Managed Incident Response and Digital Forensics

Your organisation needs a first line of defense. Our skilled cybersecurity professionals provide your organisation with the protection you need.

CARETOWER
An Integrity360 Company

THE PROBLEM & SOLUTION

The Problem

We live in a world of covert cyberwar between businesses and cybercriminals. Many organisations fall victim to state sponsored attacks or targeted cybercriminal attacks. Organisations often fail to detect security breaches in a timely manner, he average detection time during 2014 of an advanced adversary on a corporate network is 229 days*. Only 31% of organisations detect a breach by themselves whilst the remaining 69% are informed by a third party (law enforcement or public disclosure).

Without an army of trained cybersecurity experts, it is only a matter of time before your organisation falls victim to cybercriminals, state sponsored attacks or internal threats. Sophisticated attacks, such as spear phishing, put your network at risk. As acknowledged experts in our field we offer you a first line of defence in your cybersecurity protection. We offer a proactive service - planning and implementing an Incident Response and Digital Forensics program, to protect you against advanced cyberattacks.

The solution

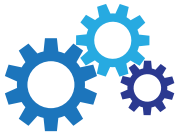
Setting up proper Cyber Incident Response capabilities within a company diverts valuable internal resource from core business activities. It is important to first understand the business needs to design a comprehensive strategy that delivers an effective response to cybersecurity incidents. At Caretower, our customers ' security and reputation is of paramount importance. Our approach to managing an Incident Response and Digital Forensics service, is shown in the following structured service:

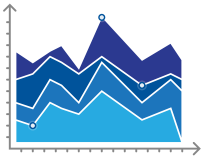
*Figures taken from Mandiant M-Trends report 2014

Preparation

01

Identify business goals
Evaluate current cybersecurity exposure
Prepare Incident Response strategy
Install and configure EnCase Endpoint Security





Detection and Analysis

02

Detect and respond threat alarms
Analyze incidents
Collect evidence

Containment

03

Prevent security incident spread – stop the lateral movement
Contain and isolate infected hosts
Kill covert channels of communication

Eradication and Recovery

04

Remediate infected hosts
Recover compromised systems
Harden security policies and measures

Lessons learned

05

Document all findings
Create a knowledge base to store information
Develop IOC's for enterprise-wide deployment

Caretower's Managed Incident Response and Digital Forensics service covers all aspects of Incident Response and Prevention as described by NIST-SP 800-83 and NIST-SP 800-61

WHAT YOU GET WITH OUR SERVICE

Managed Incident Response (MIR) and Digital Forensics (DF) benefits:

- **First line of defense** – from the MIR and DF services , you get our staff of skilled cybersecurity professionals looking after your internal security. Adversaries may be able to successfully exploit vulnerable software on your network, but they won't get past the incident response team who are constantly looking for indicators of compromise on your network.
- **Preparation** – from our experience, preparation is key for a successful incident response strategy. Our Incident Response service is based on NIST-SP 800-61 and 800-83 guidelines, adjusted to meet a higher standard. We enable your organisation to counter even the most sophisticated cyberattacks.
- **Protection against advanced adversaries** – a typical Advanced Persistent Threat (APT) is a state sponsored organism with the aim of stealing your intellectual property. Regardless of the nature of your business, we will ensure you stay protected at all times.
- **Live Incident Response** – We operate 24 hours a day, 7 days a week, 365 days a year. When we detect an attempt to compromise your network, our experts rapidly respond to block the intruder by all means possible, with minimal or no involvement from your IT team.
- **Hassle-free restoration** – restoration is often a resource intensive exercise and we understand that. We will restore the infected endpoints quickly, without any downtime or any involvement from your IT support staff. That's what sets us apart from other competitors in the market.
- **Excellent endpoint visibility** – using EnCase Endpoint Security, we are able to monitor all your endpoints for suspicious activity. Real-time dashboards give us the most recent relevant security information about your endpoints, without violating your privacy policies.
- **Conduct remote computer forensic investigations** – geographical boundaries are always a challenge when it comes to acquiring bit-stream image copies. The software we use is capable of capturing evidence located on any endpoint, regardless of location, as long as it is visible on the network. Evidence may be required for an internal HR investigation, a search warrant, disgruntled employee behaviour or a previously detected data breach.
- **Peace of mind** – we understand your constraints on time, funding and resources. The service we provide from our CSIR (Computer Security Incident Response) Team, will exceed your expectation, affording you peace of mind and a good night's sleep.

Features

Features	Basic	Enhanced
EnCase Endpoint Security Software	☑	☑
First line of defense	☑	☑
APT activity detection	☑	☑
Historical data and real-time visibility		☑
9x5 business days Security Operations Center (SOC) coverage	☑	
24x7x365 SOC coverage		☑
Standard reporting	☑	☑
Custom reporting		☑
On-premise installation	☑	☑
Live Incident Response	☑	☑
Alerting service	☑	☑
Hassle-free remediation		☑

Advanced Features - all of these are avaiable as a single add-on component and can be purchased separately:
10 investigations per year
Unlimited forensics investigations
Best-evidence in court
Expert-witness in court

** On-site forensics investigations service avaialble as a proffesional service day or as MSS add-on

Cloud Deployment Option
Cloud-based software deployment - Pricing is available on demand after scoping and solution design

Get in touch:

020 8372 1000

info@caretower.com

www.caretower.com