



## Providing help with Security Incidents when you need it most.

When the worst happens, the steps required to properly respond to a Security Incident can seem daunting. The **Check Point Incident Response Team** can help. Our responders are ready to investigate and contain attacks while focusing on getting you back to business faster. We are available 24x7 to service customers across the globe.

### COMPLETE INCIDENT HANDLING

We handle the entire incident lifecycle from triage to containment and remediation with detailed documentation and reports.

### AN EXTENSION TO EXISTING SOC/IR TEAMS

Well established teams leverage individual components of our services to cover specific needs or gaps.

### ALLIES IN RESEARCH AND INTELLIGENCE

We work closely with Check Point global research teams, intelligence partners, national Computer Emergency Response Teams (CERT), and law enforcement to understand the broader context of your security event.

### PROACTIVE SERVICES

We use the experiences from handling thousands of incidents per year to help advanced customers prepare for the worst. Not only technical preparation of systems and networks, but also practical preparation with IT staff and executive management.

### HOW DOES IT WORK?

Within 30 minutes, our responders will engage to handle any aspect of a security incident. Once the incident has been contained and remediation is under way, a post incident report will provide technical details of the attack, identify the root cause, and recommend prevention or mitigation of future attacks.

### VENDOR AGNOSTIC

Security incidents involve a wide range of applications, operating systems, and configurations. Our responders have a wide breadth of experience in systems administration, engineering, and protection development allowing us to handle any situation.

*We do not require our clients to be Check Point customers.*

### LEVERAGING LESSONS LEARNED

Our casefiles are full of lessons learned. All of our clients benefit from these valuable lessons. From up-to-the-second intelligence about current threats to long-term Incident Response Planning, let our lessons learned benefit you!

# REACTIVE

## INCIDENT RESPONSE SERVICES

- Incident management and organization
- Threat hunting
- Threat containment
- Digital forensics (disk/memory/logs/network)
- Malware analysis
- Phishing mail analysis
- DDoS analysis and mitigation
- Incident communications to management level
- Reports tailored for your organization

### GLOBAL COVERAGE

Australia: 1800-467-476

Brazil: 0-800-591-9043

Colombia: 01800-518-9368

Denmark: 808-20303

Germany: 0800-183-0489

Hong Kong: 800-906-060

Hungary: 06-800-20089

India: 000-800-040-1307

Indonesia: +62-21-27899834

Israel: 1-809-457227

Jamaica: 1-866-837-4568

Japan: (0800) 0800-888-3034

New Zealand: 0800-453749

Nigeria: +234-1-227-8927

Norway: 800-25-060

Russia: 8-10-8002-6951012

Saudi Arabia: +966 0811-100-8153

Singapore: 800-492-2448

Spain: 900-804914

Sweden: +46-101388675

UK: 0-800-088-5471

Ukraine: 0-800-501732

United States: +1(866)923-0907

Email: [emergency-response@checkpoint.com](mailto:emergency-response@checkpoint.com)

# PROACTIVE

## COMPROMISE ASSESSMENT

We work with your organization to actively **hunt** for signs of current or past compromise. This includes reviewing existing security architecture, looking for vulnerabilities, and identifying risky configurations. We hunt across the network, endpoint (Windows & Linux) and email (on premise & cloud) looking for signs of compromise past and present.

## MATURITY ASSESMENT

We work with your organization to review the entire security ecosystem with a focus toward security event flow and streamlining response time.

## IR PLANS AND PLAYBOOKS

IR planning can be stressful and needs to be detailed. Having a proper incident response plan and having it understood by the organization is critical. We can leverage our experience to help navigate the challenges of designing IR plans. In addition to an overall IR plan for the organization, short and tactical playbooks can also be critical for handling technical tasks during incidents when the minutia matters.

## TABLE TOP EXERCISES

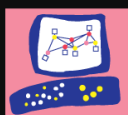
It is very important for all elements of an enterprise to be prepared for a cyber-attack. We work with you to rehearse your incident response plans and procedures at any level in the organization. From IT helpdesk through security operations to executive management.

## ENHANCE YOUR CAPABILITIES

Our focus is to educate and hone your staff's skills and abilities to respond to incidents as they happen. We provide assistance at any stage of the incident handling process from complete ownership to augmenting your existing internal capabilities.

**24/7/365**

Always available to help, call us today!



**Check Point**<sup>®</sup>  
SOFTWARE TECHNOLOGIES LTD