

# WE GET WHEN CYBERSECURITY INCIDENTS HAPPEN, RESPONSE TIME IS CRITICAL.

## CDW Amplified™ Detect and Respond Security Incident Response Services

It's every IT leader's nightmare scenario: a major security incident, locking employees from files, corrupting data and potentially devastating the organization. What if you could have a whole team of experienced security consultants just one phone call away, ready to respond at a moment's notice to any security incident you discover? Now you can.

CDW's Security Incident Response Services can help you achieve:



Reliability



Agility



Reduced Risk

### Orchestrating the Right Solution

CDW's IT Security Incident Response (IR) Services team provides assurance that your organization is aware of any security incident and is ready to respond to credential theft, malware outbreaks, security breach and other potential security incidents.

Organizations that seek outside help only after discovering a security breach often wait days or weeks for lawyers to negotiate contracts with service providers. When you decide to add CDW's Retainer-Based Security IR Services to your cybersecurity plan, that paperwork is handled up front, meaning there's no downtime between discovery and action.

**Prepaid Incident Response Service (Essential & Premium):** Depending on your service level, our one-year agreements are good for up to 120 hours of service, and up to 40 hours of event preparedness services. Event Preparedness Services included may consist of: IR Readiness Assessment, IR Program Development (Policy, Plan & Playbook Development), IR Tabletop Exercise or IR First Responder Training. This service also allows you to reallocate a portion of unused services fees to additional security advisory and assessment services at the end of your contract.

**Essential Lite IR Retainer Service (Response Time Objective):** If you require faster response time objectives but do not want to pre-purchase IR hours, the Essential Lite retainer gives you peace of mind knowing your incident will be handled in a timely manner. Should the team need to engage, all work will be billed on a time and materials basis.

**Basic Incident Response (Zero-Dollar):** We understand that a prepaid option is not right for everyone. Our Basic Incident Response Service provides you with access to CDW's IR team, should you need it. This service gives you up to 80 hours of IR services on a time and materials basis.

**Proactive & Preparedness Services:** CDW also provides four complete proactive event preparedness security services to help your team be better prepared for the inevitable. We utilize the same skilled consultants and tools for these services that we leverage to respond to security incidents.

- **Compromise Assessment:** CDW will help you understand if/when you have been compromised by providing focused threat hunting in your environment.
- **IR Readiness Assessment:** CDW will review your IR policy, plan & playbook, evaluate roles, responsibilities, processes and security tools along with performing a refresher training for IR Handlers and First Responders.
- **IR Program Development (Policy, Plan & Playbook Development):** CDW will coordinate and lead a one-day workshop assessing your existing IR policy, plan, playbook and incident notification requirements and then provide you with a complete IR policy, plan and playbook.
- **IR Planning and Tabletop Exercise Workshop:** CDW will perform an assessment including a review of policy, plan and playbooks, review of tools, roles and responsibilities. We will also provide First Responder refresher training, IR tabletop exercise, after action review, playbook updates and complete knowledge transfer.

CDW's full lifecycle of Services can support your organization no matter where you are on your journey



Design



Orchestrate



Manage



On-Premises



On-Journey



Cloud-Based



## CDW GETS SECURITY

Our team of security professionals has conducted more than 4,500 engagements across all verticals, helping clients of all sizes, each with their own needs. We get every organization has its own unique challenges. Additionally, CDW is:

- **Able to identify the ideal solution:** We maintain an ethical distance between assessment and sales functions, performing independent validation of your security posture and focusing on identifying needs and fixes rather than pushing specific products or services.
- **Trusted and professional:** CDW's security services professionals have a range of expertise in many technical disciplines and products. Many of our engineers have more than a decade of individual experience in military, government and private-sector work.
- **Stable, reliable and mature:** CDW's Security Team has operated continuously since its inception in 1998 and follows the processes and procedures of a mature consulting organization.



**CDW AMPLIFIED™  
SERVICES**

## Services Overview

The following services are included in CDW's retainer-based Security Incident Response Services:

Service	Premium	Essential	Essential Lite	Basic
Triage of incidents, including live response and analysis	✓	✓	✓	✓
Development of Indicators of Compromise (IOCs) to be utilized during containment and remediation of threats	✓	✓	✓	✓
Development of containment approach and strategy	✓	✓	✓	✓
Assistance with containment	✓	✓	✓	✓
Development of a remediation strategy and process	✓	✓	✓	✓
IT Security Incident Response Report including investigative and discovery methods and background, findings and artifacts, and remediation recommendations	✓	✓	✓	✓
Additional remediation recommendations	✓	✓	✓	✓
Response Time Objective	✓	✓	✓	—
Retainer hours	120	80	—	—
Hours of Preparedness Services included	40	16	—	—

## Certifications

We have helped more than 300 clients with their security incidents, and more than 250 clients trust CDW's Retainer-based Security Incident Response Services. CDW has achieved the following certifications:



## CUSTOMER SUCCESS STORY

**Organization:** Manufacturer

**CHALLENGE:** A 32-site manufacturing customer headquartered in the Midwest had two malware incidents occurring simultaneously. Their anti-virus solution was ineffective in protecting their workstations and the methods the customer had been using to contain and eradicate the malware was unsuccessful. In addition, the customer had almost no budget for IT Security.

**SOLUTION:** The customer contacted their CDW seller to initiate an on-demand Security Incident Response engagement. Within 15 minutes, CDW had a Security IR consultant on the phone and a IR Consultant onsite quickly. The IR Consultant:

- Worked through the weekend with the customer to contain the incident and stabilize their environment.
- Consulted with the customer regarding breaking implied trust and deploying host-based firewalls.
- Worked with the customer after their environment was stabilized on an ad hoc basis providing support and recommendations.

**RESULT:** CDW's quick response time helped the customer stop the malware from doing any more damage. In addition, the valuable insight from CDW's IR Consultant enabled the customer to reduce the chances of a similar incident recurring. CDW went from being their trusted security vendor to their trusted security partner, which enabled the customer's IT department to influence their executives to invest in improving their security strategy.

To learn more about CDW's Security Incident Response Services, contact your account manager.



**CDW AMPLIFIED™  
SERVICES**