiences, here are three key ways to effectively leverage TI for better incident response:

- **Anchor threat intelligence in incident response plans**
  One IBM Resilient customer, a major media network, found their analysts spent far too much time investigating threat intelligence data. They were chasing issues that didn't apply to them, which drained resources and severely limited their effectiveness.

  To fix this, the team grounded threat intelligence data into their existing incident response processes. Analysts escalate indicators of compromise (IoCs) into incidents, and they can access vital information about potential threats when needed—using the available intel when relevant to the circumstances they face. This led to huge improvements in time management and team effectiveness.

- **Use integrations and correlation to make threat intelligence actionable**
  By integrating threat intelligence with other data sources like SIEMs and EDR tools, analysts can gain fuller incident context and the information becomes more actionable. They can refine and target the scope of the data by considering the context, severity, and patterns. This helps analysts better understand what they're contending with and what would be best to do about it.

- **Track and measure the usefulness of your sources**
  There are plenty of intel feeds and none are one-size-fits-all. Examples include open source, closed communities, commercial sources—and then there's the threat intelligence platforms. Record how often individual feeds provide information, and the quality and how critical the information provided is. You'll soon discover if certain feeds are redundant or need to be adjusted in any way.

As we'll explore further in upcoming sections, incident response platforms (IRPs) can automate much of the manual portions of cyber incident investigation and response. Among other improvements, IRPs use data analysis and specialized logic in an approach called artifact visualization. This allows you to see how seemingly disparate incidents might be related by noting the commonalities between them—such as IT assets involved, malicious software used, malicious infrastructure communicated with, and so on.

Organizations that can identify incidents and grasp the disparate artifacts that make up the story of a breach will drive down response times from days or weeks to hours. This also helps to implement practical controls in areas like user access, data security, and communications that will prevent future incidents from occurring.

---

*"81 percent of respondents say sharing intelligence improves the security posture of their organization and 75 percent of respondents say it improves the effectiveness of their incident response plan"*

— The 2016 Cyber Resilient Organization, The Ponemon Institute

---

## Step 5. Streamline incident investigation and response

As noted in the Verizon Data Breach Investigation Report, fewer than a quarter of all incidents Verizon reviewed were detected in "days or less," while the majority took days, weeks, or months to detect[5]. With cyber incidents lasting undetected for weeks or months, malicious actors have the opportunity to establish a beachhead on compromised networks that can be difficult to remove.

One reason is that most organizations rely on ad hoc processes for investigating even straight-forward cyber incidents like phishing attacks on employees—and because of the skills gap, organizations who have the right tools and technology may struggle to find enough resources to efficiently manage the deluge of incidents.

As organizations add integrated data and threat intelligence sources to their IR processes, the opportunities to orchestrate responses in a sophisticated way grows—starting with the automation of low-level tasks.

Automation is a useful method of streaming menial, repetitive tasks, and making your team faster and smarter. When used in a broader incident response orchestration strategy (learn more about orchestration in the next section), automation can empower your team to be strategic decision makers.

In the case of an outbreak of malware, for example, a suspicious sample detected on one endpoint can be automatically grabbed and fed to an endpoint agent or next-generation threat detection platform to observe and classify. Based on the outcome of that analysis, further automated and manual processes can be queued up: identifying other infected hosts on the network and requesting permission to quarantine them, identifying a vulnerability associated with that malware infection and scheduling emergency patches to vulnerable systems, or firing off requisite notifications to internal staff or external monitors, for example. And, at each stage, requests, responses, and actions can be documented for future reference.

To begin with automation, pinpoint the right processes to streamline. These are often time-consuming, menial, and inefficient tasks that take up inordinate amounts of analysts' time, and can be safely and reliably automated. Security leaders should also analyze the risk and complexities of automating a process versus the potential efficiencies gained.

To ensure safe and reliable automation, test the processes' fidelity. Script manual actions that keep human decision-making and approval involved. Once your team builds a comfort level to know that the process is right and the technology works properly, you can decide to fully automate.

However, it's important to note that while technology-based automation can save time, it's only as strong as your overall IR function—and is most effectively leveraged in an orchestrated incident response strategy.

*"Rome wasn't built in a day, but data breaches frequently were... If you have legit creds, it doesn't take a very long time to unlock the door, walk in and help yourself to what's in the fridge."*

— The Verizon 2016 Data Breach Investigations Repory

## Step 6. Orchestrate across people, process, and technology

The promise of incident response orchestration—making response faster and more automated—has drawn the attention and interest of many security experts across the industry. But as referenced in the last section, successful and effective orchestration and automation requires a strong overall IR function. The key to effective orchestration lies entirely on the quality of an organization's IR fundamentals: people, process, and technology.

The earlier sections of this guide have been created to help you ensure these fundamental building blocks are well-thought-out, strong, and primed for future improvements. To refresh, here are essential questions to ask when assessing the strength of your IR foundation:

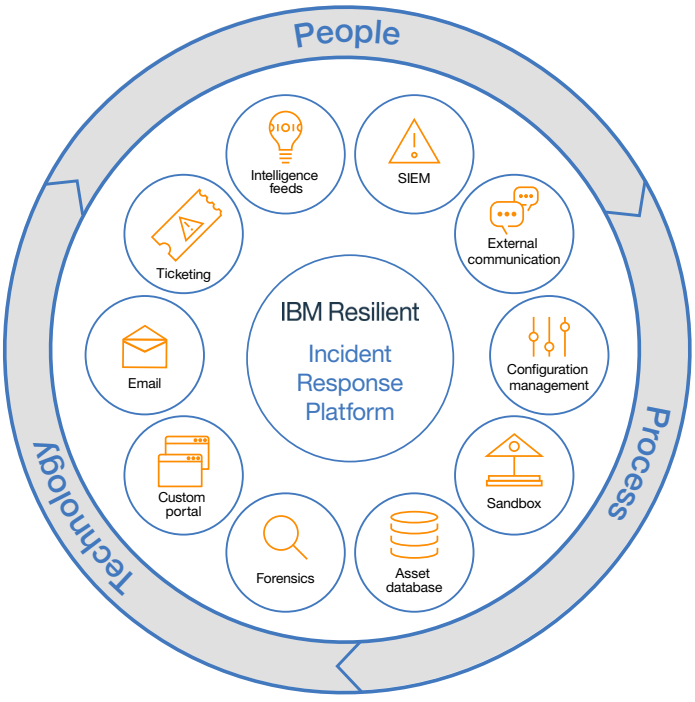



*Figure 1*: How the Resilient IRP acts as a central hub for IR orchestration.

**People:** Have you ensured your IR team is well-coordinated and well-trained? Do they have the right skills to address all aspects of an incident's lifecycle? Do they have means for collaboration and analysis?

**Process**: Do you have well-defined, repeatable, and consistent IR plans in place? Are they easy to update and refine? Are you regularly testing and measuring them?

**Technology**: Does your technology provide valuable insight and intelligence in a directed fashion? Does it enable your team to make smart decisions and quickly act on those decisions?

By addressing these questions, you can ensure your orchestration efforts will align these building blocks with real effect. If you haven't developed this foundation, the benefits of orchestration will be marginal.

The goal of incident response orchestration is to empower your response team by ensuring the humans in the loop know exactly what to do when a security incident strikes, and have the processes and tools they need to act quickly, effectively, and correctly.

Orchestration and automation are both growing in popularity among cyber security professionals, but orchestration is different in that it supports and optimizes the human-centric elements of cyber security—like helping to understand context and decision making—and empowers them as central to security operations.

This is a critical distinction because security threats are uncertain problems. Responding to a threat is hardly ever a cut-and-dried issue. Automation is a great tool for quickly and effectively executing specific tasks—but since threats are often evolving and adversaries are changing tactics, human decision-making is needed to step in for things like escalating issues or troubleshooting.

Automation is an effective tool in the broader orchestration process, but it's the human element that makes orchestration the game-changer that it is.

Orchestration applies differently to each specific organization. It should map to your unique threat landscape, IT and security environments, and company priorities. But for a quick example, the following is a classic use case of how we see orchestration employed in many of the organizations we work with.

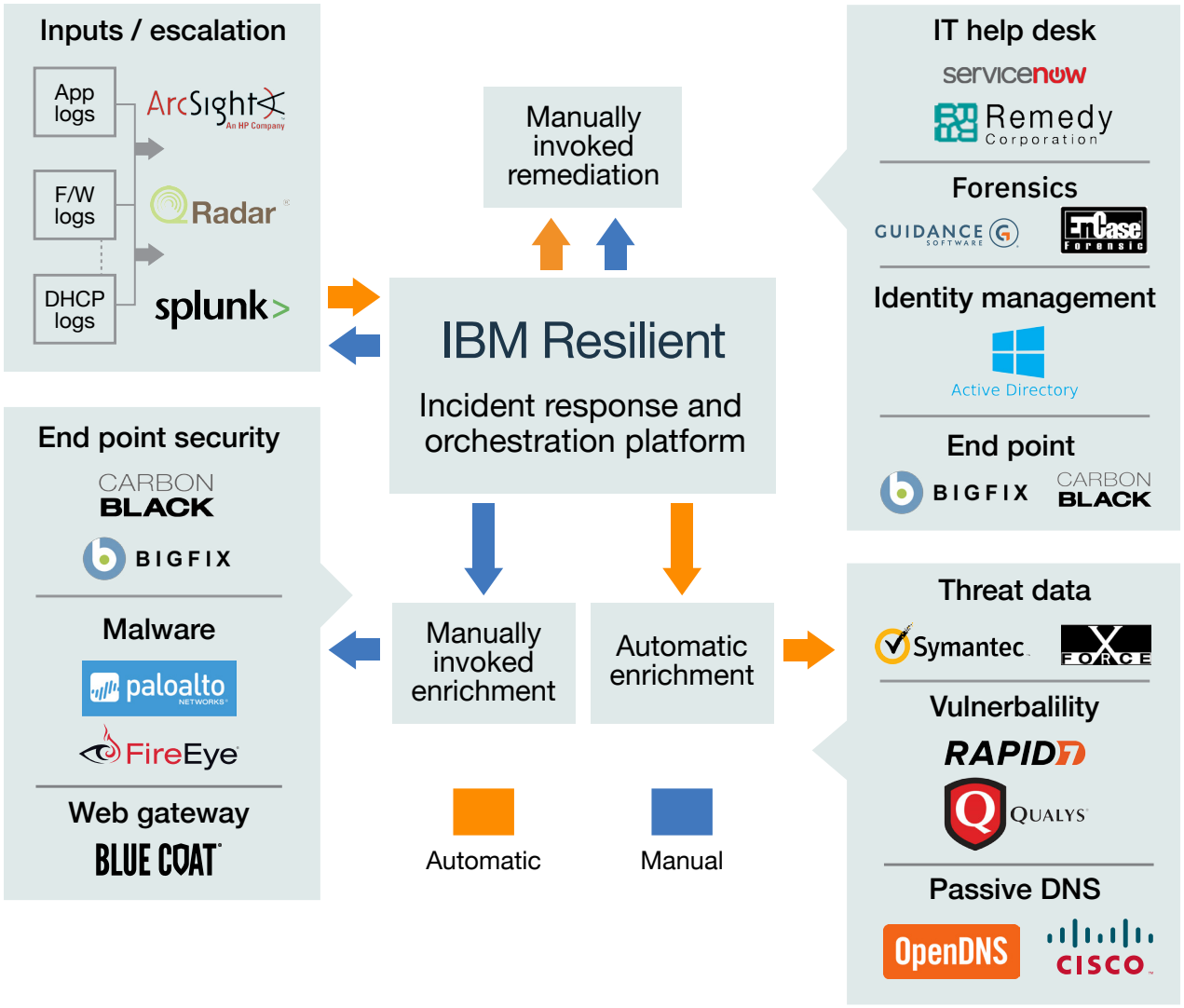



*Figure 2*: An example of an orchestrated response workflow using an integrated IRP.

In the top left of the graphic, you can see that as an incident is escalated from a SIEM alert, a record is automatically created in the organization's incident response platform (IRP). From there, in the bottom right, the platform automatically gathers and delivers valuable incident context from the built-in threat intelligence feeds and additional sources.From here, the security analysts already have critical information when they step in and take control. These analysts can leverage additional integrations to manually take on additional tasks deemed necessary—including gathering additional information about an incident from other security tools (such as endpoint security tools or web gateways) or starting to remediate the issue by alerting the IT help desk or going to the identity management to pull users off the network.

There are many different ways to orchestrate IR processes, but the goal is always the same: put your analysts in the best position to respond to threats.

## Conclusion: Building a resilient, response-ready organization

It is tempting to imagine that technology advancements will soon turn incident response into a *push button* function that can be performed by even junior employees. The truth is that IR is, and will be, complicated and multifaceted and will require the attention of intelligent security analysts.

Mature incident response combines people, processes, and technology as part of a continuum. The job of technology isn't to replace human analysts, but to empower them to do more: delivering better intelligence about specific threats, streamlining response processes, and making sure that security analysts are ready to respond.

Additionally, a mature cyber security incident response function can beget a larger, cultural transformation within your organization: integrating your security team more closely with IT operations and management, and enlisting them in the process of responding to cyber incidents in a comprehensive way.

As incident response processes mature, organizations enter a phase of proactive response, in which information gleaned from incident response becomes strategic to an organization. With proactive response, intelligence from the IR team can be fed back into a security and IT organization—shaping technology investments and acquisitions, sharpening employee skill sets, and broadening an organization's understanding of risk to encompass a broader ecosystem of physical security assets and providers, threat intelligence providers, regulators and government agencies, and more.

While few companies—even within the Fortune 500—have achieved this level of maturity, we expect the strategic application of incident response to become more common as more firms migrate to mature incident response platforms in the coming years.

## For more information

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: **https://www.ibm.com/account/reg/us-en/signup?formid=MAIL-securityresilientdemo.**

## About IBM Resilient

The mission of IBM Security is to help organizations thrive in the face of any cyberattack or business crisis. The Resilient 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 complete IR orchestration and automation platform, enabling teams to integrate and align people, processes, and technologies into a single incident response hub. Many Fortune 500 companies, and hundreds of partners globally depend upon IBM for Resilient best-in-class security solutions.



IBM Corporation
Security Group
Route 100
Somers, NY 10589

Produced in the United States of America
December 2017



1 http://www.esg-global.com/blog/dealing-with-overwhelming-volume-of-security-alerts

2 http://cyberseek.org

3 http://info.resilientsystems.com/hubfs/IBM_Resilient_Branded_Content/White_Papers/2016_Cyber_ Resilient_Organization_Executive_Summary_FINAL.pdf

4 https://securityledger.com/2016/02/focus-on-privacy-hobbles-security-at-healthcare-orgs

5 http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016

Please Recycle

BUW03068USEN-00