CHECK POINT™

CATALOG

Check Point Incident Response Team Service

Check Point Incident Response Team Service

CATALOG

THREAT EXPERT CONSULTING SERVICES

The Check Point Incident Response Team (IRT) provides expert advice with full-time, dedicated security consultants. Our team operates as an extension of your existing security and incident response teams.

DEDICATED THREAT EXPERT

We're here for you, at a moment's notice. For a minimum one-month (160 hours) term, our full-time threat expert works with your team on site or remotely. The hours can be split over several engagement periods (e.g. four one-week engagements). Leverage our threat expert to help optimize your existing IT security. Get expert advice on incident response, threat intelligence, and security operations. Our expert assists your organization with:

- Security incident preparation
- Improvement of security operations processes and procedures
- Updates or creation of threat intelligence systems and capabilities
- Support and advice
- Support of current security teams/threat teams with special events

Your response expert has full access to Check Point Incident Response intelligence. Incidents requiring escalation will be handled separately.

Minimum Engagement: **160 hours**

THREAT HUNTING

Check Point IRT can provide on-site threat hunting services, run by our senior and/or lead analysts. We identify advanced threats that may be active in your environment. This on-site activity will include deployment of passive sensors, log analysis, and intelligence analysis in the search process. Any incidents uncovered by this service and handled during the engagement will not accrue any additional charges.

Minimum Engagement: **160 hours**

INCIDENT RESPONSE SERVICES

All of the services listed below are charged in the standard per hour pricing model with a minimum engagement period of one hour. These services have suggested hours but they will be scoped by Check Point IRT to ensure the service meets your requirements.

ATTACK MITIGATION

Check Point Incident Response Team is on standby to assist customers on a 24x7x365 basis. With a 30-minute remote support SLA, Check Point IRT can rapidly assist you in containing security incidents. The sooner an incident is contained, the less damage it can inflict on your organization, and the faster your regular services are restored. Check Point IRT will perform an initial triage of the incident during the call to our hotline and activate customer-specific plans, including on-site engagement.

The Check Point Incident Response Team can assist customers in responding to:

- (D)DOS
- Data loss
- Insider threats
- Malware outbreaks
- Advanced threats and attacks
- Ransomware and cyber extortion

Recommended Engagement: **Depends on size of organization (20 hours minimum)**

INCIDENT RESPONSE PLANNING

Check Point IRT provides services to assist customers in creating and refining their incident response plans. Check Point's offerings include running incident response planning workshops and collaborating with relevant stakeholders within your organization to craft incident response strategies and technical playbooks.

Depending on the size of your organization, we recommend an engagement period of between 40-80 hours for most small and medium-sized organizations and at least 120 hours for larger organizations. However, it depends on the maturity of the incident response process and your playbooks.

Recommended Engagement: **40-120 hours depending on maturity of the organisation**

TABLE TOP EXERCISES

Check Point IRT can assist you with preparing and running tabletop exercises to rehearse their incident response plans and educate business executives on their role in critical security incidents. These on-site exercises are run by Check Point IRT experts who bring their vast experience and share valuable insights with attendees. A table top exercise engagement normally takes 40 hours, including the preparation and execution of the exercises.

Recommended Engagement: **40 hours**

MALWARE ANALYSIS

Check Point IRT has expert malware analysts who can assist your incident response or security teams with in-depth malware analysis. The malware analysts will perform a rapid triage of the malware and provide an initial report within two hours. This report will include an estimate on how long further in-depth analysis will take. In-depth analysis will include a detailed report concerning the behavior and any available intelligence about the malware.

Recommended Engagement: **8 – 40 hours (depending on malware complexity)**

POST-ATTACK ANALYSIS

Check Point IRT works with your internal IT security and incident response teams to analyze past incidents and perform a review of the processes followed, lessons learned, and how to improve future responses. This process also includes recommendations with the steps needed to prevent further occurrences or how to ensure better mitigation.

Recommended Engagement: **Scoped per incident**

FORENSICS

Check Point IRT has expert forensics analysts who can assist your incident response or security teams with in-depth forensics analysis. The forensics analysts will perform detailed analysis of memory, drives, logs and other relevant situational data before. This in-depth analysis will include a detailed report detailing all forensic findings and any available intelligence about the findings.

Recommended Engagement: **Estimated 8 hours per disk or memory image**

TRAINING & SECURITY OPERATIONS CENTER SETUP

The training is conducted by the team's senior security analysts and will be customized to specific client requirements. The team can also assist customers in creating a security operation center (SOC) and can help build its processes, procedures, and technology (Check Point and non-Check Point). For longer term engagements to assist a customer in building a SOC or incident response capability, we offer the Threat Expert service.

Check Point IRT provides you with training and advice on:

- Incident response basics
- Open source threat intelligence
- Building and managing Security operations
- Threat hunting

Recommended Engagement: **Scoped per engagement**

ADDITIONAL SERVICES

The following services are charged via an annual subscription service.

THREAT ASSESSMENT

Check Point IRT offers a full threat assessment of your environment which highlights a customer's ability to protect the environment based on a full review of all deployed critical controls. The full threat assessment details the current configuration with a focus on the controls that are deployed, including all operational, management, and technical controls.

Elements of the assessment:

- Configuration review of all security controls utilizing custom audit tools to identify weaknesses in the security posture
- Threat monitoring device to determine current threats within the organization
- Threat landscape review utilizing threat intelligence to review threats to the environment
- Interviews with key personnel to determine controls in place and issues within the organization which are causing contention
- Review of deep and dark web data for external threat evaluation

After all information is gathered, a full written report is provided with recommendations and an action plan. This plan is typically the blueprint for the organization to use in mitigating identified issues. The typical assessment takes 40-80 hours, depending on the size and scope of the assessment.

COMPROMISE ASSESSMENT

This service evaluates your environment for the presence of malicious activity and provides a full set of recommendations, including the:

- Analysis of network, endpoint, and cloud environments for the key indicators of compromise
- Identification of compromised systems
- Full report of attacker activity
- Malware analysis and threat scope review
- Full briefing to technical and management teams on the impact of the compromise

Scoped per engagement based on network, endpoint and cloud environments

Deployment Tools:

- Network and endpoint inspection technologies (Customised Check Up/Endpoint Threat Prevention Agent)
- Threat Intelligence search (ThreatCloud)
- Review of threat preventions

One-month engagement to assess environment and one-month analyst time to provide assessment and full report

For more information, visit **Check Point Incident Response.**