Incident Management Services

The Dell SecureWorks Incident Response practice provides rapid containment and eradication of threats, minimizing the duration and impact of a security breach.

Leveraging elite cyber threat intelligence and global visibility, we can help you prepare for, respond to and recover from even the most complex and large-scale security incidents.

The worst time to realize you are not prepared for a security incident is during a breach. Security incidents are crisis situations that place a great deal of pressure on not only IT, but all staff charged with responding. Without a proven response plan or strategy, stressed personnel must make crucial decisions without a clear sense of order and priority. This can easily lead to poor decisions that prolong both the duration and impact of an incident.

Dell SecureWorks provides a wide array of Incident Management and Digital Forensics services, from incident response planning and analysis to emergency incident response and forensic investigation. Should a breach occur, Dell SecureWorks can help you minimize damage and preserve evidence for legal action.

Incident Response backed by elite cyber threat intelligence

Threat intelligence supports all aspects of our services portfolio. With global threat visibility, intelligence formulated by the Dell SecureWorks Counter Threat Unit™ (CTU™) research team provides greater context on the threats your organization faces. Intelligence on threat actors and their tradecraft is actively shared between our security researchers and Incident Response security consultants through an open feedback loop. Malware analysis and reverse engineering provide further intelligence and context on the threat. As a result, clients receive sharper, more effective response support when a security incident does occur.

The Dell SecureWorks Incident Response practice applies our elite intelligence on threat actor tradecraft to every engagement. This intelligence provides valuable context on the threat--its purpose, who may be behind it and how to effectively eradicate it from your environment.
Full spectrum of Incident Management capabilities

Dell SecureWorks provides end-to-end support before, during and after a security incident:

**Incident Management Services**

**Incident Management Retainer**

Invaluable when the worst happens, and even when it doesn’t

For organizations that want to ensure they have the right resources in place should a security breach occur, the Incident Management Retainer guarantees fast availability of our elite Incident Response team. Our trained experts work with you to quickly contain, mitigate and help you recover from any size security breach.

The service provides immediate support through our Security Operations Center (SOC) and onsite support unmatched globally:

- Arrival in less than 36 hours onsite US and UK
- In-transit within 48 hours for international

The retainer service isn’t just an insurance policy to guarantee you top expertise will be available when you most need it; it’s an opportunity to heighten the capabilities of your Incident Response team.

Unused retainer hours can be redeemed for proactive services. We will contact you when you are approaching your anniversary to help you use your remaining hours.

**Proactive Services**

Whether you have a response plan in place that needs reviewing and testing or want to develop one, we can help. Experienced consultants will conduct a detailed assessment of your existing incident response documentation, personnel and procedures. Recommendations will be made to improve the plan ensuring you are prepared against any type of cyber-threat.
Incident Management and Response

Incident Management Risk Assessment

Incident Management Risk Assessment is a service that reviews your existing incident response documentation, personnel and procedures and identifies gaps in these procedures. We then provide recommendations to enhance your plan’s overall effectiveness when a breach occurs.

Response Plan Review and Development

Dell SecureWorks Incident Response security consultants help you develop an effective response plan, also known as a Computer Security Incident Response Plan [CSIRP] based on IT security best practices and tailored to your organization. Your incident response plan will detail what needs to happen so you and your team can respond quickly and effectively to a security breach, and minimize the impact to your organization. In addition, your plan or CSIRP will reflect the latest intelligence we’ve developed that addresses the types of threats and scenarios of greatest concern to your organization.

Response Training and Exercises

While the development of a sound plan is a critical step, testing the plan is necessary to determine how well you will react and respond to a declared incident. Dell SecureWorks can facilitate the creation and assessment of Incident Response Testing procedures.

Testing can be in one of several formats and will provide analysis and results for integration into future exercises. Our experienced consultants will work with you to determine the best training to test your response plan.

Tabletop Exercises

Tabletop exercises are designed to validate roles, responsibilities, coordination and decision-making. Our Incident Response security experts will design and conduct plausible simulated exercises to evaluate your team’s performance, and afterward provide detailed feedback and recommendations for improvement.

Functional Training

Functional exercises allow personnel to validate their operational readiness for incidents by performing their duties in a simulated manner. Functional exercises are designed to exercise the roles and responsibilities of specific team members and procedures in one or more functional aspects of a plan.

First Responder Training

How personnel respond and what they do is critical to ensure that not only is an incident contained, but key data is collected. We provide First Responder training to ensure the chain of command is notified properly and your employees know how to put your existing plan into action.

When a breach happens, well-prepared organizations are able to minimize business disruption, financial impact, regulatory consequences, data loss and recovery time.

Compromise Assessment

The Compromise Assessment service evaluates your organization’s ability to detect, resist and respond to a targeted or advanced threat. The service is designed to help you understand your exposure to targeted threats, including Advanced Persistent Threats (APT), and take action to reduce your risk of compromise.

Program Development

The Dell SecureWorks Program Development service helps you evaluate your organization’s ability to withstand an attack and identify strategies for effective attack mitigation. In order to best determine your response capabilities, Dell SecureWorks consultants will review your process diagrams, policies, procedures, guidelines and any other pertinent information to understand your current practices and regulatory requirements. From these, we assist you in putting together policies in place as well as defining response workflows, roles and responsibilities.

Briefings and Workshops

The Dell SecureWorks Briefings and Workshops services help you review lessons learned from previous incidents that have occurred, review the overall status of your Incident Response program, or provide guidance on topics of interest that fall within the domain of Incident Management and Response. We work with you to determine the most suitable content for these sessions.

When a breach happens, well-prepared organizations are able to minimize business disruption, financial impact, regulatory consequences, data loss and recovery time.

Incident Management and Response
Reactive Services

When a breach happens, well-prepared organizations are able to minimize business disruption, financial impact, regulatory consequences, data loss and recovery time. Investigative experts are quickly available remotely to begin risk assessment and to put together the best approach to contain the event. Various services in combination may be used to ensure complete eradication. Upon containment and mitigation, key findings will be delivered to decision makers with guidance for legal and regulatory resolution.

Incident Surveillance

In an effort to ascertain additional information about the attack source and methods, Dell SecureWorks will attempt to:

- Find specific references to Customer assets affected by the current attack within underground communications
- Identify specific references to Customer assets in attack tools or malware "kits"
- Research historic proprietary and public data regarding targeted attacks against Customer assets
- Monitor and analyze underground communications pertaining to the active attack

Digital Forensic Analysis

Using a variety of forensics tools, Dell SecureWorks can capture and analyze data stored in a combination of the following formats:

- Hard drives*
- Random Access Memory
- CD/DVD
- ‘Thumb Drive’ storage
- Mobile
- Credit/Debit Card Skimmers
- Other formats that are reasonable for analysis

*Hard drive recovery services may not be available globally

In some incident scenarios—for example, some insider attacks—remote forensics can be sufficient to meet your needs.

PCI Forensic Investigations

As an approved PCI Forensic Investigator (PFI) company, Dell SecureWorks can help you respond to and recover from the smallest to even the most complex and large-scale security incidents involving cardholder data.

Our experts leverage elite cyber threat intelligence to investigate the breach, determine its likely cause, report progress to appropriate parties as required by PCI Security Standards Council, and help you contain and eradicate the threat from your environment as quickly as possible.

Incident Coordination

In performing incident management support, Dell SecureWorks can also provide advisory services in the analysis and coordination of incidents. During incident response, we often work with the executive teams, legal, public relations and other key stakeholders. Our role is to give these key stakeholders independent information and opinions derived from the evidence presented by our incident handling activities. This key role helps you manage the cost and impact of a cyber-attack.

Incident Response Remote / Onsite

Incident Management and Digital Forensics experts provide rapid containment and eradication of threats, minimizing the duration and impact of a security breach. Whether remote or onsite, we will help handle and manage the incident. Plus, we can help collect forensic information for analysis and litigation if necessary.
Malware Analysis and Reverse Engineering

If your environment has been affected by mobile malicious code (Trojans, worms, viruses, etc.), of an unknown type, such as a “zero day exploit,” Dell SecureWorks can attempt to reverse engineer the code to better understand the code’s behavior and the impact to your business and data.

This service is provided in concert with incident handling, should the incident warrant the need. Code analysis can also be done remotely as a standalone service. If code analysis is necessary, Dell SecureWorks can produce a short technical document outlining the nature of the malicious code.

Post-Mortem Analysis

At your request, quarterly conference calls can be arranged to review lessons learned from any or all incidents that have occurred, or to review the overall status of your Incident Response program. We will discuss process and capability improvements so that incident handling is as efficient and effective as possible.

Return to normal business operations

After the immediate threat of an incident has been contained, focus shifts to eradicating all traces of the threat and recovering impacted systems. Proper and thorough removal is essential. IT staff often believe an incident is resolved, only to find themselves responding to the same incident again days later because of an incomplete elimination of the problem.

Armed with intelligence from the Counter Threat Unit and based on their own experiences working hundreds of engagements annually, Dell SecureWorks Incident Response security consultants know where to look for threats operating in your network. As a result, our experts can help you completely eradicate the threat from your environment and get your operations back to normal as quickly as possible.

Meet your compliance obligations

Our Incident Response experts understand that you have compliance obligations surrounding a breach. We help your compliance, privacy and legal teams make sense of the impact that the breach had, so intelligent decisions can be made to meet your obligations.

Visit www.secureworks.com to learn more about our information security services.

Email info@secureworks.com or phone 877-838-7947 to speak to a Dell SecureWorks Security Specialist.

About Dell SecureWorks

Dell SecureWorks uses cyber threat intelligence to provide predictive, continuous and responsive protection for thousands of organizations worldwide. Enriched by intelligence from our Counter Threat Unit research team, Dell SecureWorks’ Information Security Services help organizations proactively fortify defenses, continuously detect and stop cyber-attacks, and recover faster from security breaches.

For more information, visit http://www.secureworks.com