Managed Security Services

Leverage our experienced security operations team to improve your cyber security posture
Cyber security is no longer limited to protecting your business from reputation damage or loss of intellectual property. New data breach laws are also forcing organizations to review their strategy on preventing and mitigating breaches. Furthermore, successful and effective cyber security is not limited to implementing technology and policies, but is just as much about training, preparing staff and designing processes. The result is that organizations are (or soon will have to be) shifting to some form of security operations. The challenge is to get an optimal balance between people, processes and technology for in-house security operations. This has put us on a path where we are not merely providing Managed Security Services (MSS), but more often guiding and supporting our clients in their journey to develop their (in-house) cyber security capabilities and Cyber Security Operations Center (C-SoC).

FOX-IT uses its own advanced C-SoC to deliver Managed Security Services. With this service, we provide detailed insights into the risks and impact of cyber threats for specific organizations. Using this risk management information, our clients are better protected against cyber threats and can improve their overall security posture. Current information about new threats results in a more proactive security operation. Business decisions regarding security-related investments can then be based on facts.

For us, cyber security is very much a business oriented around people. We tend to form deep relationships with our MSS clients. It often becomes a process of cyber capability development. Helping clients to understand exactly what it takes to protect their environment, the amount of work it requires, and the decisions that we both need to make as a result of that proves very important. With so many targeted attacks on our customer base for instance, there are times that we have new type of attacks and run into unforeseen issues. Understanding what these issues are, how they materialize and how we can prevent or reduce them, is an important process and one that we embrace to develop top-end security practices. As we do this together with our clients, we strive to develop a security community that is constantly learning and adopting in terms of how to protect itself against the most advanced cyber attacks.
“Cyber security is people driven business.”
A familiar challenge

Cyber attacks are not an isolated spontaneous phenomenon: they are ultimately devised and executed by people for a specific purpose. Some are automated to a large degree; others are more tailored and sometimes get a lot of attention in the news. Human behavior cannot be captured and recognized by technology alone.

It seems obvious that attempting to prevent and mitigate advanced attacks conducted by people with technology only is not an achievable goal. And yet this has been the trend for some time. The simple reason for this is the economic reality of finding and retaining experienced information security professionals to conduct security operations. The benefits of security are difficult to quantify and security products are expected to solve security issues with minimal configuration and maintenance.

Change is inevitable: emerging legislation and increasing media attention on cyber attacks and security breaches are making the current approach unworkable in the long run. But how can you enhance security without incurring the costs associated with operating your own security operations?

Our approach
What systems should be able to do is provide usable feedback, options and context to cyber experts. Technology is an enabler rather than an objective: ultimately only skilled people can counteract the actions of dedicated, skilled and creative people. This is an inconvenient truth: technology and therefore cyber security is ineffective without threat intelligence and security professionals. This is exactly why security operations are essential for mature cyber security capabilities. Fox-it has been in the enviable position of growing its security operations and evolving with the changing conditions that challenge our clients for more than fifteen years.

During this period, our service has evolved to providing our clients with a great degree of protection through our tailored approach to delivering our innovative managed security services.

It starts with asking the right questions
Experienced information security professionals know that complete prevention of security breaches is usually not economically viable, if not downright impossible. But as an organization, you should, in any case, ensure optimal defenses appropriate to your threat and risk profiles. Sometimes attackers will spend millions to steal certain data, while the attacked organizations try to protect themselves with solutions at a fraction of that cost.

If you want to protect the continuity, finance, intellectual property and reputation of your business, the answers to the following questions are vital:
1. **What threats are you protected against at this time?**
What threats exist? Which data are of vital importance to your business continuity, your financial situation and your intellectual property? What is the status and cover of your protection? Which attacks have already occurred against your organization?

2. **Are you aware of all attacks, and to what extent are you protected?**
Do you have insight into any and all of the attack phases, or just the end of the attack chain? Does your security architecture offer an insight into both known and unknown attacks? Are you able to investigate attacks or just prevent them? Can you recognize suspicious patterns in data flows?

3. **What is the business risk of incidents (lessened at an early stage or not), and how can you deal with it?**
What is the relationship between the malware and your business interests? Do you have sufficient context for the attacks to be able to define possible business risks? How quickly are you able to respond to attacks? Do you have an action plan for cyber incident response?

The answer to such questions determines our tailored approach to your security needs.

**The core of our operations cycle**
Once we have a clear picture of how a digital environment is organized, our analysts start looking at the events produced by both existing and our proprietary security technology. To keep our response time very low, we rely on a variety of analytics to generate high-probability events that our analysts will investigate. These events will become cases when there’s sufficient indication of potential malicious behavior. Analysts then seek to determine whether or not this is worth to investigate further.

Arriving at this triage decision quickly is a crucial aspect of a short response time. Our technology covers multiple vectors, including the network, endpoints and events produced by other (security) components. This data is abstracted to a common intelligence oriented language that allows our analysts to do rapid triage analysis. If it becomes a case investigation, analysts will then build a case by adding sightings, objects and other evidence to a case until it is considered actionable for mitigation.

As soon as the determination is made that a case is malicious, analysts will contact predefined persons within the client’s organization, based on where the incident took place and the assets involved. Following this initial triage, the case is expanded until it is considered complete and actionable. All evidence added to the case are linked, and add context to future cases and enhance analytics in the future, further improving our detection capability.
Three types of Managed Security Services

In FOX-IT’s Security Operation Center (SOC), our dedicated security specialists closely monitor the digital environment of our clients. They detect and research cyber threats and suspicious activities such as advanced hacking attempts, data leaks, signs of Advanced Persistent Threats (APTs) and virus outbreaks.

In cases of imminent threats, our clients are informed within minutes and receive detailed advice on what measures to take. This way, you are notified about acute cyber threats and the potential impact of these threats on your business and daily operations.

Be in control of your cyber security with the FOX-IT SOC

As a trusted security partner, we assist our clients in making the right choice in order to optimally manage their information security. Clients can utilize our monitoring information to refine their security policy in order to improve preventive measures and overall maturity level.

For those clients who want to take a hands-on approach to security operations, we offer a hybrid service delivery form. This enables clients to conduct their own operations with support from the Fox-SOC. Some clients prefer this option to get assistance with their own SOC operations or use the Fox-SOC for operations outside of office hours or help them build their own SOC operation in the future. FOX-IT’s Managed Security Services are based on a proprietary Cyber Threat Management platform, which integrates with our clients’ existing security infrastructure to deliver one of the following three types of services:

1. **Dedicated SOC** Customers use 24/7 detection and analysis capability offered through the FOX-IT SOC.

2. **Hybrid SOC** The hybrid SOC model offers a unique solution for organizations to gain knowledge about advanced security monitoring. Along the way, clients become more skilled in dealing with cyber threats. Gradually, they can take over more and more tasks. In general we transition to perform only the more specialized tasks requiring specific knowledge.

3. **On premise SOC** In the situation where there is a SOC within your own organization, FOX-IT can offer a tiered SOC capability, allowing for extension of both resources and threat intelligence services.

FOX-IT supports clients with specific training programs to gain knowledge and improve capabilities to take the next step without any concern whatsoever. Not only will we provide our technology and expertise, we can also assist in assessing, training and the professional development of SOC staff through our FoxAcademy. As we guide and support clients in the process of building and developing their (in-house) security operations, we focus on striking the balance right between people, processes and technology. This has put us on a path where we not merely provide Managed Security Services (MSS), but actually guide and support our clients in their journey to develop their (in-house) cyber security capabilities. This way, our clients can fully benefit from the flexibility and added value of our Managed Security Services.
Three service levels

**Silver**
- 24/7 security monitoring service
- Three quarterly WebEx briefings and one annual face-to-face meeting
- Two in-depth examinations of incidents per year (2x4 hours)

**Gold**
- 24/7 security monitoring service
- Two quarterly WebEx briefings and two annual face-to-face meetings
- Four in-depth examinations of incidents per year (4x4 hours)
- Early access to sector threat briefing

**Platinum**
- 24/7 security monitoring service
- Four quarterly face-to-face briefings
- Eight in-depth examinations of incidents per year (8x4 hours)
- Access to threat analyst team
- Assigned threat management advisor
- Early access to sector threat briefing
- Company specific threat briefing
- Monthly threat briefing via conference call
Our clients have a wide array of reasons to choose FOX-IT as a trusted security partner to optimally manage their information security.

**Transparency through technology**
Fox-IT has developed its own technology from the ground up. As we developed our own cyber security proposition, we found the available commercial solutions lacking the capabilities we required. As a result, we deploy our own Cyber Threat Management Platform (CTMp) technology for the highest efficiency and investigative capability. But it’s not just for our own benefit: it gives clients the possibility to look over our shoulders as we analyze incidents, generate intelligence and perform your own (additional) analysis.

**An intelligence partner for situational awareness**
Our service goes beyond providing information about threats. As part of our Managed Security Services (MSS), we actively share knowledge with our clients. Our MSS clients receive relevant security news, even before the information is made known to the public. They also receive detailed advice about what mitigation measures to take.

FOX-IT security experts provide detailed insights in relevant security trends. New threats are explained and clarified. Clients will learn how to deal with these threats in a proactive manner. This increased situational awareness enables them to improve their information security level and cyber security strategy.

The Cyber Threat Management portal provides real time incident- and trend information. Our clients will also receive a monthly report with all the relevant information in one summary.

**Incident readiness**
Our Managed Security Services provide incident readiness as a matter of course: in order to provide in-depth analysis as part of our service we employ forensic data retention. This permits retroactive indicator of compromise (ioC) checking and it permits very detailed reconstruction of breaches, which paves the way for rapid mitigation and process improvement. Our detailed case management system also ensures that investigations are well documented to substantiate findings in relation to emerging data breach laws.

**Actionable case reporting**
FOX-IT’s forensic (Forensic Experts in IT) background has inspired our technology and the Managed Security Services based on it. Our analysts don’t merely report alerts produced by systems. We show what happened before and after the fact, and provide context and commentary that allows our clients to immediately prioritize the mitigation actions and improve their security in a measurable way. In addition to providing context, and contrary to many managed security providers, we pride ourselves on only reporting only true positives to our clientele.
Rapid response with our CERT team
Easily pivot to our experienced CERT team: In case of targeted attacks directed at our client’s organization, the FoxCERT team is standing by to conduct further investigation and help them deal with even the most advanced state sponsored threats. With knowledge about your digital assets, infrastructure and processes, and access to proven technology already in place, our CERT team is ideally positioned to help clients deal with incidents in short order.

Scale up with hybrid delivery
Our CTM$ technology supports a hybrid service delivery model that enables our clients to start with a fully managed services offering. And granularly take operations in-house, as their overall Cyber Threat Management capabilities develop. Secondly our clients can choose to start directly at the level of operations that they feel comfortable with on taking in-house. We also provide the training necessary to develop in-house staff for this purpose.
Be ready for today’s cyber threats with FOX-IT’s Managed Security Monitoring

- **Always be prepared** for cyber incidents with 24/7 security monitoring and instant incident reporting.
- **Only be notified in case of real cyber threats.**
- **SOC experts are directly available** for detailed advice about what measures to take for an optimal information security posture. You will receive immediate advice during incident escalations and scheduled security briefings.
- **Layered defense:** monitoring of known and unknown threats through a combination of network, endpoints, honeypots and/or log file collection.
- **Our service level is always at a high level** because of the economies of scale. This service is in the very capable hands of highly experienced security analysts working with high quality threat information.
- **It is more cost-efficient than running your own monitoring service**, which requires continuous investments in personnel, technology and intelligence.
- **With the Cyber Threat Management platform (CTMp), you can look over the shoulders of our analysts**, seeing what they see and, optionally, doing what they do.
- **If your organization aspires, we provide you with a solid transition path towards an independent or hybrid SOC through our training programs and the use of our CTMp.**
- **The service can be operational within several days** and has minimal impact on daily operations, especially when compared to other solutions needing significant longer implementation times. When organizations do not have FOX-IT MSS in place to encounter incidents, this fast installation routine is very appreciated.
- **In case of targeted attacks, our FoxCERT team is standing by** to start an in-depth investigation.
“Cyber threats pose one of the most serious economic and national security challenges to the United States, and my Administration is pursuing a comprehensive strategy to confront them. As we have seen in recent months, these threats can emanate from a range of sources and target our critical infrastructure, our companies, and our citizens.”

President Barack Obama – April 1, 2015 – www.whitehouse.gov

If you are interested in our products or services, please send an e-mail to fox@fox-it.com

If you have an account manager already, please contact him or her directly.
FOX-IT prevents, solves and mitigates the most serious cyber threats with smart solutions for government, defense, law enforcement, critical infrastructure, banking and multinational corporations worldwide. It’s our mission to develop technical and innovative solutions that ensure a more secure society. We accomplish this by offering advanced cyber security solutions and services that are trusted by governmental bodies and large enterprises worldwide. We have a strong focus on innovation and a tireless dedication to our clients, our values and our integrity.

As advancements in Internet technology expand opportunities for misuse by increasingly sophisticated cyber criminals, state actors and terrorists, FOX-IT is continuously at the forefront of protecting our customers against these threats.

Part of NCC Group
We are part of global cyber security specialist NCC Group, which we joined in November 2015. Being part of a global organization with 15,000 customers, 32 locations worldwide and more than 1,600 employees brings many advantages, including the ability to provide 24/7 assistance for our customers.