Cyber Incident Response Team (CIRT) Professional Services Catalog

CRITICALSTART®

Table Of Contents

02 **Why Critical Start CIRT Professional Services?**

- Services Breakdown

04 **Proactive Services**

- Tabletop Exercises
- IR Plans & Playbooks
- Cyber Readiness Assessments
- Threat Hunting
- Threat Hunting Training
- Incident Readiness Training
- Penetration Testing
- Vulnerability Assessment

07 **Reactive Services**

- Incident Response
- Digital Forensics
- Compromise Assessment
- Post-Incident Monitoring

10 **Incident Response Retainer**

- What It Is
- Benefits

Why Critical Start CIRT Professional Services?

CRITICALSTART® Cyber Incident Response Team (CIRT) Professional Services offer comprehensive end-to-end solutions to help supplement your existing expertise.

Our robust services portfolio provides added value through deep industry expertise, national reach, and on-demand resources to create customer loyalty and enhance profitability. Our focus on designing and managing solutions to expand our partners' capabilities can impact organic growth, produce new profitable revenue streams, and act as your differentiator in a highly competitive market. Our full-service offering can offset low hardware margins and promote a healthy margin mix. Leverage CIRT Professional Services to expand your company's capabilities by augmenting your services practice with our team of experts!

Services Breakdown

Proactive Services

- Tabletop Exercises
- Incident Response Plans and Playbooks
- Cyber Readiness Assessments
- Threat Hunting
- Threat Hunting Training
- Incident Readiness Training
- Penetration Testing
- Vulnerability Assessment

Reactive Services

- Incident Response
- Digital Forensics
- Compromise Assessment
- Post-Incident Monitoring

Proactive Services

Tabletop Exercises

Test your organization's ability to respond to attacks and build resiliency through moderated scenarios.

How can you tell if your company's incident response or business continuity plan is sufficient before you need to put it into action? Tabletop exercises are a highly effective way to determine emergency preparedness before a crisis occurs.

We design our tabletop exercises to test your organization's IR Plan and security controls by addressing simulated cyberattacks, disaster recovery, and other crises.

These interactive exercises can be performed on-site or remotely and include:

- ✓ **Situation Manual:** Includes scenarios based on your current infrastructure, capabilities, risk, and impact
- ✓ **Stakeholder Engagement:** Ensures involvement of key contributors within your Computer Security Incident Response Team (**CSIRT**)
- ✓ **Constructive After-Action Report/Improvement Plan:** Based on comprehensive feedback
- ✓ **Customized Scenarios**

Incident Response (IR) Plans & Playbooks

Ensure that your IR plan addresses the latest risks.

Even a small cybersecurity incident, such as a malware infection, can escalate into a bigger problem, ultimately leading to a data breach, data loss, and interrupted business operations. An up-to-date IR Plan helps you proactively prepare for a security breach and recover quickly when an incident occurs.

Protect your data, your brand, and your budget.

The average cost of a data breach in 2024 was **$4.88 million**[1]. Business continuity, disaster recovery, and corporate image are also huge concerns, especially if your business relies on third-party vendors. Our IR Plan Review helps you mitigate these risks by updating your existing IR Plan to improve in specific areas or developing a first draft for a fresh start. As a supplemental service, our highly skilled CIRT can also validate the final draft with your CIRT through a tabletop exercise.

Our CIRT professionals:

- ✓ Engage with your CIRT stakeholders as key contributors
- ✓ Tailor a plan to your existing infrastructure and capabilities
- ✓ Align with your organization's policies, NIST Framework, and industry-proven best practices
- ✓ Produce a final document of tested processes, approved by your technical leaders

[1] IBM Cost of a Data Breach Report 2024

Proactive Services (Continued)

Cyber Readiness Assessments

Cyber Readiness Assessments evaluate all aspects of your cyber defense operations. When it comes to cybersecurity preparedness, what you don't know can hurt you. We provide full access to our platform for 90 days, allowing organizations to explore multiple cybersecurity frameworks and self-assess based on their needs.

As part of this access, organizations can select one assessment for our team to conduct on their behalf — whether a Full NIST CSF 2.0 Assessment or a Targeted Community Profile Assessment — while maintaining the ability to self-assess on additional frameworks.

You can choose from the following services, depending on your specific concerns:

Your Concerns	How We Can Help	Expected Outcomes
Is my team ready to identify, respond to, and recover from specific threat vectors, such as ransomware, business email compromise, or insider threats?	**Targeted Cybersecurity Assessments** Using the National Institute of Standards and Technology (**NIST**) Cybersecurity Framework (**CSF**) 2.0 Community Profiles, we provide deep insights tailored to your organization's unique security challenges.	• Focused security assessment based on your industry and threat model • Benchmarking against leading frameworks (e.g., NIST, CSA Cloud Controls Matrix, Cyber Risk Institute) • Prioritized security roadmap to strengthen cyber resilience
How does our implementation of existing technologies and processes compare to security best practices and industry standards?	**Full NIST CSF 2.0 Assessment** provides a comprehensive, control-by-control evaluation of your cybersecurity program. We assess policies, technical controls, and operational processes to deliver a detailed maturity score and roadmap for improvement.	• Comprehensive qualitative maturity measurement against the five categories of the NIST CSF • Gap Analysis and Prioritized Remediation Plan to identify and address weaknesses • Executive Security Strategy Report to align cybersecurity initiatives with business objectives
Is my team prepared to identify, respond to, and recover from known and unknown security threats?	**Risk-Based Cyber Readiness Assessment** leverages our Risk Assessment services to evaluate your cybersecurity maturity. This approach includes 90 days of full access to our platform, allowing organizations to self-assess on multiple cybersecurity frameworks. As part of this trial, our team will perform one assessment of your choice, while you can continue self-assessing on other frameworks independently.	• Ongoing visibility into security maturity with automated tracking • First assessment is free, helping organizations gain insight into immediate security priorities

Proactive Services (Continued)

Choosing the Right Assessment for Your Needs

Every organization faces unique cybersecurity challenges based on its industry, threat landscape, and regulatory requirements. Whether you need a broad, full-spectrum evaluation or a targeted deep dive into specific security concerns, our assessments provide actionable insights to enhance your security posture.

Available Community Profiles

- ✓ Incident Response & Cyber Risk Management (NIST SP 800-61 Rev. 3)
- ✓ Cloud Security (CSA Cloud Controls Matrix V4.0)
- ✓ Financial Sector Security (Cyber Risk Institute Profile)
- ✓ Ransomware Risk Management (NIST IR 8374)
- ✓ Manufacturing Cybersecurity (NIST IR 8183r1)
- ✓ Botnet Threat Mitigation (Cybersecurity Coalition Botnet Profile)
- ✓ DDoS Threat Mitigation (Cybersecurity Coalition DDoS Profile)

Additional Risk Assessment Offerings

- ✓ Quick Start Risk Assessment
- ✓ NIST CSF 1.1 Guided Assessment
- ✓ NIST CSF 2.0 Guided Assessment
- ✓ CIS Critical Security Controls v8
- ✓ CIS Critical Security Controls v8.1
- ✓ NIST SP 800-171 v2 Security Requirements

Proactive Services (Continued)

Threat Hunting

Conducted by our security experts, we proactively and iteratively search through your networks to detect and isolate advanced threats that evade existing security solutions.

Threat Hunting Training

A proven methodology to help your team stop hidden attacks.

The longer a threat stays inside your network, the more damage it can do. Our Digital Forensics and Incident Response (**DFIR**) team can teach your defenders how to proactively identify malicious activity within your network and take appropriate action.

Understand your risks and identify a path to a more mature, proactive security posture.

As an alternative to our traditional threat-hunting service in which we do all the work and then provide you with the results, we offer on-site or remote threat-hunting training using advanced data science to detect evolving threats.

- ✓ Application of behavioral analytics to enhance baselines and detect malicious use of tools/protocols
- ✓ Prompt notification of unknown compromises or attacks in progress
- ✓ Industry-vertical information sharing
- ✓ Identification of areas of improvement within the organization’s vulnerability management strategy
- ✓ Interim and final findings reports and briefings

Incident Readiness Training

Prepare your team before an attack happens.

During an investigation, every second matters. Early action can return business operations to normal faster. Our incident readiness training is designed to help your team gather and triage evidence our CIRT will request early in an investigation. We provide training unique to your environment, technologies, and critical digital assets.

We understand that the initial stages of an investigation can be difficult to navigate.

As a supplement to an IR Plan, IR Readiness Training is designed for technical professionals participating in an investigation. Offered on-site or remotely, this training identifies which evidence to gather first, techniques for evidence handling, and procedures for evidence collection.

- ✓ Application of behavioral analytics to enhance baselines and detect malicious use of tools/protocols
- ✓ Prompt notification of unknown compromises or attacks in progress
- ✓ Industry-vertical information sharing
- ✓ Identification of areas of improvement within the organization’s vulnerability management strategy
- ✓ Interim and final findings reports and briefings

Proactive Services (Continued)

Penetration Testing

Ensure the robustness of your organization’s security posture through comprehensive penetration testing services.

In today’s increasingly digital world, safeguarding your sensitive data and critical assets is paramount. Our Penetration Testing Services proactively identify vulnerabilities in your IT infrastructure and applications before malicious actors can exploit them.

Our expert team conducts thorough assessments using ethical hacking techniques to simulate real-world cyberattacks. Our services include:

- ✓ Customized Testing Scenarios: We tailor each penetration test to your unique environment, considering your infrastructure, applications, risk profile, and potential threats.
- ✓ Exhaustive Testing: We leave no stone unturned, meticulously examining your network, systems, and applications for weaknesses, ensuring we uncover both known and unknown vulnerabilities.
- ✓ Stakeholder Engagement: We work closely with your team, ensuring key stakeholders are involved in the process, including your security team, IT staff, and management.
- ✓ Comprehensive Reporting: Following each test, you’ll receive a detailed after-action report, including a prioritized list of vulnerabilities and actionable recommendations to improve your security posture.

Vulnerability Assessment

Proactively manage your cybersecurity risks with our in-depth Vulnerability Assessment Services.

Identifying and addressing vulnerabilities is crucial to maintaining a solid defense against cyber threats. Our Vulnerability Assessment Services are designed to provide you with a clear understanding of your organization’s security weaknesses, allowing you to prioritize and remediate them effectively.

Key features of our Vulnerability Assessment Services include:

- ✓ Thorough Scanning: We employ advanced scanning tools and methodologies to comprehensively assess your network, systems, and applications for vulnerabilities.
- ✓ Risk Prioritization: Our assessments provide you with a risk-based prioritization of vulnerabilities, allowing you to focus your resources on addressing the most critical issues first.
- ✓ Flexible Assessment Frequency: Our Vulnerability Assessment Services offer the flexibility to determine assessment intervals in close collaboration with you and your stakeholders. We’ll work together to establish a monitoring schedule that aligns with your specific security needs, whether it’s conducted on a regular basis or at specific milestones in your cybersecurity strategy. This collaborative approach ensures that assessments are performed at intervals that best suit your evolving security requirements and priorities.
- ✓ Actionable Recommendations: Our reports include detailed recommendations for remediation, helping you close security gaps and enhance your overall cybersecurity.

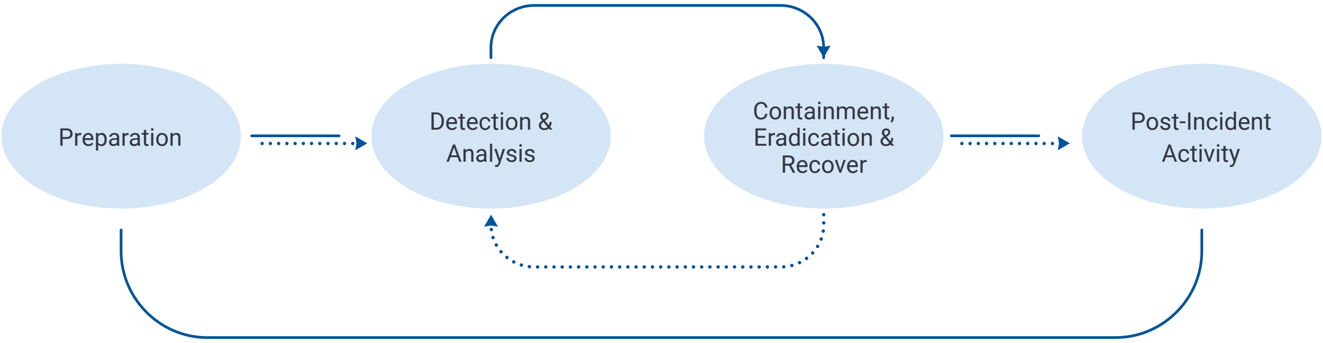
By choosing our Vulnerability Assessment Services, you’ll be better equipped to protect your organization from potential threats, maintain compliance with industry regulations, and bolster your overall security strategy.

Reactive Services

Incident Response

Leverage our CIRT to lead your team through the critical stages of an incident.

When your organization is compromised, we utilize our industry knowledge and professional expertise to use best-in-class tools and technologies to detect and analyze the threat, assist in containment, eradication, and recovery efforts, and continue to work with your team through post-incident activities.



Our experts pursue and maintain gold-standard industry certifications through various accredited entities, namely GIAC, CompTIA, EC-Council, and vendor-specific certifications.

- ✓ Crisis management to lead your team through the critical stages of an incident
- ✓ Initial, interim, and final findings reports and briefings
- ✓ Post-Incident Monitoring for 30 days to aid in the identification, containment, and remediation of threats and to support targeted threat hunting operations (optional for non-Critical Start customers)
- ✓ Malware reverse engineering to develop Indicators of Compromise (**IOCs**) and other details to aid in the identification of similar code and to support threat-hunting activities

Digital Forensics

Obtain actionable intelligence from digital evidence by utilizing our digital forensics experts.

Use our on-demand forensic investigators with experience in the Payment Card Industry Data Security Standard (**PCI-DSS**), Health Insurance Portability and Accountability Act (**HIPAA**), General Data Protection Regulation (**GDPR**), and other regulatory standards, including the International Organization for Standardization (**ISO**), National Institute of Standards and Technology (**NIST**), Cybersecurity Framework (**CSF**) for highly sensitive investigations. Our experts utilize tools, technologies, hardware, and knowledge to answer the who, what, when, where, why, and how.

Our investigators will provide:

- ✓ Forensic Imaging & Analysis
- ✓ Investigative Reporting
- ✓ Expert Witness Testimony
- ✓ Evidence Seizure, Chain-of-Custody & Secure Storage

Reactive Services (Continued)

Compromise Assessment

Rapidly identify, contain, and remediate threats to stop the bleeding.

Our team of experts utilizes your integrated Endpoint Detection and Response (**EDR**) and Security Information and Event Management (**SIEM**) platforms to proactively hunt, identify, and eradicate threats inside your environment.

IOCs discovered while performing a compromise assessment can be utilized to create new and improved detection rules for supported EDR or SIEM platforms, preventing similar threats to your organization in the future.

Haven't implemented an EDR or SIEM platform yet? No worries. Our team can deploy tools that will enable a thorough and successful threat hunt without any additional cost.

Benefits of a compromise assessment include:

- ✓ Minimize risk, reduce exposure, and preserve evidence where necessary
- ✓ Identify gaps left by current threat intelligence to reduce overall risk and median time to respond
- ✓ Highlight previously undetected threats and anomalous activity inside your network

Post-Incident Monitoring

Our Post-Incident Monitoring services utilizes the power of our **Cyber Operations Risk & Response™ platform** to help identify, contain, and remediate threats, as well as support targeted threat hunting operations during a breach.

This service includes:

- ✓ Active 24x7x365 monitoring by seasoned professionals and purpose-built technology
- ✓ Context-based alert prioritization tuned from threat assessment and business impact analysis
- ✓ 30-day license for integrated EDR products
- ✓ Leveraging global and customized/personalized playbooks and threat intelligence

Handle breaches across diverse attack vectors.

We handle criminal and non-criminal matters related to a wide variety of incidents, including:

- ✓ Malware-based attacks (Ransomware, Trojans, etc.)
- ✓ Phishing attacks
- ✓ Zero-day attacks
- ✓ Password attacks
- ✓ IoT attacks
- ✓ Critical Infrastructure attacks
- ✓ Cryptojacking
- ✓ Insider threats (espionage, fraud, etc.)
- ✓ Financial crimes
- ✓ Business Email Compromise

Incident Response Retainer

What is an IR Retainer?

An Incident Response (**IR**) Retainer is a pre-negotiated service agreement that ensures that we are at the ready should you experience a data security breach or incident. This allows you to proactively plan for the worst while at the same time gain peace of mind knowing that qualified experts are available to quickly investigate and help resolve cybersecurity incidents should they occur.

Get the most out of your IR Retainer

IR retainers are typically negotiated in 3-year contracts to ensure continuity in coverage while also locking in pricing that may otherwise fluctuate year-to-year. Ensuring maximum value is recognized from the retainer, a pre-negotiated rate is established and allows for the flexibility to shift up-front spend from reactive to proactive services.

Critical Start's IR Retainer

✓ IR retainer hours are available in bundles of 40, 80, and 120 hours and are valid for a 12-month period[1]

✓ Service levels are pre-determined and governed by a signed Service Agreement

✓ IR retainer hours are invoiced at the time of sale

✓ You can easily increase IR hours at any time within the 12-month retainer period

✓ You will pay no more than the pre-negotiated rate outlined in the Service Agreement for additional hours

✓ Gain additional value by converting any hours remaining after 8 months to Proactive Services

Benefits of an IR Retainer

✓ 24x7x365 access to incident response experts

✓ Faster response and times are reduced with prearranged communication channels and predefined response playbooks

✓ Eliminate the need for onboarding and technology integration during a turbulent time for your organization

✓ Unimpeded security incident/compromise scoping, triage, investigation, containment, eradication, and remediation

✓ Alleviate downstream risks through the pursuit of digital forensic best practices

✓ Defensible processes to satisfy regulators and be expert witness ready

✓ Fulfill cyber insurance requirements

✓ Possible reduction in cybersecurity insurance premiums

[1] After the 12-month period ceases, IR hours are forfeited. [2] Cannot transfer / convert into Microsoft IR hours

For more information, contact us at:

https://www.criticalstart.com/contact/