IDC MarketScape

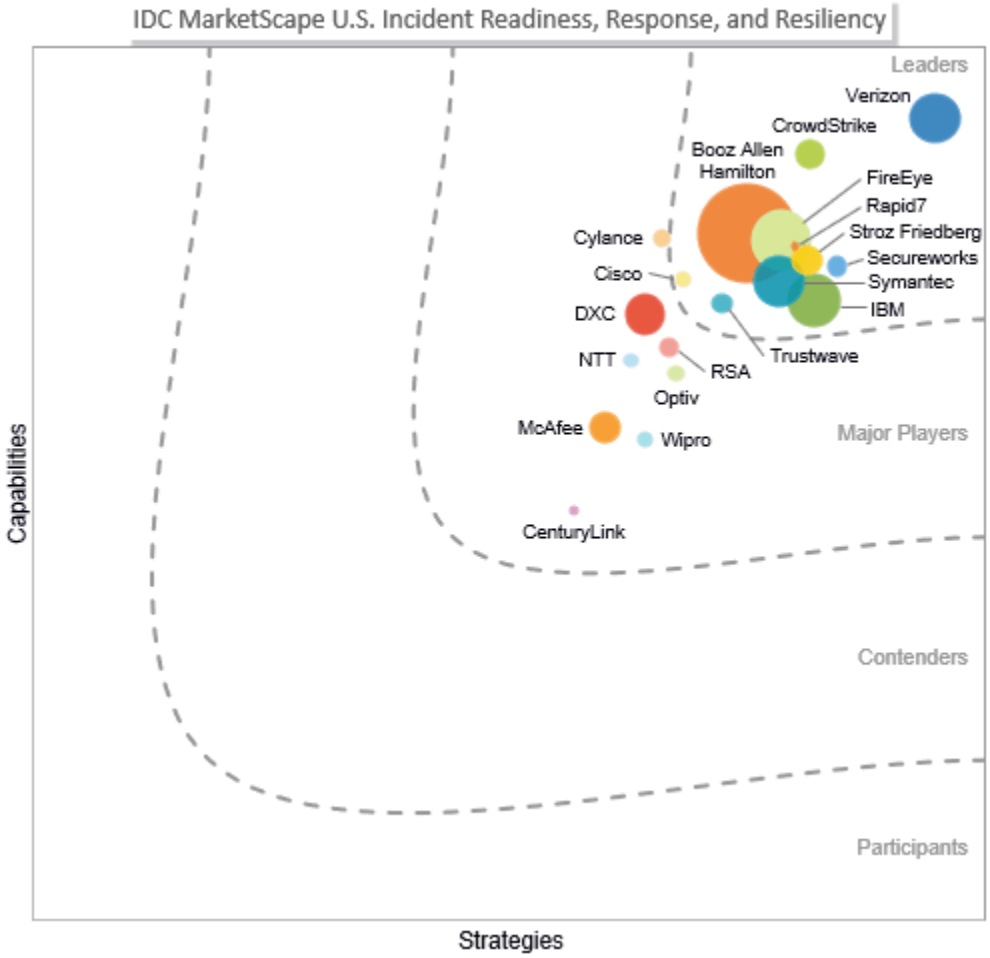
# IDC MarketScape: U.S. Incident Readiness, Response, and Resiliency Services 2018 Vendor Assessment — Beyond the Big 5 Consultancies

Christina Richmond Pete Lindstrom

## IDC MARKETSCAPE FIGURE

## FIGURE 1

**IDC MarketScape U.S. Incident Readiness, Response, and Resiliency Vendor Assessment**




Source: IDC, 2018

September 2018, IDC #US44257117

Please see the Appendix for detailed methodology, market definition, and scoring criteria.

## IDC OPINION

The incident response (IR) services marketplace comprises providers such as the Big 5 consulting firms, start-ups, security services consulting organizations, and managed security services providers (MSSPs). Earlier in 2018, IDC published its first document on incident readiness, response, and resiliency services when it looked at the Big 5 U.S. consulting firms in *IDC MarketScape: U.S. Incident Readiness, Response, and Resiliency 2018 Vendor Assessment — Big 5 Consulting Firms* (IDC #US43588417, March 2018). The current document reviews companies that do not fall under the Big 5 definitions. It includes those providers whose revenue is derived from both the small and the midmarket as well as the large enterprise and government.

While traditional incident response is focused on identifying and containing a security breach or attack, this document broadens the scope to include pre-attack readiness and post-attack resiliency. IDC believes that service providers need to evolve beyond a point-in-time engagement, to both satisfy increasing demand for security consulting and remain competitive and viable.

Enterprises can differentiate their security programs with readiness, response, and resiliency capabilities. Even those with no immediate need for incident response services struggle with ensuring they are ready to respond to a large incident, and fairly routine smaller incidents may turn into larger ones. The experience that IR service providers gain from working on many different incidents at many different companies is an invaluable perspective that enterprises crave for strategic planning purposes.

Using the IDC MarketScape model for this study, IDC has compared 19 U.S. firms whose revenue is derived from small, midmarket, and large enterprises or government and that offer IR services. Through in-depth interviews with the service providers and their customers, IDC evaluated the vendors in this study of comprehensive IR services and, through granular evaluation, IDC found that each provider possesses certain strengths and weaknesses when compared with a peer group. The differences appear in both current capabilities and future strategies.

Some of the service provider capabilities that were reviewed during the study are:

- Breadth and depth of core and complementary offerings, encompassing readiness, response, and resiliency
- IR services delivery methods (remote, onsite, private cloud, public cloud)
- Methodology, including approach to analyzing, scoping, and validating incidents for purposes of prioritizing IR activities
- Customer communication strategy
- Incident checklists and documentation
- Investigation and case management tools
- Threat intelligence and big data/analytics capabilities
- Service-level agreements (SLAs), retainers, and onboarding processes
- Bench strength and skills of IR personnel
- Talent acquisition, retention, and education/reskilling

IDC believes there are several service provider capabilities that will drive growth and maturity in the IR marketplace, and allow service providers to sharpen and differentiate their value propositions. These are described in the Appendix section of this report.

For this IDC MarketScape study and evaluation series, IDC grouped the service providers into the following categories:

- Big 5 firms that often sell more strategic services that are acquired through a CFO's office
- Service providers that fall outside the "Big 5 consultancy" definition and have the resources and experience levels to be able to assist in major incidents

Please refer to *IDC MarketScape: U.S. Incident Readiness, Response, and Resiliency 2018 Vendor Assessment – Big 5 Consulting Firms* (IDC #US43588417, March 2018) for insight into the Big 5 capabilities.

**Cautionary note:** Do not read this document by scanning only the Leader quadrant. All participants in this study have been selected because they are strong providers and each participant differentiates itself uniquely. It is entirely possible that the best IR service provider for your company is a Major Player and not a Leader. Also use caution in equating the size of the marker in Figure 1 with the most experienced and appropriate provider to your business. As noted in the Appendix, the size of the individual vendor markers in the IDC MarketScape represents the *relative* market share of each individual vendor within the specific market segment being assessed. Many up and coming, newer providers are experiencing rapid year-over-year growth because of new technologies and approaches and should be considered.

## IDC MARKETSCAPE VENDOR INCLUSION CRITERIA

IDC collected and analyzed data on 19 IR service providers as part of this IDC MarketScape. IDC narrowed the field of providers for this study based on the following criteria:

- **Standalone service capability across the incident readiness, response, and resiliency life cycle.** Each service provider was required to possess delivery capabilities in some or all of the incident readiness, response, and resiliency life cycle (see the Appendix for an explanation of incident response).
- **Retainers.** There is a broad range of retainers offered within incident response services. For the Big 5 consulting document, it was a requirement to offer retainers. In this second document, there is more of a variety with some service providers not offering retainers and/or including incident response within managed security services (MSS).
- **Revenue.** While there was no minimum required, each service provider was required to prove 2017 U.S. revenue garnered in the incident response arena.
- **Geographic presence.** Each vendor was required to have IR delivery capability in the United States.
- **Time frame.** The time period studied was 2016-2017, with research ending toward the middle of 2018. It is possible that service providers have enhanced services since that time. Where possible, IDC notes that changes are expected, but it is incumbent upon the buyer to request a services update from the shortlist of companies you have compiled.

## ADVICE FOR TECHNOLOGY BUYERS

Organizations that want to conduct a thorough evaluation of incident response services face a challenging task. The marketplace is heavily fragmented with some providers highlighting certain capabilities like criminal investigations, technical prowess, breach or attack type, or even worldwide presence. They may focus on certain industries like retail or government support, and they may go to market through the CFO or the IT department. As a result, some enterprises choose to have multiple relationships with multiple IR providers for specific services. Enterprises rarely outsource IR services entirely but augment to lesser or greater degree their in-house IT/IR staff, processes, and technology.

Enterprise approaches to evaluation and selection of IR service providers vary widely – another indication of marketplace turbulence. Vendor selection criteria were discussed during customer interviews, and they include multiple factors – the most highly rated of which are outlined here:

- Reputation and previously existing relationships
- Global response capability
- Nature of breach
- Response times
- Depth of experience, technical competence, and forensics capabilities
- Industry-specific experience

Additional but less significant factors included market positioning, full service versus component offerings, pricing, flexibility with pricing and terms and conditions, performance in a trial event, resource availability, location and certifications, references, breadth of tools, customer service, and infrastructure support and collaboration.

The main reasons to choose a provider is their technical acumen, reputation for security technology, security operational management, and threat visibility. These firms have other attributes, strengths, and weaknesses that may be evaluated and compared with other IR responders as indicated:

- Select a strategic provider as your key readiness, response, and resilience firm prior to any incident occurring. Consider a retainer, or at least work with the applicable provider, to ensure you understand its methods and it is familiar with your organization.
- Use smaller breach readiness projects such as penetration testing, tabletop exercises, and red teaming to test the capabilities of your strategic provider. Ensure it is providing key insights and management oversight, as well as demonstrating its communication skills.
- Ensure that providers have the resources available to address the business, technical, and communication needs of your organization. Constantly reassess these resources as consultants come and go from the providers.
- Fill provider gaps based on circumstances when situations arise. One provider may not be able to provide all the services necessary. When the time comes, this strategic provider should be able and willing to assist in identifying key services that will be more pertinent to the situation. If the provider can't recognize its own gaps and assist in filling them, it should not be a strategic partner.
- Ensure that your IR provider has standard methods and timing for pertinent communications during an incident, and that it is building an incident portfolio that includes details as addressed in reference architectures that avoid ambiguities in certain reference name expressions (such as a "ref1..ref2" format) along the way. The key guiding criteria should be

whether someone reviewing the information in three years (such as trial lawyers) will be able to understand exactly what occurred.

- Be wary of technical lock-in. Evaluate any tools that may be required independently for strategic portfolio fit within the organization. If a provider requires technology that must be purchased but isn't a strategic solution, consider other options.

As part of the broader decision process, organizations should bear in mind the following considerations and recommendations:

- **Breadth of offerings, including core and complementary services.** Identify the types of services that are offered by each service provider you evaluate. You may need to make a decision about whether to acquire all the needed services from a single provider or from two or more providers.
- **Incident response plan testing.** No matter how good a plan is, you don't want to be putting it and your playbook into action for the first time during an actual cyberattack. Testing approaches include:
  - Simulation/cyber range/war gaming immersive simulations of a breach beyond tabletop exercises, which include all stakeholders that would be included in a real incident: C-suite executives, legal, corporate communication, the board of directors, the crisis team, the systems organization, and the IT organization
  - Desktop/tabletop exercises involving key stakeholders and the IT organization
  - Red/blue/purple team penetration testing and corresponding practice drills involving key IT organization personnel
- **Scope of delivery methods.** Match up your requirements with providers' ability to deliver services remotely and at onsite locations worldwide.
- **Types of attacks.** Not all service providers respond to all types of attacks. Some specialize in malware-related and other technical attacks, while others may address spear phishing and criminal investigations.
- **Policy and plans.** Providers discussed in this study offer all or most of the policy and plan creation elements included in NIST 2.3 (NIST A [2012] **nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf**). Some go beyond NIST to align with other industry standards by including additional or optional supplemental services. Be sure that policies and plans are integrated across business units, departments, locations, and so forth. Responsibilities, decision-making paths, and prescribed actions should be clear to all who are involved in incident detection and response.
- **Partner versus vendor delivery.** If the providers you are evaluating engage delivery partners in some capacity, be clear about who is providing what, as well as the lines of responsibility and accountability. Some partnerships are formed for purposes of the PCI Forensic Investigator Program because this type of investigation may present a conflict of interest depending on a provider's overall business offerings. Other partnerships may be to extend resource capacity during a surge of events.
- **IDC's recommendation: a published standard (e.g., NIST, ISO, or SANS Institute) should be the foundation of a participant's offering.** Review the methodology of service providers so that you feel comfortable with their approach. While every attacker and breach are different, the methodology should be a proven process that undergoes continual improvement based on postmortems and lessons learned. A service provider should be able to explain its methodology in detail, provide or show sample deliverables, and discuss IR team roles and responsibilities and how and why they may change over the course of an engagement. It may

be helpful to review the methodology against one or two scenarios that are plausible for your organization.

- **Service-level agreements and retainers.** A retainer agreement details the terms, conditions, and timing of incident response.

  The most common arrangement is a retainer to which SLAs are attached, and these may be tiered. Customers pay an up-front fee to have the service provider "on call" for future assistance. Onboarding approaches vary from provider to provider as is the time required to complete the paperwork.

  Be sure your service provider allows you to apply unused retainer dollars toward other services (see Table 1).

- **Documentation.** It is worthwhile to compare the standard items or issues tracked by service providers during an IR engagement. Some service providers augment the list described in NIST 3.2.5 (NIST A [2012] **nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf**).
- **Communications.** IDC believes the optimal approach to communications during an incident response engagement is for the provider to use some standard templates and some ad hoc communications tailored to the specifics of the client and investigation. Ideally, written communications supplement interactive communications such as daily briefings, but the cadence of all communications should be agreed upon by the provider and the customer.
- **Containment strategy.** Ask service providers to describe the criteria they have established to help them choose and recommend a containment strategy. IDC believes the most important criterion is operational impact — that is, keeping the business running.
- **Pricing models for incident response services.** Assume that pricing models are negotiable, at least to some extent. Models include retainer, per hour, per day, per week, and discounts on multiple services. Retainers are typically set up on an annual basis. Some providers have developed variations such as:
  - A fixed price offering with a set number of hours for emergency response
  - Tiers of hours attached to retainers
  - Ad hoc services negotiated with blocks of time
  - Flexible pricing based on scope of work
  - Zero-dollar retainers
- **Security talent.** While certifications were generally viewed by end customers as important but not critical, they can be an indicator of a provider's investment in its people, along with mentorship, training, and systems for sharing information among first responders. Evaluation of talent without firsthand experience is difficult, so it may be helpful to understand how the provider forms IR teams and matches team member skills to customer requirements. Should you require incident response in multiple locations, you may want to compare the qualifications, experience, and skills of the potential or assigned teams that could be involved. And, if top requirements include skills, such as management/board-level presentations, or expertise in specific areas, such as risk or compliance, understand how these resources are incorporated into the provider's team.
- **Customer service.** Find out whether your potential service provider has a formal customer experience program if this is important to your organization. If it is, you may want to delve into the specifics. For example, understanding how customer satisfaction is determined and how planned service improvements are validated with customers. A dedicated account manager

can be essential to the delivery of consistent customer service, but processes should be in place to ensure that the service level isn't dependent on a single person.

## TABLE 1

### Service-Level Agreements

| SLA Component | Time Ranges Based on Service Provider Responses |
|---|---|
| SLA for call back or first contact with a customer after an incident is reported | 1 to 8 hours |
| SLA for beginning remote incident response | 2 to 48 hours |
| SLA for onsite arrival | 24 to 72 hours, applicable to continental United States, North America, and/or global destinations |

Source: IDC, 2018

## VENDOR SUMMARY PROFILES

This section briefly explains IDC's key observations resulting in a vendor's position in the IDC MarketScape. While every vendor is evaluated against each of the criteria outlined in the Appendix, the description here provides a summary of each vendor's strengths and challenges.

### Booz Allen Hamilton

Booz Allen Hamilton (BAH) is positioned as a Leader in the 2018 IDC MarketScape for U.S. incident readiness, response, and resiliency services – beyond the Big 5 consultancies.

BAH states that it offers full incident life-cycle IR solutions that consider the whole business impact. It offers a range of services including:

- Strategy and assessments
- Incident response and cyberinvestigations
- Cyberdefense operations and engineering support
- Managed threat services

These services encompass a proactive, reactive, and managed incident response capability ranging from assessments, wargaming, incident program planning and playbook development, and tabletop exercises to breach response and a postmortem assessment to reconcile learnings into the IR plan going forward. The company completed the acquisition of Morphick in the fall of 2017 to extend its commercial security services offerings and add managed detection and response capabilities to its arsenal. Booz Allen blends its consulting with "managed threat services" thereby distinguishing its managed services from traditional alert analysis by offering outcome-based detect and respond services to protect its customers from attackers. And finally, BAH provides ongoing threat hunt operations to identify evidence of adversary activities that have evaded traditional threat detection.

BAH is the only firm in the world to hold all three of the U.S. Government's elite cyber-accreditations including the Cyber Incident Response Assistance (CIRA) and Vulnerability Assessment Service accredited by the National Security Agency as well as the GSA Highly Adaptive Cybersecurity Services. It is the only company to also be accredited by the Forum of Incident Response and Security Teams (FIRST) and by Crest CSIR stating that BAH processes meet the standards used by many government, educational, and financial institutions throughout the British Commonwealth and beyond. In addition, BAH has industry depth in the financial, health and life sciences, energy, and transportation sectors. The company touts that its cyber experts hold more than 6,800 individual certifications.

### *Strengths*

Customers rated BAH highly for its planned research and development initiatives in the incident response market as well as for its unique hiring methodology, which is critical in an industry with the skill shortage that security encounters.

### *Challenges*

The company is not as well known in the commercial enterprise as it is for its government work. BAH hired industry veteran Bill Phelps to lead its up-and-coming commercial security services division, which is seeing strong growth. However, BAH is up against many industry incumbents and may experience stiff competition.

### *Consider BAH When*

Large enterprises that want a large team of security service talent on the bench as well as strong government-grade capabilities should consider Booz Allen Hamilton.

## CenturyLink

CenturyLink is positioned as a Major Player in the 2018 IDC MarketScape for U.S. incident readiness, response, and resiliency services – beyond the Big 5 consultancies.

With the acquisition of Level 3 in 2017, according to CenturyLink it is now the second-largest U.S. communications provider to global enterprises. While much of the integration had not yet occurred at the time of this document, CenturyLink states that many changes and improvements are under way to its readiness, response, and resiliency services because of the blending of the two companies.

Since 2008, CenturyLink has transformed its business by acquiring several strategic companies, each of which has given CenturyLink new capabilities and many of them focused on security services. This transformation included the acquisition of Savvis Communications in 2011, which helped broaden CenturyLink's services portfolio by adding managed security services as well as domestic and international enterprise networking, hosting, colocation, and cloud infrastructure and services. Level 3, which was acquired in 2017, is a global internet service provider based in Broomfield, Colorado. Level 3 offers a multilayered approach at the edge through its network-based security method versus using a point solution architecture. The company has a strong threat research team that provides visibility into the threat landscape to proactively detect threats and alert its customers. With the acquisition, CenturyLink adds network-based security, with a multilayer security design at the edge. This acquisition occurred after our evaluation of CenturyLink and the company's position may be elevated in the next study due to the additional capabilities it has acquired.

CenturyLink's incident response offerings reside within its MSS business that focuses on midmarket and enterprise customers but also has a breadth of government customers. CenturyLink has been providing managed security services for over a decade and has a number of offerings that are customizable to its customers. CenturyLink sells security in two ways: as an add-on to core company offerings such as network and hosting (mainly basic services) and as a standalone network-agnostic service for larger organizations that desire a true MSS partner.

Federal government entities and/or compliance-driven midmarket and enterprise organizations will find CenturyLink MSS a good option.

### *Strengths*

An analysis of the client's current incident management plan must be conducted by CenturyLink before the incident management service can be enabled, which IDC feels is a trend on the rise. Another cutting-edge trend that CenturyLink capitalizes on is a usage-based pricing model. IDC believes that inclusion of basic IR within MSS and offered on an opex basis will be seen more often in the coming year. One CenturyLink customer characterized it as "fairly responsive" and "generally respond within two to four hours of the time a log shows up."

### *Challenges*

While CenturyLink has been protecting and responding to incidents for its network communications customers for 20 years, it stood up the incident response service in 2016 and is a relatively new provider of services. The novelty of pricing and inclusion in MSS is a strong positive, but on the flip side, the company doesn't use any standard templates for response though it will do in the future. One customer stated that CenturyLink suffered some "lag time between sales and deployment" and that CTL "has a problem with executing from the front-line sales guy to the back-end engineer."

### *Consider CenturyLink When*

Large enterprise organizations looking for a network provider to also handle its day-to-day managed security can benefit from the unique usage pricing model and network visibility that CenturyLink provides.

## Cisco

Cisco Systems Inc. is positioned as a Leader in the 2018 IDC MarketScape for U.S. incident readiness, response, and resiliency services – beyond the Big 5 consultancies.

Cisco is a multinational technology conglomerate headquartered in San Jose, California, in the center of Silicon Valley. It develops, manufactures, and sells networking, telecommunications, and other high-technology services and products. Through its numerous acquired subsidiaries, such as OpenDNS, WebEx, Jabber, and Jasper, Cisco specializes into specific tech markets, such as Internet of Things (IoT), security, and energy management. Cisco introduced the Network Intuitive concept in 2017, and security is stated as foundational in its annual report. Its security services division resides within the advanced services business unit and offerings are organized into advisory, implementation, optimization, managed, training, and technical services. Incident readiness, response, and resiliency falls mostly in the advisory business.

The company continues to invest in acquisitions both broadly and specifically in security. Investments also are being made to simplify how customers work in a multicloud world to maximize business benefits in all areas of Cisco's offerings. The security practice includes approximately 5,000

professionals and touts over 300+ threat intelligence researchers in the form of Cisco Talos aligned with the IR practice. Security Everywhere is a concept Cisco coined in 2017 and demonstrates the integration of security in all Cisco offers. The company states that security is a "requirement of digitization."

Cisco has strong market traction in the enterprise, and as a result, the incident readiness, response, and resiliency services offerings fit well with its large existing base of customers. Cisco believes customers are at different stages of their security maturity. Therefore, Cisco can utilize its portfolio to create different entry points.

While the Cisco incident response practice is relatively young having been created in 2015, there is a lot of rigor in the IR process. Cisco creates unique internships that drive additional hiring opportunities.

Cisco customer feedback praised the company for incident response communications, overall incident handling, and process.

### *Strengths*

Cisco demonstrated a unique internship program with 50+ interns to select from in security alone. In a market rife with talent compression, this will help build out and sustain the company's security and IR talent. The company received consistent high marks from customers and offers a transparent and unique pricing structure.

### *Challenges*

Although Cisco has a solid brand name and reputation, it is not as well known in security services as it would like. It will continue to take some time for Cisco to build a reputation and market share in this area. Cisco does not have plans for offering integration into customer response management systems. This appears to be a growing trend which Cisco might wish to consider.

### *Consider Cisco When*

Large enterprises looking for networking and security product and services strength combined with an up-front pricing structure would do well to consider Cisco.

## CrowdStrike

CrowdStrike is positioned as a Leader in the 2018 IDC MarketScape for U.S. incident readiness, response, and resiliency services – beyond the Big 5 consultancies.

CrowdStrike is a privately held provider of proactive security services and one of the most rapidly growing companies in this space. The company serves a fairly wide spread of customer types and verticals.

CrowdStrike specializes in incident response. The company's portfolio of proactive services covers the spectrum from tactical to strategic. In proactive engagements with clients, rather than focusing on compliance auditing, CrowdStrike leverages its intelligence-led IR approach and understanding adversary tactics and techniques experience to identify security gaps within its client organizations or sit alongside executives to develop security strategies. CrowdStrike utilizes intelligence collected from attackers, other clients, and incidents occurring worldwide. Armed with an understanding of how attackers gain and maintain access to a victim's network, CrowdStrike emulates known attacker activity to test the security and readiness of clients' networks and personnel. CrowdStrike then

provides tailored actionable recommendations designed to prepare clients in the event of a security breach.

CrowdStrike touts its experience responding to security incidents with helping its clients prioritize their defense activities. Using its threat intelligence capability, CrowdStrike offers several assessments, analyses, and investigations and creates per-incident teams of SMEs according to the needs of the engagement. CrowdStrike seeks to customize its approach because each incident is different as are the client environments and their respective investments in technology.

CrowdStrike offers remediation activities that depend on the nature, scope, and details of the incident, as well as on the known and presumed capabilities of the threat actor and any governance requirements that may exist from local or governmental authorities. As for its differentiators, CrowdStrike cites Falcon Insight and Falcon Prevent, its cloud-based EDR and next-gen AV offerings, that enables consultants to gain visibility across a victim's endpoint infrastructure and prevent active malicious traffic and behavior from getting in the way of an effective investigation. In addition, the scalable cloud-based architecture of the platform (upward of over 150 billion events collected per day) allows the response team to begin work remotely in identifying/classifying the threat and to take corrective actions to begin to expel attackers from client environments before the impact increases. Their cyberthreat intelligence provides visibility into both endpoint activity and threat actor's actions and motivations. CrowdStrike teams get "rear view" looks at what happened in the past with Falcon Forensics Collector, a software tool that enables consultants to remotely retrieve snapshots from client endpoints. CrowdStrike also promotes its deep technical expertise combined with technology-agnostic capabilities, which gives its consultants the knowledge and technical expertise to leverage whatever security investments clients have already made, including legacy signature-based endpoint technology, open source tools, and various SIEMs, among other technologies.

CrowdStrike's security consultants work with the company's Global Threat Intelligence team to track adversary activity worldwide and produce customized, actionable intelligence for clients. This enables the CrowdStrike team to understand adversary motives and TTPs in an effort to anticipate their actions and attribute attacks.

CrowdStrike sees its size relative to the Big 4 consultancies as an advantage — the company is able to quickly identify operational gaps and adjust its own processes across departments internally. If CrowdStrike tries something that works well, the company incorporates it into operations. One example is of forming tiger teams to identify mechanisms and tools necessary to facilitate cost efficiencies. Another strength is the CrowdStrike workforce — team expertise derives from decades of collective security practice experience in private industry, security firms, and government agencies.

CrowdStrike offers proactive services for breach readiness at an hourly rate per consultant, with discounted hourly rates that scale down depending on hourly volume or quantity of hours purchased with a prepaid retainer. In addition, CrowdStrike offers an hour estimate reduction on certain engagements where services are delivered concurrently (i.e., two services that are 100 hours each can be delivered together for a total of 160 hours).

CrowdStrike states that investments in IR services are driven by tactical observations (information and insights derived from client engagements) as well as strategic planning (where the company believes the attackers and industry are heading). Such investments are prioritized as part of CrowdStrike's regular operations, hiring, and product development work.

### *Strengths*

One of the fastest-growing companies in the U.S. incident readiness, response, and resiliency services market, CrowdStrike uses its size and flexibility to its advantage. Customers using the CrowdStrike Falcon Complete product which provides 24 x 7 remediation services, takes preapproved actions on endpoints to block malicious activity, clean up malware, and quarantine infected systems state that the service alleviates the need for security teams to coordinate with help desk teams to take remediation actions. In addition, this service offering comes with a $1 million breach guarantee.

### *Challenges*

CrowdStrike is a younger incident response firm, but scrappy. Its customers are very pleased with its service capabilities as evidenced by their Net Promoter Score as provided by CrowdStrike. IDC believes it still has room to mature and grow in the areas of formalized customer service process and management of its team members. CrowdStrike is growing rapidly and globally and will be challenged to develop standard operation and process tools to support its rapid growth and expansion.

### *Consider CrowdStrike When*

When a company seeks an intelligence-led, hands-on "mitigate the adversary" approach by a young company that lives to thwart the bad guys, CrowdStrike should be considered.

## Cylance

Cylance is positioned as a Major Player in the 2018 IDC MarketScape for U.S. incident readiness, response, and resiliency services – beyond the Big 5 consultancies.

Cylance is a security technology and consulting organization that offers products and services that proactively prevent rather than reactively detect the execution of advanced persistent threats and malware. Cylance technology is deployed on over 10 million endpoints offering EDR protection to hundreds of enterprise clients worldwide including Fortune 100 organizations and government institutions. The Cylance Incident Response team utilizes its proprietary technology suite along with the consultant responder experience to assist clients with complex breaches, including within industrial control system environments. In addition, Cylance leverages its global threat intelligence to give clients visibility into the evolving threat landscape.

According to Cylance, its key differentiators include using artificial intelligence and machine learning-based pre-execution detections to determine if a file is good or bad based purely on the information in the file itself, and then do that at a sustainable, massive scale. The company believes that the ability to do this across a huge number of samples is important because modern malware creation is automated. In addition, Cylance believes that using these solutions for investigations allows quick response while managing client data privacy concerns. In addition to leveraging machine learning models for binary detection, Cylance is also implementing models within its EDR tool, OPTICS. According to Cylance, this allows it to reduce detection and containment time significantly as a result of the models highlighting the malicious activity for the incident responders.

In its Compromise Assessment engagement which IDC sees as relevant to readiness, response, and resiliency, Cylance looks at these five elements:

- Data exfiltration and sabotage
- Command and control activities

- User account activity
- Malware and persistence mechanisms
- Network, host, and application configurations

Cylance utilizes a methodical approach when performing incident response by a combination of both custom and commercially available tools. Typically, Cylance follows three distinct phases when performing incident response: hunt, investigate, and acquire. These phases overlap the traditional incident escalation workflow in a Security Operation Center:

- Hunt for suspicious behaviors and environmental risks in the environment
- Investigate hosts of interest for threat actor activities
- Acquire and analyze forensic evidence from hosts

The company states that its consultants collect the optimal data sources required to evaluate the environment at each phase. This is because variability in the IT environment and operational requirements prohibit over collection of host event data in time-sensitive matters. And the company further explains that there is a cost to process, store, and analyze endpoint data at scale. Cylance accommodates these issues by providing an appropriate set of collection techniques at each phase. Host event data integrity and fidelity is important in later phases when a smaller set of hosts of interest have been identified. If available, network event sources in the IT environment are correlated with host data.

Cylance offers a full menu of digital forensics and incident response (DFIR) consulting services, ranging from tabletop exercises, IR process and workflow development, IRP development, onsite IR training, SIEM/IR/hunt training, and IR readiness reviews in the top-tier IR retainer packages. The principal of "least data for incident response and compromise assessments" allows the firm to quickly collect data from all hosts in the client environment, parse it into an analysis platform, and employ big data analytics to enable rapid hunting and scoping of incidents.

Cylance believes in encouraging its employees to produce new and innovative tools. Collaboration and peer review during development is also encouraged, which has resulted in a faster development life cycle.

## *Strengths*

Clients believe that Cylance products are "simple to manage and very effective that don't require a complex support process." One client feels that there is a "more personal relationship" with the engineering team as well.

## *Challenges*

One client stated that Cylance will "continue to have room to grow and move into different market spaces with more complex environments that are not as black and white." Environments with a lot of "legacy technology and applications can cause frequent needs for workarounds."

## *Consider Cylance When*

Cylance is a strong technical forensic resource when malware and/or unknown adversaries are in the customer environment. Think of the company for fast global response to large enterprise and government clients.

## DXC Technology

According to IDC analysis, DXC Technology is considered a Major Player in the 2018 IDC MarketScape for U.S. incident readiness, response, and resiliency services – beyond the Big 5 consultancies.

In early 2017, CSC and Hewlett Packard Enterprise (HPE) combined to create DXC Technology, an IT service provider. Throughout that year, DXC consolidated its offerings and platforms for security, blending detection and response capabilities from HPE and workflow, orchestration, and response capabilities from CSC.

Today, DXC offers a range of end-to-end IT and security services. In terms of IR services, DXC follows what it describes as a client need-driven approach. Incident analysis and response services are primarily provided remotely for clients on a 24 x 7 basis. DXC provides remote assistance based on agreed service level, this can be as soon as 15 minutes from call for assistance. In the event that it is determined that onsite presence is required, DXC aims to have specialists onsite as soon as reasonably possible. This model is designed to allow clients and DXC professionals to have the face-to-face time as needed to facilitate the appropriate communications and drive actions associated with successful execution of incident response. Additional consultants can be mobilized to supplement onsite support as well as remote support.

Digital forensics and incident response are delivered via the Flexible Retainer and Base Incident Response models. Both models are designed to provide clients services in computer security incident response support and forensics, log, and malware analysis. Each model is front ended with an IR readiness service, which is delivered via the DXC Enterprise Engagement Process (EEP). The EEP is designed to gain a detailed understanding of the client's existing IT processes, escalation mechanisms, key stakeholders, and critical resources. The EEP is designed to enable clients to leverage DXC's processes, knowledge, and experience in efforts to provide consistency and quality of the implemented technology. Upon completion of the EEP process, the client and DXC are prepared for ongoing DFIR support to be delivered remotely or onsite as client needs dictate.

Within DXC, incident response services are included within security advisory services. DXC is making significant personnel investments in this area, with head count anticipated to grow by nearly 50% during the upcoming fiscal year. This development represents a substantial investment and demonstrates that security is top priority at DXC going forward. In addition, DXC is making multimillion-dollar investments in its threat intelligence and hunting platform – investments that are designed to enable the company to continue its proactive and pre-emptive approach when dealing with incidents.

### *Strengths*

A reference client stated that the DXC Enterprise Engagement Process was very thorough and produced a road map that outlined some "specific concerns they could take to their management and board." The "overall engagement was very good" and covered "a smattering of a lot of things, including policy and incident response management."

### *Challenges*

At the time of the study, DXC did not offer integration into customer response management systems. This appears to be a growing trend, one in which DXC has decided to invest. DXC has been working on an IR management integration with ServiceNow that is near completion.

### *Consider DXC When*

Large enterprises that are looking for readiness and resiliency advisory in addition to incident response should consider partnering with a company such as DXC.

## FireEye

FireEye is positioned as a Leader in the 2018 IDC MarketScape for U.S. incident readiness, response, and resiliency services – beyond the Big 5 consultancies.

FireEye is a security technology and consulting organization with more than 1,000 global security experts in more than 26 countries providing 24 x 7 x 365 coverage from seven global Cyber Threat Operation Centers (CTOCs). Each year, FireEye logs over 100,000 hours on incident response engagements and tracks over 16,000 threats. FireEye's intelligence-led, technology-enabled approach is designed to help organizations prevent, detect, respond, and contain incidents to limit their impact and reduce the risk of future cyberattacks.

The company leverages a combination of commercial FireEye products and custom tools developed by the Mandiant consulting organization. According to FireEye, key differentiators include options for deployment of cloud and on-premise technology of network sensors and endpoint detection and response (EDR) solutions for investigations, which enable rapid response while managing client data privacy concerns. The company says that it can begin investigating a client's network immediately and deploy endpoint forensic technology to examine systems within four hours. In addition, FireEye sources and curates its own threat intelligence with a dedicated team of analysts and researchers that gather intelligence from three proprietary sources:

- Adversary intelligence: More than 160 analysts and researchers in 16 countries monitor worldwide threats and perform targeted intelligence collection operations to provide incident responders with a current view into the threat landscape.
- Machine intelligence: Malware detection from FireEye network devices and endpoint agents deployed globally provide visibility into over 16 million virtual analyses of binaries per hour, giving FireEye visibility into current attack activity. FireEye recently integrated a machine learning malware identification model, called MalwareGuard, into its endpoint agent, an addition that enables the automated identification and containment of malware for which signatures and detection methodologies do not exist.
- Victim intelligence: Over 300 incident responders at the front lines provide insight into the tactics, techniques, and procedures used by attackers in the world's largest cyberattacks.

For incident response services, FireEye provides rapid response and investigation with a customized containment plan based on the attack and remediation plan tailored to the client's environment. Investigations typically identify affected systems, applications, and networks; malicious software and vulnerabilities; and information accessed or exfiltrated. FireEye's approach to incident response involves deploying network and endpoint inspection technology for investigations and applying context from its intelligence sources to provide attribution and motivation into cyberattacks. FireEye provides detailed investigative reports of incident activity and a comprehensive containment, recovery, and remediation plan that includes both tactical and strategic recommendations.

FireEye's incident response retainer includes both dedicated incident response and malware analysis teams that can provide immediate remote support during an incident. The company offers tiers of retainers for various budgets and service-level commitments.

### Strengths

For forensic investigation and malware reverse engineering, Mandiant has been the brand to beat for a long time. In fact, one client stated, "when it comes to doing deep-dive forensics and investigation, they're the best resources available." In addition, locations and availability are very good which enables consistently rapid response.

### Challenges

However, a client with a positive impression of FireEye's technical acumen states "when it comes to exercises that go beyond malware, that's probably an area of relative weakness for them." This client felt that FireEye was "too much into the bits, because that's the bread and butter of what they do" and that management reports can be too granular. However, FireEye has received this feedback and is making strides to raise business-level discussions and reports to a higher ground by expanding its strategic service offerings, including remediation services.

### Consider FireEye When

FireEye is a strong technical forensic resource when advanced persistent threats and/or unknown adversaries are in the customer environment. Think of the company for fast global response to large enterprise and government clients.

## IBM

IBM is positioned as a Leader in the 2018 IDC MarketScape for U.S. incident readiness, response, and resiliency services – beyond the Big 5 consultancies.

IBM, an Armonk, New York-based multinational technology and consulting business, began offering its IR services in 1995. The company's vendor-agnostic incident response services are part of the IBM X-Force Incident Response and Intelligence Services (IRIS) practice. Included under the umbrella of IBM's response and proactive services are a range of offerings: Vision Retainer, Advanced Threat Assessment, IT and analysis, retainers, and IR/CIRT/CSIRT program development and managed detection and response.

IBM offers IR services as part of its security life-cycle approach; also included in the IBM X-Force IRIS portfolio are intelligence services (strategic threat assessment, cyberthreat intelligence workshop, and premium threat intelligence)) and remediation services (breach remediation, strategic remediation and implementation, and agile incident management).

IBM receives IR requests from a 24 x 7 hotline, and each engagement is assigned an engagement manager supported by a primary investigator. Onsite or remote IR teams are assembled based on the client's technology, incident scope, and potential threat factors. Within IRIS, IBM takes a comprehensive approach to team structure. A team is made up of professionals in IR, intelligence services, and remediation. Within the comprehensive teams, IBM has specific roles. Consultants are dedicated purely to client-facing IR engagements and proactive services. Analysts perform malware analysis and reverse engineering. Two intelligence professionals are assigned to every IR engagement – one dedicated to analyzing data from the IR engagement itself in an effort to categorize threats and the other responsible for gathering intelligence that can be used to inform and improve other client engagements.

Recently, IBM has made significant investments in IR team. The company has recruited highly qualified personnel to complement the existing team. These individuals have experience and expertise

in IR, threat intelligence, and remediation who were brought on board to supplement IBM's existing capabilities and subsequently build out the competency of the team out.

According to IBM, plans are in place designed to improve response speed among cyberincident-first responders who are trained on initial triage and evidence collection. IBM intends to make its X-Force services a major focus area. The company will continue to emphasize strong alignment of IR and intelligence services to the X-Force brand and partner with its application security, resilient, and GTS offerings. New and enhanced offerings in the coming months include X-Force IRIS Active Threat Assessment and X-Force IRIS Vision Retainer.

### *Strengths*

According to IBM, the company's IBM X-Force IRIS uses a hub and spoke model where consultants, analysts, and researchers are deployed throughout the globe and centrally supported by experts like malware analysts, threat intelligence analysts, and researchers.

This organizational structure of its incident response team streamlines response to customer emergencies or proactive needs within their particular geography. A formal Client Experience platform is engaged for customer satisfaction and IBM has plans to build an iterative feedback loop.

### *Challenges*

Customers expressed strong satisfaction with IBM's incident response capabilities level of engagement and high-touch experience with responders.

### *Consider IBM When*

Large enterprises that are looking for capabilities that go beyond traditional incident response offerings and need assistance with security transformation should consider partnering with a company such as IBM.

## McAfee

McAfee Professional Services, Foundstone Consulting, is positioned as a Major Player in the 2018 IDC MarketScape for U.S. incident readiness, response, and resiliency services – beyond the Big 5 consultancies.

McAfee Foundstone offers professional and strategic security solutions to help organizations maintain a strong security posture. The company touts that it assists its clients to balance the strategic benefits of business consulting with a tactical, hands-on approach to technology consulting and security training. Specifically, McAfee provides the following strategic consulting services in addition or adjacent to its incident response offerings:

- Risk management
- Privacy, compliance, and data protection
- Security program and operations development
- Incident response and IR program development
- Strategic and operational threat intelligence/research
- Operational and integrated architectures
- Tactical consulting on software and application security services and network and infrastructure security

- Training on software security development
- Assessments and certification programs

McAfee consultants believe that the Security Engagement management Process (SEP) provide a pivotal differentiator to its clients as it includes continual communication to ensure the success of the engagements. Foundstone offers a Forensics and Incident Response Education (FIRE) course help incident response clients normalize their environment after a negative event has occurred. Forensic techniques to identify, respond to, and recover from both an insider and outsider attack are core to the curriculum. This comprehensive, technically detailed course enables participants to reinforce security posture or to become more "resilient," which is a core tenet of this IDC MarketScape.

The company's incident response and professional services are available globally through a presence in all major theatres (North America [NA], EMEA, Asia/Pacific [APAC], Japan, LA).

### *Strengths*

IDC finds the Security Engagement management Process and the Forensics and Incident Response Education training course compelling.

### *Challenges*

McAfee is behind other service providers in its acquisition and retention strategy for employees. While it requires reskilling and training to enhance responder certification levels, the company does not go above and beyond to develop curriculum with universities or to drive internships as some other providers do. In this competitive market where security talent is so difficult to acquire, it is imperative to think outside the box and do everything possible to acquire and retain talent.

### *Consider McAfee When*

Large enterprises that seek a global security professional services firm offering a range of readiness, response, and resiliency programs would do well to contact McAfee.

## NTT

NTT is positioned as a Major Player in the 2018 IDC MarketScape for U.S. incident readiness, response, and resiliency services – beyond the Big 5 consultancies.

NTT Group covers 87 countries and consists of 244 datacenters and 241,000 employees. NTT is headquartered in Tokyo, with regional headquarters for North America, Europe, and the Asia/Pacific region. NTT brings together the security-specific resources and delivery capabilities across the group.

NTT Security was established in 2016 as the specialized security company of the NTT Group, embedding managed and consulting services into the wider solutions of NTT Group companies of Dimension Data, NTT Communications, and NTT DATA worldwide. NTT Security has multiple SOCs, R&D centers, and over 1,500 security experts that handles hundreds of thousands of security incidents annually across six continents. NTT Security services are sold via the NTT Group companies of Dimension Data, NTT Communications, and NTT DATA.

The company's mission is to secure the foundation of a connected society by embedding cybersecurity in digital transformation initiatives. Its approach is to work closely with clients to understand their organization and implement the right cybersecurity controls to meet their needs. NTT's incident

response can be combined with the company's other cybersecurity offerings such as managed security services.

### *Strengths*

NTT allows an organization to convert retainer hours at the end of the contract to a broad set of resiliency services which provides additional value when the client hasn't needed to exercise response services. A benefit of using NTT's proactive services is that the NTT analyst that does the assessment of an organization's incident response program will most likely be the analyst that will respond if they have a breach, which provides the client with a level of advance familiarity and can speed up the response.

### *Challenges*

NTT is still sorting through integration issues internally between its operating companies and centralized security offerings. In addition, the firm has been criticized for challenges for inconsistent log management services. Specific to incident response, readiness, and resiliency, the company has not received criticism.

### *Consider NTT When*

Midsize and enterprise organizations of 500–5,000+ employees that are seeking a partner with complex multi-geography capabilities should look at a company such as NTT.

## Optiv

Optiv is positioned as a Major Player in the 2018 IDC MarketScape for U.S. incident readiness, response, and resiliency services – beyond the Big 5 consultancies.

Optiv is a privately owned provider of end-to-end cybersecurity services based in Denver. Since 2002, Optiv has been providing IR services aimed at preventing and responding to large-scale attacks and intrusions of all types. The company's incident responders, investigators, and malware reverse engineers help prepare clients for an incident, identify attacks, uncover indicators of compromise, provide guidance to reduce attack surface, and respond to incidents should they occur.

As part of providing access in times of need, Optiv offers its Incident Response Retainer, a service designed to ensure that Optiv expertise is available only a phone call away. The Incident Response Retainer is an annual agreement for services designed to help make clients more resilient in the face of attack. The retainer also provides a pre-negotiated set of hours that can be activated if an incident occurs. Once an Incident Response Retainer is in place, clients can have all the necessary contracts and nondisclosure agreements in advance, saving valuable time in the event of an investigation or incident response need. Optiv offers various levels of retainer and different levels include custom SLAs and available IR hours for use.

The company touts the following benefits of this retainer program:

- Pre-negotiated contractual terms and conditions in place that provide peace of mind
- The time saving due to agreements arranged in advance
- Access to Optiv's incident responders, investigators, and malware engineers
- Use of first-class tools in the industry as well as Optiv's proprietary database of malware signatures and viruses

- Guaranteed discounted rates for service should the need to investigate arise
- Proactive services that can help prevent a compromise from occurring and make clients more resilient in the face of an incident

Optiv has a five-step approach to delivering its IR services. Each step includes numerous activities with major service deliverables: assess (includes real-time insight into incidents), collect (includes gathering evidence of an attack), analyze (includes determining attack vector, establishing timelines, and providing senior executives with next steps), investigate (includes tracking and documenting all findings), and remediate (includes developing action plans and recommendations).

Over the next 12–18 months, Optiv plans to expand its services by including deep/dark web threat intelligence searches for specific engagements. In some cases, Optiv also plans to bring in its risk and compliance team as a follow-on for those clients that may not fully understand their risks. Optiv also is working on a process that would allow the company to quickly pull in any subject matter experts among its technology and partner ecosystems if such expertise is needed for an IR engagement.

### *Strengths*

Optiv's onsite "Enterprise Incident Management" (EIM) workshop is recognized for providing a breadth of incident readiness capabilities such as tabletop exercise workshop tests, an organization's incident plan and playbook, and to review the maturity of each functional component within an enterprise incident management program structure. In addition, 100% of unused retainer dollars can be used toward other EIM offerings.

Optiv has also done a good job at going above and beyond to address its customer's needs, which has not been typical with other providers.

### *Challenges*

Optiv's corporate marketing programs are immature and future plans include the development of a formal customer experience program and processes for integrating customer feedback from incident response engagements for improved future offerings. In addition, Optiv could broaden talent acquisition and retention programs to include partnerships with universities and the development of curriculum.

### *Consider Optiv When*

Optiv is an eager and motivated service provider desirous of capturing share in this arena. The skills the company offers are good and while marketing and talent programs need some time to develop the technical skills are present for incident response.

## Rapid7

Rapid7 is positioned as a Leader in the 2018 IDC MarketScape for U.S. incident readiness, response, and resiliency services – beyond the Big 5 consultancies.

Rapid7 is a provider of software security and services based in Boston, Massachusetts. The company's consultants have investigated hundreds of compromises of all sizes and severity. The teams offer a combination of backgrounds in threat intelligence, host and network forensics, security operations, and malware analysis; they work with their customers' technology and, when existing tools are not sufficient, they have partnerships with technology providers to deploy tools for rapid analysis and incident scoping.

The company offers incident response services designed to provide clients with access to the experience and technical expertise needed to accelerate incident investigation and containment. The incident response services include all proactive aspects of a successful detection and response program, and the reactive elements that entail rapid response, scoping, and guidance through remediation activities. Rapid7's teams work with client's in-house teams throughout every stage of incident response, including post-incident activities and program improvement.

Rapid7 aims to provide a single point of contact for clients from initial response through remediation and cleanup. This contact is ultimately responsible for coordinating, communicating, and reporting on every aspect of incident response activity.

Incident response retainers provide clients with the ability to engage skilled personnel rapidly in the event of a compromise. Clients experiencing an incident will be assisted by an engagement manager within one hour to plan an approach. Within 24 hours, Rapid7 begins remote technical work in investigating the compromise; onsite investigations begin within 48 hours. Rapid7 promotes its approach as going beyond traditional retainers – clients can convert their pre-purchased hours for the purposes of evaluating their business, existing capabilities, and classification of relevant assets, users, and data.

Rapid7 's incident response is designed to provide valuable insight that inform and advance all of its IR services while at the same time ensure greater success for individual clients. The activities include incident management, detection and analysis, scoping, regular status reports and communications, and guidance for remediation and cleanup. As for specific proactive and reactive IR services, Rapid7 offers breach response, compromise assessments, breach readiness assessments, tabletop exercises, IR program development, and a variety of blended and custom engagements.

Rapid7 touts its ability to tailor offerings to the specific needs of its clients and can even partner with experts from other teams within the company – including Penetration Testing and Advisory Services – to run blended engagements and full-scope assessments of security programs. In a similar vein, Rapid7 works with the controls a client has in place during threat simulations (live and tabletop based) to effectively measure the response relative to the environment. In addition, since each industry is subject to different threats and regulatory requirements, Rapid7 takes that into consideration when creating the scenarios and response analysis.

## *Strengths*

A customer state that "they've done a CSMA (cybersecurity maturity assessment)" with Rapid7 that was "a very thorough evaluation and reporting." They "like the [company's] expertise and do a really good job responding quickly when issues arise."

## *Challenges*

One customer stated that "sometimes communication can be disjointed and because of acquisitions, Rapid7 can seem 'siloed' but that the initial sales person has really helped" navigate the company. Another stated that there have been "some challenges around project management."

## *Consider Rapid7 When*

Focused more on the small to midsize companies, Rapid7 provides templatized assessments, customized tabletop, and incident response challenge exercises and a full breadth of incident response services.

## RSA

RSA is positioned as a Major Player in the 2018 IDC MarketScape for U.S. incident readiness, response, and resiliency services – beyond the Big 5 consultancies.

RSA is a global security technology and service company providing more than 30,000 customers around the world with security capabilities to protect their assets and environment from cyberthreats.

The RSA global Incident Response Practice provides a portfolio of services that include incident response retainers, proactive incident discovery/compromise assessment, and knowledge transfer services. Proactive and rapid response services include:

IR Retainers. RSA offers a portfolio of retainer services which provide for the proactive engagement of the RSA IR team and response to incidents within hours. Deliverables include a Preliminary Analysis Report, which scopes the nature of the incident and provides recommendations for next steps and remediation.

- **IR Discovery.** The IR team uses the RSA NetWitness Platform to proactively hunt for indications of adversary activity. Deliverables include a Findings Report that provides remediation recommendations for any threats that have been identified.
- **IR Response.** This service provides rapid access to IR expert "boots on the ground" when attack activities are suspected. Deliverables include a Findings Report that highlights the scope and nature of the incident and provides recommendations for next steps and remediation.
- **IR Jumpstart for Analytic Intelligence and Subscription services.** These services enable customers of the RSA NetWitness Platform to optimize their product investments by working hand in hand with the RSA IR team to conduct proactive "hunting" and analysis activities.

RSA uses a framework for data forensics and incident response that takes into consideration data from multiple sources including in-house systems, open source research, and threat intelligence sources. In addition, the approach includes network analysis, host forensics, and malware analysis. In addition to the services outlined previously, education services are available from RSA University, and product maintenance and personalized support services are available from RSA Customer Support.

### *Strengths*

RSA's standout proficiencies are the company's account management and customer retention strategy.

### *Challenges*

RSA provided little information about future road map initiatives regarding its investment strategy and the future acquisition and retention of security talent. That said, the company has a strong history of innovation and investment into its security tools and services.

### *Consider RSA When*

Large enterprises that seek a global security professional technology and services firm offering a range of readiness, response, and resiliency programs would do well to contact RSA.

## Secureworks

Secureworks is positioned as a Leader in the 2018 IDC MarketScape for U.S. incident readiness, response, and resiliency services – beyond the Big 5 consultancies.

Secureworks is one of the few pure-play vendors in the current security services marketplace. The vendor offers a comprehensive list of security services, including incident response services, threat intelligence services, security and risk consulting, and managed security services. Since 2007, Secureworks has been offering dedicated IR services. Although IR services rely heavily on quality human resources, Secureworks has also realized the importance of automation in IR service delivery. At present, Secureworks is already automating portions of the sensing and sense-making phases of online host inspection. The vendor is planning to enhance its IR workflow management systems with more automation and add more self-service mechanisms for clients. On the analytics side, almost all advanced security analytics are delivered by Secureworks itself, including its own Red Cloak advanced endpoint analytics.

The Secureworks Counter Threat Platform (CTP) leverages both proprietary and third-party technology. The platform utilizes predictive technology that consists of artificial intelligence and machine learning to address threats in an automated rapid response. The Counter Threat Unit (CTU) research team and the Senior Intrusion Analyst (SIA) team use proprietary tools, including a very large database, to monitor the global threat landscape and analyze emerging threats and vulnerabilities.

Secureworks continues to research and provide advanced threat prevention and detection tools such as sandboxing and endpoint threat prevention, as well as detection and response tools. Secureworks' strategy is to use machine learning and behavioral analytics that can decrease the impact on human analysts by analyzing telemetry collected in a fast and automated process, which in turn can provide quicker response time.

In incident response services, Secureworks has a low cost of entry for clients with on-demand contracts that feature a minimal financial commitment to initiate IR services. Separately, a lot more clients engage with Secureworks Security Risk and Consulting (SRC) to help develop business plans through information security audits and risk assessments. Over 70% of SRC clients turn into MSS or retainer-based IR clients as a result of these engagements.

### *Strengths*

A Secureworks customer that had engaged the service provider using unused retainer hours for a tabletop exercise stated it was a "very customized exercise. They used terms and companies we had to deal with. It was more unique than a stack of PPT. They also had a different team come down and give us forensic evidence training for our IT department" which was "very technical and customized for us." In fact, Secureworks was rated quite well by customer references. In addition, IDC feels that Secureworks' containment readiness planning process is quite comprehensive across the client's operational, business, and future resilience elements.

### *Challenges*

A negative from one customer was "still kind of pricey, so getting something out of it from the retainer is good. You get what you pay for and it's nice to have the insurance."

### *Consider Secureworks When*

Companies of all sizes seeking a managed security service provider with deep integration between its detection, response, and ongoing day-to-day management should consider Secureworks.

## Stroz Friedberg

Stroz Friedberg's Digital Forensics and Incident Response Services (part of Aon's Cyber Solutions) is positioned as a Leader in the 2018 IDC MarketScape for U.S. incident readiness, response, and resiliency services – beyond the Big 5 consultancies.

Aon's Cyber Solutions combines the services of digital risk management firm Stroz Friedberg with Aon's Professional Risk Solutions and Global Risk Consulting practice. As an integrated entity, Cyber Solutions specializes in holistic cyber-risk management. Its areas of focus include digital forensics, incident response, and proactive cybersecurity services; cyberinsurance and risk quantification; cyberinvestigation; and eDiscovery.

Following Stroz Friedberg's acquisition by Aon, the company is positioned to offer a complete set of cybersecurity services, from assessment, testing, and improvement of an organization's security posture to incident response, quantification, and transfer services. The company's solutions include approximately 50 specific services from red team testing, to forensically sound incident response that holds up in litigation, to ongoing scanning of a client's environment to ensure breaches are contained, to peer review and preparation (GC/QA) and expert witness testimony that can help mitigate regulatory fines and lawsuits, to claims preparation and advocacy to maximize economic recovery from an insurance carrier.

Stroz Friedberg's Digital Forensics and Incident Response professionals work with Fortune 100 companies, 80% of the AmLaw 100, and the top 20 U.K. law firms to solve complex cyber-risk challenges. The firm's approach to incident response relies on proprietary and agnostic tools and creating defensible evidence preservation and chain of custody.

### *Strengths*

Retainer hours can be used right away for almost any proactive or reactive service, except expert witness testimony and clients can purchase additional hours at the same blended rate at any time during the contract, which gives additional budgeting certainty and flexibility. One customer stated that Stroz Friedberg's communication was "excellent." He also stated that they "almost overcommunicating," and that the program/project manager was involved in every call, updating every group within company.

### *Challenges*

Today, the company does not provide cyber range services but will do so in the future. The only negative from a customer was that Stroz Friedberg's services are not inexpensive, but the firm is rapidly developing a number of new offerings aimed at the midmarket. Customer service is not formalized into a program today, but perhaps with the acquisition by Aon, it will be in the future.

### *Consider Stroz Friedberg When*

Large enterprises looking for legal expert witness representation and experience with the law enforcement community would do well to consider Stroz Friedberg.

## Symantec

Symantec is positioned as a Leader in the 2018 IDC MarketScape for U.S. incident readiness, response, and resiliency services – beyond the Big 5 consultancies.

Symantec is a global provider in cybersecurity, providing security software and services to help organizations, governments, and people secure their most important data wherever it lives. Symantec has more than 11,000 employees and operates in more than 35 countries around the globe.

In 2015, Symantec deployed a global incident response service, which engaged more than 120 customers within a year of its launch. Symantec's incident response is part of the cybersecurity services portfolio that includes in-depth offerings covering the full attack life cycle by providing services for before, during, and after an attack. Symantec advocates integration of its incident response services within cybersecurity services to fuel an organization's cybersecurity program with better insight, faster detection, and response capabilities. The pillars of this claim are DeepSight Intelligence services to track and analyze adversary groups, key trends, and events around the globe; Symantec's managed security services for 24 x 7 continual threat detection; and incident response services for rapid response, strategic planning, and advanced threat hunting.

A unique aspect of Symantec's IR service is the company's base retainer embedded within the managed security services offering with which all MSS clients receive as a basic level of incident response, inclusive of terms and conditions (T&Cs) and SLAs.

### *Strengths*

As of July 2017, all MSS agreements include incident response base terms and conditions providing customers the IR retainer for free (zero dollar), which includes IR-specific terms and conditions, call back SLA of 3 hours, remote assistance SLA of 12 hours, and lower list price on additional retainer response time if needed. IDC considers this a future trend and advanced within MSSPs. One customer stated that Symantec did a "phenomenal job sharing best practices and the resources on the ground kept abreast of what was going on." This client appreciated the "entire process and how Symantec approached it." Another client engaged Symantec for tabletop exercise and found it "very concise and cohesive" and stated that Symantec was willing "to answer questions after the exercises."

### *Challenges*

Asked what a client would like to change about Symantec as an incident responder, they stated "focus more efforts on conclusion deliverables which were a little rough at the end." Another client commented that remaining retainer which was used engaging Symantec for a tabletop exercise was unclear how it translated into hours or days and "was not straightforward" and that travel expenses were not taken out of the retainer. They also stated this was a "minor" feedback.

### *Consider Symantec When*

Large enterprises should consider engaging Symantec for retainer, readiness services, and response and advanced threat hunting when looking for an MSSP with low pricing and flexible retainers and for a provider with a uniquely embedded zero-dollar retainer within the managed security service.

## Trustwave

Trustwave is positioned as a Leader in the 2018 IDC MarketScape for U.S. incident readiness, response, and resiliency services – beyond the Big 5 consultancies.

Trustwave is a cybersecurity and managed security services provider that has a strong history and foothold in the compliance market. Through the cloud-based TrustKeeper platform, which boasts more than three million enrollees, Trustwave offers automated and cost-effective data protection, risk management, and threat intelligence to its customers. Customers range from small to midsize companies as well as distributed enterprises that need to be in compliance with various regulations.

Trustwave's incident response and readiness program (IRRP) provides 24 x 7 global expert response with flexible hours, IR assessment to determine current incident response maturity level, and risk assessments to identify the client's ideal state. Typically, multiyear strategic plans are developed to help the client achieve a 4-hour remote and 24-hour onsite SLA, if required. Training, plans, and playbooks are all customized to individual client requirements.

Trustwave goes through a 10-point plan in its IRP:

- IR assessment to assess the infrastructure and processes against security incident readiness
- Development of computer security incident response plans, playbooks, templates, and procedures
- Security fundamentals, incident response, and advanced forensics/malware analysis training
- Team development and analysis of the roles of IR team
- First-incident responder advanced technical training for IR team
- Tabletop exercises for decision making and to build procedural exercises in order to digest the IR plan and review the processes
- Attack simulations/purple teaming scenarios that simulate real attacks or run live-fire exercises to test people, technology, and procedure readiness under real incidents
- Project close/review and deliverables to customer
- Annual repeated review of tabletop exercises and existing plan
- IR Retainer at reduced rate for any incident that may arise during the contract, if no incident hours may be substituted for other services

## *Strengths*

The Trustwave project update report provides clear update and very clear insight into the number of hours remaining in the retainer. One customer stated that it, "couldn't speak higher of [Trustwave personnel] and of the speed with which Trustwave responded." This customer rated Trustwave highly because it'd "never had a provider respond so quickly and their technical expertise was incredible."

Another customer mentioned that "account management has been fantastic and Trustwave is very communicative. They do a great job of listening to your needs. Any time we've used their services they are extremely responsive. They want to solve the problem and are not just watching the clock."

## *Challenges*

A customer stated that Trustwave's "tabletop exercises are about average compared to others in the marketplace." Trustwave does not have plans for offering integration into customer response management systems. This appears to be a growing trend which Trustwave might wish to consider.

## *Consider Trustwave When*

Small to midsize companies and distributed enterprises that have tight compliance restrictions should look at partnering with a company such as Trustwave.

## Verizon

Verizon is positioned as a Leader in the 2018 IDC MarketScape for U.S. incident readiness, response, and resiliency services – beyond the Big 5 consultancies.

Verizon is a New York-based telecommunications company that offers a breadth of security services to enterprises across the globe. The security business stands within the Verizon Enterprise Solutions business unit within its wireline business that provides business and government customers with communications products and enhanced services, including broadband data and video, corporate networking solutions, datacenter and cloud services, security and managed network services, and local and long-distance voice services.

Known for its Data Breach Investigation Report (DBIR) and undisputed strength in threat intelligence and threat hunting, the company leverages this visibility in a multitude of offerings from readiness, response to resiliency services. Data is collected and analyzed from its network backbone, its MSS engine, the Verizon Threat Research Advisory Center (VTRAC), Vocabulary for Event Recording and Incident Sharing (VERIS) framework, and research/threat hunting.

The Verizon Threat Research Advisory Center Investigative Response Team boasts 300+ full-time team members across the globe providing incident response coverage in 100+ countries and is one of the largest non-military IT investigations companies in the world. Verizon conducted 500+ IT investigations last year and was retained to investigate 9 of the 11 largest data breaches on record. The team members possess an average of 14 years of IT investigations experience and the company has digital forensics labs in the Americas, APAC, and EMEA.

### *Strengths*

The company assessed favorably overall. Key areas of strength are the firms' framework and methodology used in response, access to all complementary readiness and resiliency services, and very detailed checklists and reports during assessment and response. Verizon continues to innovate and enhance its security service offerings to stay current and ahead of the breach readiness, response, and resiliency market.

### *Challenges*

One customer rated Verizon in the middle of the scale for "onsite training," which didn't give guidance on how to do better or improve. The customer expected/assumed this. The company stated, "recommendations were not in scope of delivery" and the customer felt it was "odd to not include lessons learned and improvements just on a cursory level."

### *Consider Verizon When*

IDC recommends large enterprises looking for a global security provider with a span of capabilities and consulting services should consider Verizon.

## Wipro

Wipro is positioned as a Major Player in the 2018 IDC MarketScape for U.S. incident readiness, response, and resiliency services – beyond the Big 5 consultancies.

Wipro provides a span of security and consulting offerings to large enterprises across the globe. Wipro is headquartered in Bangalore, India. Wipro has 10 security platforms that support a vendor-agnostic approach to services.

Wipro's Cyber Incident Response team addresses core areas that apply to different cyberevents around situation awareness (including understanding potential breadth and scale of the incident and identifying locations of potentially compromised systems) and damage assessment (including focusing on ascertaining the data accessed or exposed and understanding what relevant issues will need to be addressed in future actions).

Wipro engages clients in Strategic Total Outsourcing Services (STOS) engagements where Wipro is responsible for end-to-end IT services provided for clients. At the onset of engagements, Wipro benchmarks the clients' existing security response policy, processes, and the interlocks with various stakeholders to ensure that good practices are instilled in the beginning of engagements. In STOS engagements, Wipro is accountable for providing end-to-end incident response services including both eradication and remediation services. By the virtue of this commitment, Wipro owns SLAs around restorations of services.

In the current STOS engagements where Wipro supports IR, typically the IT help desk and SOC services provide the 24 x 7 manned hotline for IR services. In addition, Wipro's Technical Support Group is available 24 x 7 for providing incident response support services across engagements. At a minimum, IR responses will include a team lead and a forensic/log analysis expert. Wipro recognizes that it's becoming more difficult to make the talent located in India available at client sites worldwide in a timely manner during incidents. Over the next 12–18 months, Wipro plans to increase the number of skilled incident staffers locally throughout its geographic regions beyond India. Within the past 12 months, Wipro has been able to expand its consulting pool of local onsite resources by upward of 50 staffers. According to the company, this expansion reflects the company's continued focus to build similar skill sets across the board, specifically around threat management.

In its ongoing efforts to be more efficient, Wipro uses Demisto for implementing security incident orchestration as well as the IBM Resilient Incident Response Platform for centralized management of various activities associated with security incident management. With the threat scenario only expanding combined with the shortage of skills, Wipro anticipates the need for increased support from third parties specifically around incident response.

For IR consulting services, customers prefer fixed price engagements. In the next 12–18 months, Wipro plans to introduce retainer IR services. As part of the introduction of these services, Wipro plans to roll out a 24 x 7 manned IR hotline for its retainer clients.

## *Strengths*

According to a customer interviewed, Wipro provided "staff augmentation" and were "very professional," provided a "global view," and "communicated a lot with suggestions and what to do" in the crisis.

## *Challenges*

Depth of insight into Wipro's framework and methodology were not provided. In addition, the company has fewer customer retention activities than others including not providing a dedicated customer account manager. Providing a dedicated account manager is a trend in the marketplace and it would benefit Wipro to consider adding such a role.

### *Consider Wipro When*

Consider Wipro for large Strategic Total Outsourcing Services engagements in which Wipro benchmarks the clients' existing security response policy, processes, and the interlocks with various stakeholders to ensure that good practices are instilled in the beginning of engagements.

## APPENDIX

## Reading an IDC MarketScape Graph

For the purposes of this analysis, IDC divided potential key measures for success into two primary categories: capabilities and strategies.

Positioning on the y-axis reflects the vendor's current capabilities and menu of services and how well aligned the vendor is to customer needs. The capabilities category focuses on the capabilities of the company and product today, here and now. Under this category, IDC analysts will look at how well a vendor is building/delivering capabilities that enable it to execute its chosen strategy in the market.

Positioning on the x-axis, or strategies axis, indicates how well the vendor's future strategy aligns with what customers will require in three to five years. The strategies category focuses on high-level decisions and underlying assumptions about offerings, customer segments, and business and go-to-market plans for the next three to five years.

The size of the individual vendor markers in the IDC MarketScape represents the relative market share of each individual vendor within the specific market segment being assessed.

## IDC MarketScape Methodology

IDC MarketScape criteria selection, weightings, and vendor scores represent well-researched IDC judgment about the market and specific vendors. IDC analysts tailor the range of standard characteristics by which vendors are measured through structured discussions, surveys, and interviews with market leaders, participants, and end users. Market weightings are based on user interviews, buyer surveys, and the input of IDC experts in each market. IDC analysts base individual vendor scores, and ultimately vendor positions on the IDC MarketScape, on detailed surveys and interviews with the vendors, publicly available information, and end-user experiences in an effort to provide an accurate and consistent assessment of each vendor's characteristics, behavior, and capability.

## Market Definition

Breach or incident response planning aims to help organizations prepare to act in the case of security breach or attack by putting in place organized procedures to manage the effect of a breach in the event of such a security incident. The objective is to limit the damage of the security incident and reduce recovery time and costs through the prompt identification, isolation, and eradication of the problem. Incident response readiness or planning sets policies that define what is considered as an attack and also puts in place a well-defined, step-by-step process to be followed in case of an incident. Incident resiliency aims to continue the improvement trajectory set out during readiness and response.

## Strategies and Capabilities Criteria

This section outlines the characteristics IDC believes technology buyers must take into consideration when making a purchase decision related to incident response. The factors are weighted because IDC

believes that some are more important than others in maximizing opportunity and realizing market success (see Tables 2 and 3).

## TABLE 2

### Key Strategy Measures for Success: U.S. Incident Readiness, Response, and Resiliency Services — Beyond the Big 5 Consultancies

| Strategies Criteria | Definition | Weight (%) |
|---|---|---|
| Customer service | Providers plan to use numerous methods to measure customer satisfaction. | 21.00 |
| | Providers plan to have dedicated account managers for customer retention purposes. | |
| | Providers plan to have a clear procedure for sharing customer service feedback with customers and partners. | |
| | Providers can describe in detail their future process for tracking planned customer service improvements and validating them with customers. | |
| | Providers can describe in detail specific plans to increase the consistency and repeatability of customer service delivery in the future. | |
| Delivery | Providers describe their future internal organizational structure for incident response team(s) in detail and explain why it supports superior service delivery. | 20.00 |
| | Providers describe their future criteria (e.g., NIST SP 800-61r2 3.3.1), which ideally reflect a situational response to keeping the business running based on nature of incident, sophistication, and motives. | |
| | Providers have plans to integrate with their customers' response management systems. | |
| | Providers plan to have a defined, repeatable framework/methodology for delivering incident response services. | |
| | Providers plan to have a strategy for creating incident response teams that enables fast, efficient dispatch. | |
| Employees | Providers articulate their future strategies and tactics for attracting and hiring talent. | 20.00 |
| | Providers describe the strategies and tactics they plan to use in the future to motivate and retain talent. | |
| | Providers describe the methods they plan to use in the future to educate, reskill, and certify their employees. | |
| | Providers describe the standards and/or best practices they expect to use in the future to evaluate the breadth and depth of their incident response services delivery people. | |
| Functionality or offering | Providers plan to offer the full spectrum of policy creation services according to NIST SP 800-61r2 2.3. | 12.00 |

## TABLE 2

### Key Strategy Measures for Success: U.S. Incident Readiness, Response, and Resiliency Services — Beyond the Big 5 Consultancies

| Strategies Criteria | Definition | Weight (%) |
|---|---|---|
| | Providers plan to offer the full spectrum of plan creation services according to NIST SP 800-61r2 2.3.2. | |
| | Providers plan to offer diverse methods of incident response plan and capability testing. | |
| | Providers plan to include threat intelligence in their incident response service delivery, along with broad visibility of customers' environments. | |
| Growth | Providers plan to employ numerous activities designed to retain customers. | 5.00 |
| Innovation/R&D strategy and R&D activities | Providers plan to pursue various innovation | 10.00 |
| | Providers can describe planned, future incident response services innovations. | |
| Marketing | Providers plan to use numerous marketing tactics to promote their businesses. | 1.00 |
| Portfolio | Providers invest in multiple areas of their businesses to help them lower delivery costs, increase customer value, improve profitability, and remain competitive. | 9.00 |
| | Providers have plans to improve service-level agreements (SLAs) related to retainer business. | |
| | Providers have future plans to examine multiple elements within their delivery process during postmortems (e.g., NIST SP 800-61r2 3.4.2). | |
| Sales and distribution | Providers plan to improve incident response service delivery through a well-reasoned sales/distribution strategy. | 2.00 |
| Total | | 100.00 |

Source: IDC, 2018

## TABLE 3

### Key Capability Measures for Success: U.S. Incident Readiness, Response, and Resiliency Services — Beyond the Big 5 Consultancies

| Capabilities Criteria | Definition | Weight (%) |
|---|---|---|
| Cost competitiveness and management | Providers manage costs with attention to delivery, profitability, customer value, and competitive stance. | 2.00 |
| | Providers use a variety of tools to help customers with purchase decision. | |
| Customer service | Providers have a formal customer experience program. | 16.00 |
| | Providers use numerous methods to measure customer satisfaction. | |
| | Providers assign dedicated account managers for customer retention purposes. | |
| | Providers employ numerous activities designed to retain customers. | |
| | Providers have a clear procedure for sharing customer service feedback with customers and partners. | |
| | Providers can describe in detail their process for tracking planned customer service improvements and validating them with customers. | |
| Delivery | Providers use incident handling checklist(s) (e.g., NIST SP 800-61r2 3.5). | 22.00 |
| | Providers use a standard list of items and/or issues (e.g., NIST SP 800-61r2 3.2.5) that they track during each engagement. | |
| | Providers are able to integrate with their customers' response management systems. | |
| | Providers have a defined, repeatable framework/methodology for delivering incident response services. | |
| | Providers follow a comprehensive set of steps to analyze, scope, and validate each incident (e.g., NIST SP 800-61r2 3.2.4). | |
| | Providers use standard templates to ensure consistency and use ad hoc templates when appropriate. | |
| | Providers have a clear process or plan for working with customers that choose to do their own eradication and/or remediation. | |
| | Providers have a strategy for creating incident response teams that enables fast, efficient dispatch. | |
| | Providers describe their criteria (e.g., NIST SP 800-61r2 3.3.1), which ideally reflect a situational response to keeping the business running based on nature of incident, sophistication, and motives. | |

## TABLE 3

### Key Capability Measures for Success: U.S. Incident Readiness, Response, and Resiliency Services — Beyond the Big 5 Consultancies

| Capabilities Criteria | Definition | Weight (%) |
|---|---|---|
| Employee management | Providers describe their internal organizational structure for incident response team(s) in detail and explain why it supports superior service delivery. | 14.00 |
| | Providers articulate their strategies and tactics for attracting and hiring talent. | |
| | Providers describe the strategies and tactics they use to motivate and retain talent. | |
| | Providers describe their methods of educating, reskilling, and certifying employees. | |
| | Providers describe the standards and/or best practices they use to evaluate the breadth and depth of their incident response services delivery people. | |
| Functionality or offering | Providers offer the full spectrum of policy creation services according to NIST SP 800-61r2 2.3.2. | 14.00 |
| | Providers offer a robust set of core and complementary consulting and adjacent security services. | |
| | Providers offer essential incident response services related to detection and vulnerability remediation. | |
| | Providers offer the full spectrum of policy creation services according to NIST SP 800-61 2.3. | |
| | Providers offer diverse methods of incident response plan and capability testing. | |
| | Providers include threat intelligence in their incident response service delivery, along with broad visibility of customers' environments. | |
| Growth execution | Providers are growing at a rate comparable with the average growth rate of study participants. | 3.00 |
| Innovation/R&D | Providers pursue various innovation and R&D activities. | 6.00 |
| | Providers describe recent incident response services innovations. | |
| Marketing | Providers describe the effectiveness and outcomes of their marketing strategies by target market segment. | 3.00 |
| | Providers employ numerous marketing tactics to promote their businesses. | |
| | Providers articulate their marketing strategies related to each target market segment. | |

## TABLE 3

### Key Capability Measures for Success: U.S. Incident Readiness, Response, and Resiliency Services — Beyond the Big 5 Consultancies

| Capabilities Criteria | Definition | Weight (%) |
|---|---|---|
| Portfolio benefits | Providers use a variety of software tools to aid incident response speed and effectiveness. | 16.00 |
| | Providers offer an incident response hotline that is staffed 24 x 7. | |
| | Providers assign a dedicated account or engagement manager who serves as first point of contact for incident notification. | |
| | Providers demonstrate flexibility in SLA offerings. | |
| | Providers offer multiple services designed to help their customers "close the loop" and improve security resiliency. | |
| | Providers conduct post-incident internal postmortems to identify improvements to service delivery (e.g., NIST SP 800-61r2 3.4.2). | |
| | Providers examine multiple elements within their delivery process during postmortems (e.g., NIST SP 800-61r2 3.4.2). | |
| | Providers have a clear process for making improvements identified in postmortems and integrating them into standard operating procedures. | |
| Pricing model | Providers allow customers to apply unused retainer dollars toward other services. | 3.00 |
| Sales and distribution | Providers minimize or exclude the use of partners for incident response delivery. | 1.00 |
| Total | | 100.00 |

Source: IDC, 2018

## LEARN MORE

### Related Research

- *IDC's Worldwide Security Products Taxonomy, 2018* (IDC #US43535614, February 2018)
- *Worldwide Data Loss Prevention and Classification Market Shares, 2016: Cloud Disruption Ahead* (IDC #US43408717, January 2018)
- *Meltdown, Spectre Attack Dangers Require Careful Risk Analysis, Thorough Patch Testing* (IDC #lcUS43470218, January 2018)
- *Worldwide Security as a Service Forecast, 2017-2021* (IDC #US43234517, December 2017)
- *IDC FutureScape: Worldwide Security Products and Services 2018 Predictions* (IDC #US43286117, December 2017)

- *Worldwide Threat Intelligence Security Services Forecast, 2017-2021* (IDC #US43149317, November 2017)
- *Pursue Patch Independence: Latest WannaCry Event Prompts Need for Risk-Based Defenses* (IDC #US42570717, May 2017)

### Other Resources

- Community emergency response teams (CERTs)
- Computer security incident response teams (CSIRTs)
- Forum for Incident Response and Security Teams (FIRST)
- Carnegie Mellon University, *Handbook for Computer Security Incident Response Teams* (**resources.sei.cmu.edu/asset_files/Handbook/2003_002_001_14102.pdf**)
- ISO/IEC 27035:2011, *Information technology – Security techniques – Information* security incident management (**www.iso.org/iso/catalogue_detail?csnumber=44379**)
- NIST, *Computer Security Incident Handling Guide (800-61 Revision 2)* (**nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf**)

## Synopsis

This IDC study presents through the IDC MarketScape model a vendor assessment of providers offering incident response services. The assessment reviews both quantitative and qualitative characteristics that define current market demands and expected buyer needs for incident response services. The evaluation is based on a comprehensive and rigorous framework that assesses how each vendor stacks up to one another, and the framework highlights the key factors that are expected to be the most significant for achieving short- and long-term success in the incident response marketplace.

"With the relentless onslaught of sophisticated cyberattacks, enterprises must be proactive about incident readiness, response, and resiliency. In-house solutions are challenging to fund and maintain at the required level, so organizations increasingly are turning to service providers for assistance. As more providers enter this rapidly growing marketplace, buyers have more choice but also more complexity related to evaluation and selection. Thorough vetting takes time and attention to the providers' people, processes, and technology. Enterprises should make this endeavor a priority." – Christina Richmond, IDC program vice president, Worldwide Security Services

## About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

## Global Headquarters

5 Speen Street
Framingham, MA 01701
USA
508.872.8200
Twitter: @IDC
idc-community.com
www.idc.com

---