CROWDSTRIKE

White Paper

10 Key Considerations When Evaluating a Services Retainer

Abstract

In an era of rapidly evolving cyber threats, an effective services retainer can mean the difference between swift containment and catastrophic damage. This white paper presents 10 critical considerations to guide chief information security officers (CISOs) in selecting an IR provider that offers more than just technical expertise — one that functions as a long-term strategic partner. Key topics include response time, service flexibility, proactive and post-incident offerings, global reach, and the impact of a strong services retainer on cyber insurability. Throughout, you'll discover how CrowdStrike's Services Retainer stands apart, offering modular, scalable options and a holistic portfolio of over 50 pre-breach, breach and post-breach services. By examining these considerations and exploring the CrowdStrike advantage, security leaders gain a roadmap for aligning IR capabilities with broader business goals and ensuring maximum resilience against today's most advanced cyber adversaries.

Table of Contents

The role of a chief information security officer (CISO) has evolved dramatically as cyber threats continue to become more sophisticated and destructive. In today's high-stakes environment, choosing the right incident response (IR) retainer isn't just about finding a vendor with technical capabilities — it's about selecting a strategic partner that aligns with your organization's unique needs and long-term cybersecurity goals.

A services retainer from a high-quality provider can save the day. Intrusions by eCrime adversaries, ransomware groups or nation-state threat actors are serious types of cyberattack that would outmatch most cybersecurity teams. The fast reaction of a world-class IR team can take control of the situation and boot the adversary from the environment.

If no serious incident occurs during the retainer term, a high-quality provider will allow you to apply pre-purchased retainer hours to other services that will mature and develop your security program, lowering the risk of a serious incident.

A CrowdStrike Services Retainer transforms your role from crisis manager to strategic leader, delivering the confidence to face any threat and the power to reshape your organization's security future.

The CrowdStrike Advantage

Key Differentiators of the CrowdStrike Services Retainer

A global network of skilled responders paired with the cloud-native CrowdStrike Falcon® platform enables rapid, precise action within minutes of an alert.

Modular and customizable retainer services adapt to specific risk profiles, industries and operational requirements.

A comprehensive portfolio of over 50 unique services covers the pre-breach, breach and post-breach phases of IR, including assessments focused on cloud, software as a service (SaaS) and identity.

Extensive front-line experience in responding to high-profile global cyberattacks provides deep understanding of adversary tactics.

An ecosystem of vetted service partners and tech alliances ensures comprehensive coverage and seamless integration with existing tools.

Pre-incident planning and post-incident remediation services strengthen overall security posture before and after breaches.

Scalable, global IR capabilities include 24/7/365 coverage and teams in strategic regions worldwide.

Pre-coordinated relationships with over 40 cyber insurance carriers facilitate swift investigations and efficient responses.

A long-term partnership approach provides a strategic roadmap aligned with the organization's evolving cybersecurity needs.

Structured incident escalation processes facilitate seamless collaboration across internal teams and external entities.

This paper outlines 10 considerations for security leaders that are evaluating the renewal or acquisition of a services retainer.

1. Response Time and Availability

One of the most critical factors in IR is how quickly a team can be mobilized. During a breach, every second counts — delays can lead to data loss, financial damage, reputational harm and prolonged downtime. The narrow window to contain a breach demands swift action, as adversaries exploit even brief delays.

Response time isn't just about speed — it's about how effectively a team can mitigate damage, contain threats and preserve evidence for forensic analysis and regulatory compliance. Rapid action accelerates recovery, minimizes downtime and supports business continuity.

When selecting a services retainer, prioritize 24/7/365 availability and committed response times that are measurable for every scenario. CrowdStrike offers global, follow-the-sun support, ensuring elite responders are ready to contain threats and restore order immediately — no matter the time or place.

Questions for security leaders evaluating IR response times:

- What are the vendor's committed response times?
- Are response times stated clearly? How are those times measured?
- Is the IR team available 24/7/365? How is coverage handled across time zones?
- What is the process for escalating incidents to ensure that critical issues are prioritized and addressed immediately?
- How are automation and technology leveraged to reduce response times?

The CrowdStrike Difference

CrowdStrike's global network of highly skilled incident responders — paired with the power of the cloud-native Falcon platform — enables them to act with unprecedented speed and precision. Within minutes of an alert, you have seasoned experts taking charge of the situation, quickly identifying the breach's scope, mitigating the damage and initiating containment. But CrowdStrike's response doesn't stop there. While containing the threat, CrowdStrike also hunts down its origins, identifying the root cause to prevent follow-on attacks. The end result is a faster, more effective response that minimizes business disruption while neutralizing the threat.

2. Flexibility

Every cybersecurity incident is unique, varying in attack type, adversary intent, targeted systems and impact. What seems minor in one environment can be catastrophic in another, depending on the affected systems' criticality. A services retainer must reflect this diversity, offering flexible, scalable services aligned with your risk profile, infrastructure and operations.

Flexibility ensures your organization isn't constrained by rigid frameworks ill-suited to the incident's scope. For example, a phishing attempt compromising credentials may need minimal intervention, while a ransomware attack on critical systems demands advanced forensics, containment and recovery efforts. A strong services retainer can scale response efforts, efficiently addressing both small security events and complex breaches without over-allocating resources.

Evaluate whether the provider can tailor its services to your industry's regulatory requirements — such as HIPAA or the GDPR — and adapt to your technology stack, workflows, and cloud or on-premises environments.

A flexible services retainer positions your organization to efficiently handle the unpredictable nature of cyber threats, ensuring you can use your resources effectively and avoid critical gaps in an evolving threat landscape.

Questions for security leaders evaluating services retainer flexibility:

- Can the vendor customize its retainer services to align with our organization's specific threat profile and industry requirements?
- Does the retainer offer scalable response options that can adapt to both minor incidents and major breaches?
- How well can the vendor integrate with our existing security infrastructure, including cloud environments, on-premises systems and third-party applications?
- Are there options within the retainer to adjust services as our organization's needs evolve or as the threat landscape changes?
- What level of proactive support — such as readiness assessments or threat hunting — can we activate through the retainer? Can these services be scaled up or down as needed?
- How does the vendor handle regulatory changes or new compliance requirements? Can it quickly adapt to new legal obligations within our industry?

The CrowdStrike Difference

The CrowdStrike Services Retainer is built with modularity in mind, allowing organizations to customize their engagement based on their specific risk profile, industry and operational requirements. Whether you need ongoing advisory services, red team activities or a full-scale IR team on standby, CrowdStrike's retainer can adapt and scale to meet your evolving security needs. From handling minor incidents that require forensic investigation to deploying teams in the event of a sophisticated breach, CrowdStrike ensures that the response aligns with the unique demands of your organization.

3. Scope of Services Offered

When evaluating a services retainer, the goal isn't just to meet compliance requirements or reduce insurance premiums — the retainer should also help strengthen your security posture and prepare you for potential threats. A high-quality retainer offers more than breach response — it delivers proactive services, including readiness assessments, tabletop exercises, cloud security assessments and advanced red team exercises to fortify defenses and enhance your team's readiness.

Concerns about "wasted" hours are mitigated when retainers include these proactive measures. Tabletop exercises refine response plans and reduce reaction time, while threat hunting identifies hidden adversaries, stopping attacks before they materialize. Services like red teaming and attack surface assessments uncover vulnerabilities, enabling your organization to address weaknesses before they're exploited.

A world-class provider turns downtime into opportunities for improvement, integrating proactive assessments and threat intelligence to build resilience. The right retainer is more than a safety net — it's a strategic tool to prevent incidents, prepare your team and reduce overall risk, ensuring your organization is ready for whatever comes next.

Questions for security leaders evaluating the scope of retainer services offered:

- Does the retainer cover the full life cycle of IR, including proactive, reactive and post-incident services?
- Are pre-incident services like readiness assessments, threat intelligence briefings and tabletop exercises included to prepare my team for potential breaches?
- How comprehensive are the vendor's reactive response capabilities, and does the vendor provide forensic analysis, containment and recovery in the event of an incident?
- Does the retainer cover specialized scenarios like insider threats, supply chain compromises and cloud-native attacks that are relevant to our infrastructure and threat profile?
- Does the vendor offer post-incident services like root cause analysis, regulatory reporting and detailed recommendations for remediation and for improving our IR plan?
- Are the services flexible enough to scale based on the severity of incidents, and can they adapt to our organization's industry-specific regulatory and compliance requirements?

The CrowdStrike Difference

CrowdStrike offers an extensive portfolio of over 50 unique services designed to provide comprehensive coverage across the pre-breach, breach and post-breach phases of the incident life cycle. These services ensure that organizations are not only prepared to respond to cyberattacks but equipped to prevent them and recover stronger if an incident occurs. In the pre-breach phase, CrowdStrike delivers proactive capabilities such as threat intelligence briefings, attack surface assessments, tabletop exercises and red teaming, helping organizations identify vulnerabilities and strengthen defenses before a breach can occur. During a breach, CrowdStrike's elite IR teams provide rapid triage, forensic analysis, containment and recovery efforts to mitigate the impact and quickly restore operations. Following an incident, CrowdStrike's post-breach services include root cause analysis, regulatory reporting, remediation planning and a discussion of lessons learned, ensuring that vulnerabilities are addressed, compliance requirements are met and your organization emerges more resilient. With this robust suite of services, CrowdStrike ensures that every aspect of your organization's cybersecurity posture is covered, from prevention to recovery.

4. Expertise and Track Record

When evaluating a services retainer, the vendor's track record is critical to ensuring an effective response during a breach. The vendor's expertise and experience — especially with incidents in your industry — provide confidence that it can handle the specific threats you face, from ransomware to nation-state actors.

A proven vendor brings not only technical skill but strategic insight to make fast, informed decisions that minimize damage and accelerate recovery. It excels at timely communication, efficient escalation and coordination with internal teams, regulators, legal counsel and law enforcement. Its ability to triage incidents, preserve forensic evidence and manage high-pressure situations ensures a smooth and effective response.

Security leaders should also assess the vendor's history of handling large-scale breaches and its capacity to lead complex, multi-geography responses. Equally important is the vendor's commitment to post-incident follow-through, offering actionable analysis and proactive guidance to strengthen defenses against future threats.

Ultimately, a strong track record ensures the vendor can contain threats, remediate vulnerabilities and restore operations swiftly.

Questions for security leaders evaluating the track record of their potential services retainer provider:

- What is the vendor's experience with handling incidents similar to the specific threats we face?
- How well has the vendor responded to high-profile, large-scale breaches? What were the outcomes of those engagements?
- Does the vendor have industry-specific experience and a deep understanding of regulatory requirements that apply to us?
- How transparent is the vendor in providing post-incident reporting and analysis?
- What is the vendor's reputation for communication and leadership during incidents?
- How well does the vendor manage communication — both internally and externally — during a breach?
- Does the vendor have a proven track record of calm, decisive leadership in crisis situations?
- How does the vendor approach continuous improvement and proactive services based on past IR experiences?
- Does the vendor leverage its past experiences to offer proactive services like red teaming, tabletop exercises and threat hunting?
- Can the vendor provide references or case studies that demonstrate successful incident management across multiple industries and geographies?

The CrowdStrike Difference

When it comes to expertise and track record, CrowdStrike stands out as the industry leader, with years of front-line experience in responding to some of the most significant and consequential breaches of the past decade. CrowdStrike's IR teams have been at the forefront of some of the most high-profile global cyberattacks, giving them a deep understanding of adversary tactics and techniques. This unparalleled experience enables CrowdStrike to respond swiftly and decisively to breaches of all sizes, whether they involve nation-state actors, ransomware or supply chain attacks.

During an active breach, CrowdStrike brings not only technical capabilities but the strategic expertise needed to manage complex incidents. CrowdStrike's ability to quickly assess, triage and contain breaches is built on years of real-world experience dealing with the most sophisticated adversaries. Moreover, CrowdStrike excels in coordinating across different stakeholders — whether it's internal security teams, legal departments, regulatory bodies or law enforcement — ensuring that every aspect of the response is managed effectively and efficiently.

Fueled by deep IR expertise, CrowdStrike also delivers proactive services that help organizations fortify their defenses long before a breach occurs. CrowdStrike red team simulations and tabletop exercises leverage real-world attack scenarios to provide your team with invaluable training, and post-breach analysis provides actionable insights to improve your overall security posture. Whether it's in the middle of a crisis or in preparation for future threats, CrowdStrike's proven track record ensures your organization is ready to defend against whatever comes next.

5. Ecosystem of Partnerships

Incident response is a team sport. A services retainer connected to a robust ecosystem of technology and service partnerships ensures a swift, effective response. Vendors leveraging top-tier tools, intelligence and cross-industry expertise can address complex breaches involving third-party applications, cloud providers or supply chain vulnerabilities. Strong relationships with threat intelligence feeds and forensic services provide real-time insights to reduce response times and streamline compliance with regulatory and legal obligations, especially during data breaches and nation-state attacks.

Partnerships with cyber insurance providers and legal experts help manage financial and legal fallout, simplifying claims and regulatory reporting. Integration with endpoint detection and response (EDR), security information and event management (SIEM) and cloud platforms ensures seamless system alignment and faster response efforts. Access to training and development resources further empowers security teams to stay ahead of emerging threats.

A well-connected IR vendor brings cutting-edge tools, intelligence and partnerships to ensure faster recovery, improved compliance and enhanced protection against sophisticated threats.

Questions for security leaders evaluating the partner ecosystem of a potential services retainer provider:

- Does the vendor have established partnerships with key technology providers (e.g., EDR, SIEM and cloud platforms) that integrate with our existing infrastructure?
- Can the vendor collaborate with third-party vendors — such as cloud providers or supply chain partners — to resolve incidents that extend beyond our internal systems?
- Does the vendor have alliances with cyber insurance providers and legal advisors to support the claims process and legal remediation after an incident?
- Are there partnerships in place to provide ongoing training, red teaming and threat hunting services to continuously strengthen our security posture?

The CrowdStrike Difference

CrowdStrike's ecosystem of vetted service partners operates across adjacent areas of the IR process, ensuring comprehensive coverage and support during an active breach. Whether it's working with crisis communications advisors, legal advisors or cyber insurance providers, CrowdStrike only collaborates with trusted partners that meet the highest standards of quality and reliability. These partnerships allow CrowdStrike to streamline IR efforts, ensuring that every phase of the response is handled with precision. By working with specialists in these related fields, CrowdStrike can offer a seamless and coordinated response that addresses every aspect of the incident, reducing downtime and helping organizations recover swiftly.

In addition to CrowdStrike's service partnerships, its tech alliance partners enable CrowdStrike to integrate with a wide array of security tools, from EDR systems to SIEM platforms. This integration speeds up IR engagements by allowing CrowdStrike to quickly deploy solutions and pull valuable data from the tools your organization already uses. CrowdStrike's tech partnerships ensure faster and more effective response, reducing the time it takes to detect, contain and remediate incidents.

6. Pre- and Post-Incident Support

Effective IR isn't just about what happens during a breach — it's also about what happens before and after. It's possible to overlook the importance of **pre-incident planning** and **post-incident remediation** when selecting a services retainer, but these stages are critical in ensuring that the response is efficient and the organization is stronger afterward.

Questions for security leaders evaluating the pre- and post-incident support of a potential services retainer provider:

Pre-Incident Support:

- What proactive services does the retainer include to strengthen our security posture before a breach occurs?
- Does the vendor offer incident readiness assessments and guidance on developing or refining our IR plan?
- How does the vendor engage with our team to improve our response capabilities through training or workshops?

Post-Incident Support:

- What level of forensic analysis and reporting is included in the retainer after an incident?
- Does the vendor offer guidance and services to support regulatory reporting and compliance obligations after a breach?
- How does the vendor help improve our long-term security posture through lessons learned and remediation planning?

The CrowdStrike Difference

Before an incident occurs, CrowdStrike works with your team to develop **IR plans**, run **tabletop exercises** and conduct **readiness assessments** to identify any gaps in your defenses and practice the mechanics of the response process. These activities are designed to build a strong foundation so that when an incident occurs, your team can act quickly and decisively.

After an incident, the focus should shift to **lessons learned and fortification**. CrowdStrike's post-incident services include a full forensic investigation, root cause analysis and detailed reporting that can be used to address vulnerabilities and prevent future attacks. By engaging in post-incident analysis, you can turn a breach into an opportunity to strengthen your overall security posture.

7. Scalability and Global Reach

In today's connected world, organizations face cyber threats that cross borders and exploit regional variations in defenses, laws and regulations. Your IR provider must deliver consistent global support, ensuring protection no matter where an incident originates. This includes not only geographic reach but expertise in regional compliance requirements — such as those listed in the GDPR in the EU or the SEC disclosure rules in the U.S. — as well as knowledge of jurisdictional challenges and coordination with local law enforcement.

A global IR provider must scale resources to match incident severity, from localized breaches to multi-region attacks, and deploy forensic experts, legal resources and containment teams as needed. The provider's ability to support diverse IT infrastructures — including cloud, on-premises and hybrid systems — ensures effective response across all environments, no matter the location.

With global expertise and scalable solutions, the right provider ensures seamless cross-border coordination, regulatory compliance and robust protection for your operations worldwide.

Questions for security leaders evaluating the scalability and global reach of a potential IR provider:

- Does the vendor have a proven ability to support IR efforts across multiple regions and time zones?
- Can the vendor navigate diverse regulatory requirements across different geographies, such as those of the GDPR, CCPA and SEC disclosure rules?
- How scalable are the vendor's IR resources? Can the vendor handle small, localized incidents and large-scale, multi-region attacks?
- Does the vendor have a global presence, with teams and partners in key regions to ensure rapid response and collaboration across borders?
- Can the vendor integrate seamlessly with our global IT infrastructure, including cloud, on-premises and hybrid systems located in different geographies?
- How does the vendor ensure continuous communication and coordination between global teams, internal stakeholders and external partners during a global incident?

The CrowdStrike Difference

CrowdStrike is uniquely positioned to deliver scalable, global IR for organizations of all sizes and across every industry. With teams and partners located in strategic regions around the world, CrowdStrike ensures that response efforts can be initiated within minutes, no matter where or when an incident occurs.

CrowdStrike's 24/7/365 coverage means your organization is never left vulnerable, and CrowdStrike's ability to scale resources ensures that it can handle everything from localized security events to large-scale, multi-region breaches. In addition, CrowdStrike's deep understanding of global compliance requirements — combined with world-class technology integrations — allows its IR experts to manage complex incidents while adhering to regulatory standards in every jurisdiction.

With committed response times that lead the industry, CrowdStrike guarantees your organization receives fast, effective support, reducing downtime and mitigating damage before it escalates.

8. Impact to Cyber Insurability

The importance of cyber insurance has introduced a new consideration for CISOs evaluating a services retainer: **How will a services retainer impact your organization's ability to obtain and maintain cyber insurance?** Insurers are increasingly demanding robust IR capabilities as a prerequisite for coverage, and the quality of your services retainer can play a significant role in your insurability and cyber insurance profile.

Questions for security leaders when aligning their retainer with cyber insurance:

- Does the vendor's IR service meet the requirements outlined by our cyber insurance provider for coverage eligibility?
- How does the vendor's track record of handling incidents influence our overall risk profile with insurers?
- Does the services retainer include proactive services like readiness assessments or tabletop exercises that insurers may view favorably when assessing our coverage needs?
- Will the vendor provide detailed, timely documentation and reporting that align with our insurer's requirements in the event of a claim?
- Can the vendor help us improve our cybersecurity posture in ways that could positively impact policy negotiations or create enhanced terms and conditions?
- Does the vendor have experience working directly with cyber insurance providers during incidents? Can the vendor help streamline the claims process?
- Is the vendor on-panel with our cyber insurance provider?
- How many cyber insurance panels does this potential IR vendor sit on?

The CrowdStrike Difference

CrowdStrike is deeply entrenched in the cyber insurance ecosystem, with extensive partnerships across over 40 pre-established cyber insurance carriers. Due to these insurance carriers' familiarity with CrowdStrike's IR practices, CrowdStrike can begin investigations swiftly and respond efficiently to reduce the impact and cost of a cyber breach.

CrowdStrike's services retainers help organizations improve their cyber insurability by offering **proactive security assessments, detailed reporting and evidence of strong response capabilities**. In addition, CrowdStrike's post-incident reporting meets the stringent documentation requirements often requested by insurers, ensuring that you remain in good standing with your cyber insurance provider even after an attack.

9. Long-Term Partnership and Relationship

Incident response isn't a one-off service — it's an ongoing relationship that evolves alongside your organization's cybersecurity needs. When choosing a services retainer, consider whether the vendor is invested in building a **long-term partnership** that aligns with your organization's growth, risk profile and industry-specific challenges.

Questions for security leaders looking for a long-term strategic partner with their potential services retainer provider:

- Does the vendor demonstrate a clear commitment to understanding our organization's unique risk profile and evolving security needs over time?
- How will the vendor help us mature our security program with proactive services like tabletop exercises, red team/blue team simulations and threat hunting engagements?
- Can the vendor provide a strategic roadmap that aligns with our short-term, mid-term and long-term goals for improving IR and overall cybersecurity posture?
- How flexible is the vendor in adapting its services as our organization grows, enters new markets or faces changing regulatory requirements?
- Does the vendor offer continuous support and guidance beyond IR, helping us stay ahead of emerging threats and improving our defenses over time?
- What metrics and benchmarks will the vendor use to measure the progress and effectiveness of our security improvements over the course of the partnership?
- How does the vendor plan to integrate with our internal teams, providing training and knowledge transfer to improve our in-house capabilities and build long-term resilience?

The CrowdStrike Difference

The CrowdStrike Services team's approach is to develop a long-term roadmap that aligns with your security goals, whether it's strengthening your defenses today, preparing for tomorrow's threats or building resilience for the future. From the very beginning, CrowdStrike focuses on understanding where your security program currently stands and where you want it to be in the short term, mid term and long term.

CrowdStrike tailors a strategic plan that includes proactive services like tabletop exercises, red team/blue team simulations, threat hunting engagements and continuous improvement programs. These services are designed to not only enhance your security posture but mature the capabilities of your internal teams. In the short term, for example, CrowdStrike may focus on testing your current IR plans through simulated tabletop exercises, identifying areas for immediate improvement. In the mid term, CrowdStrike can expand these efforts to include more hands-on red team/blue team engagements, where your defensive strategies are tested in real-world attack scenarios to sharpen your team's response abilities. Over the long term, CrowdStike will collaborate with you to build a resilient, future-ready security program that continually adapts to the evolving threat landscape, ensuring your organization is always prepared to face emerging risks.

By partnering with CrowdStrike, your organization can embark on a comprehensive, strategic journey designed to grow and mature your security program, allowing you to stay ahead of adversaries and achieve lasting cyber resilience.

10. Incident Escalation

In a high-pressure IR scenario, the ability to quickly escalate issues to the right internal and external teams can make all the difference. Whether it's legal, regulatory or law enforcement involvement, the vendor should have established protocols for rapid escalation to ensure that the right stakeholders are informed and engaged at the right time.

Questions for security leaders looking for efficient escalation of an incident with their potential services retainer provider:

- Does the vendor have clearly defined escalation protocols that ensure the right internal and external stakeholders are notified promptly during a critical incident?
- How quickly can the vendor escalate an incident to key teams — such as legal teams, regulatory authorities and law enforcement — when necessary?
- What is the vendor's experience in managing escalations involving compliance, regulatory bodies and industry-specific reporting requirements?
- Can the vendor facilitate seamless communication and coordination between our internal response teams and external parties during high-pressure incidents?
- Does the vendor have established relationships with law enforcement, legal advisors or regulators that can aid in escalating incidents effectively?
- How does the vendor ensure continuous updates and transparency during the escalation process so that all relevant parties are kept informed in real time?

The CrowdStrike Difference

CrowdStrike's incident escalation processes are built to facilitate seamless collaboration across internal teams and external entities. CrowdStrike coordinates closely with your legal and compliance teams, executives, regulatory authorities and law enforcement when necessary, ensuring that all escalation protocols are followed without delay. This structured approach helps prevent unnecessary confusion and allows for swift resolution in high-stakes situations.

With the CrowdStrike Services Retainer, CrowdStrike's expertise becomes your expertise.

In the current threat landscape, selecting the right services retainer is critical for both immediate response and long-term organizational resilience. A well-chosen services retainer enables a rapid and coordinated reaction to incidents, minimizing potential damage and facilitating quicker recovery. And, a truly effective retainer should also help an organization proactively strengthen its defenses, improve its response capabilities and meet compliance requirements.

CrowdStrike's Services retainer provides comprehensive coverage across the entire incident life cycle, addressing both immediate IR needs and long-term cybersecurity objectives. With a global reach, scalable services and extensive expertise across diverse industries, CrowdStrike ensures that organizations are prepared to handle incidents of any size or complexity. CrowdStrike's services are designed to respond swiftly and effectively in the event of a breach and to help strengthen your organization's security posture through proactive measures such as threat hunting, tabletop exercises and vulnerability assessments.

Ultimately, CrowdStrike's Services retainer is not just about reactive measures but about building a sustainable, future-proof cybersecurity strategy. By providing the tools and expertise needed for both prevention and remediation, CrowdStrike supports the long-term maturity of your security program, helping your organization stay ahead of emerging threats and regulatory changes.

When you choose CrowdStrike as your IR partner, you're ensuring that your organization benefits from expert guidance, tailored services and a commitment to continual improvement, ensuring a robust defense and enhanced readiness for future challenges.

Learn more here

About CrowdStrike

CrowdStrike (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with the world's most advanced cloud-native platform for protecting critical areas of enterprise risk — endpoints and cloud workloads, identity and data.

Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform delivers rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

CrowdStrike: We stop breaches