GUIDE TO DETECTION & RESPONSE

RETHINK YOUR CYBER RESILIENCE STRATEGY
E-BOOK
From the field

Over the last few years, you’ve probably heard phrases such as “the tactics, techniques, and procedures crafted by highly resourced threat actors are falling into the hands of less skilled adversaries”. That’s long speak for “expect a lot more script kiddies to start pwning your systems”. As Dr. Ian Levy from GCHQ recently pointed out, a lot of the attacks we’re seeing nowadays aren’t “Advanced Persistent Threats”, they’re simple hacks performed by “Adequate Pernicious Toerags”.

Nothing illustrates this phenomenon better than the group we’ve dubbed “The Romanian Underground”. This is a group that we have had first-hand experience with on a number of occasions while performing incident response and forensics work.

The Romanian Underground are, simply put, a bunch of IRC chat room buddies who decided it would be cool to take up the hobby of “hacking”. Most of these kids, upon joining the collective, have little to no Unix skills to speak of. They probably know about five commands in total. Newcomers are taken under the wing of a mentor who provides them with simple tools and training to get them started on their new hobby. These mentors are almost as unskilled as the newcomers - they probably know about five more Unix commands than their apprentices. But they’ve been in the game for a few weeks already, and have a wealth of experience.

As newcomers learn the ropes (which usually implies that they’ve learned to configure and use a couple of tools), they’re promoted to mentors, and take on their own set of apprentices. This hierarchical model closely resembles popular pyramid selling schemes you might have heard of. Of course, the guys involved in The Romanian Underground aren’t looking to become millionaires by selling soap - the pyramid scheme is a form of gamification, where the goal is to collect as many owned systems as possible and move up the ranks.

Naturally, it’s the guys at the top of the pyramid who really benefit from all of this. They’re the ones providing the tools, and by pushing all their manual work down-stream, they get access to thousands of compromised systems. Meanwhile, the newcomers are happy to proudly identify themselves as “hackers” on their Facebook pages (alongside other unrelated hobbies such as windsurfing or snowboarding).

The toolkits being pushed down the pyramid are usually designed to exploit or brute force common services such as SSH and webmail servers. What might surprise you (or not) is that these toolkits, in the hands of completely unskilled noobs, are being used to compromise PCI-DSS-compliant organizations across the globe. The Romanian Underground represent just one of many groups that form part of a growing trend of low-skilled hackers and cyber criminals. The motives of the masterminds behind these groups are, you guessed it, financial gain. Acquiring access to a large number of compromised company networks allows them to cherry-pick prime targets for cyber extortion and data exfiltration. And any company is a potential target.

The fact that these groups are able to compromise PCI-DSS-compliant organizations is a testament to the fact that purely preventative cyber security solutions simply aren’t cutting it anymore. And the reason why so many companies are now being owned in this style is due to the fact that they simply don’t have an ounce of visibility into post-breach activities on their networks.

That’s not to say that skilled attackers aren’t also out there. But, as a company that’s been involved in more European cyber crime investigations than any other company in the world, we can tell you that there’s no point in worrying about the NSA or APT28 until you know you can at least stop these guys.
In our experience, most companies only discuss cyber security as it relates to the broader topic of risk management. While performing risk analyses, companies identify threats or risks relevant to their organization and then prioritize them based on likelihood, impact, and cost to mitigate. When addressing cyber threats, we’ve noticed a potential disconnect between the risk that companies perceive and the reality of the situation. We’d like to help clear that up.

Sophisticated cyber attacks tend to start at the top and work their way down. It’s the opposite of “low-hanging fruit.” When new types of attacks are discovered, they’re usually attributable to highly resourced threat actors (i.e., nation states). These adversaries, by default, go after the highest-value targets first. As the tactics, techniques, and procedures (TTPs) used in such attacks become public knowledge, they trickle down into the hands of less organized cyber criminals. New TTPs first see use against heavy industry and finally, everyone else (manufacturing, retail, SMEs, etc.).

Threats to an organization aren’t limited to attacks from the outside. Accidental and intentional leaks can and do originate from company insiders with enough access to critical or confidential assets. Upstream attacks, where a partner, supplier, or contractor are compromised by an attacker looking to establish a beachhead in an adjacent organization are also very common. In several incident response cases we’ve been involved with, even physical intrusion of a company’s premises was used as part of the attack vector.

Cyber attacks come in many forms, ranging from commodity malware (such as ransomware) to highly skilled attacks performed by nation-state actors. We’ve broken these threats down into separate categories.

### Commodity threats

Commodity threats are highly prevalent, and have been for decades. A company’s chance of encountering commodity threats is, therefore, extremely high. However, due to their prevalence and long history, there are plenty of good software solutions available designed to protect against these threats. And these solutions work as intended. If a business is hit by a commodity threat (such as crypto-ransomware), the impact is usually fairly low. Most of the time it’ll be blocked by endpoint protection software. If it does get through, there are two options – pay the ransom or fix the problem. Don’t pay the ransom and a handful of staff will lose some productive work time. Pay and, most of the time, you’ll get the data back. Ransom amounts are low by company standards. So, the likelihood of seeing a commodity threat is high, the impact tends to be low, and the mitigation cost is basically free (we assume you’re smart enough to be running an endpoint protection solution already).

### Cyber crime

Cyber crime represents the next category on our risk assessment scale. This category moves beyond the realm of commodity malware threats, and onto targeted attacks. Companies are selected as targets for various reasons. In some cases, a victim is chosen because they are “broadcasting” themselves via weak or vulnerable infrastructure. Other targets are selected simply because the attacker has taken interest in a particular organization, for one reason or another.

Cyber criminal attacks are often opportunistic - the attacker has an easy way in, sees an opportunity to make money, and takes it. Cyber crime is by-and-large financially motivated. Once the adversary has breached the target’s network, systems or data will be held for ransom. We refer to this phenomenon as “cyber extortion”. These types of attacks are very much on the rise, and can target organizations of any size, from SMEs to large enterprises.

We predict that the introduction of the NIS and GDPR regulations will further embolden cyber criminals and cyber extortion schemes. Once these regulations are in effect, companies may be more willing to fork over a ransom, in order to sweep the news of a breach under the rug rather than face the expensive task of responding to and reporting the incident.
Cyber crime can be broken down into roughly two categories – organized and non-organized. Organized cyber criminal groups are very close, in terms of sophistication, to nation-state actors. The Bangladesh bank attacks of 2016 are a good example of organized cyber crime. Non-organized cyber criminals often run as lone wolves. They have less resources, and their skill can vary. The Romanian Underground falls into this category.

Two years ago, we’d have rated the likelihood of falling prey to cyber criminals as low. Today, the likelihood is medium, and on the rise. The financial and business impact of a targeted cyber crime attack can vary. In many of the cases we’ve responded to, ransoms demanded by non-organized cyber extortionists only ran into the tens of thousands of Euros - not a hefty sum for most organizations. But we don’t imagine that any organization would simply pay the ransom and go about their business. The knowledge that an intruder is in their network is going to be enough to call in an incident response team to sort out the situation.

If an adversary manages to exfiltrate important data, the costs of a cyber crime incident can really start to skyrocket. This is especially true if customer data was involved. No matter what, a breach is most likely going to incur reputational, legal, PR, business, and internal productivity costs. And the considerations are no longer limited to protecting your business and its sensitive data, but regulatory bodies like the European Union have made new requirements. For example, the EU’s General Data Protection Regulation (GDPR) requires organizations to be adequately prepared to detect, respond and report personal data breaches within 72 hours.

Nation state
Companies that worry about being targeted by nation-state attacks typically know who they are. They also know that defending against a nation-state attack is almost impossible. Regardless, they’re forced to try (since they can’t afford not to). The impact of nation-state attacks can vary from having top secret intellectual property stolen by overseas competitors or governments, to having your nuclear enrichment halted when centrifuges are destroyed, like in Iran.

"TARGETED ATTACKS DON’T CARE ABOUT YOUR ‘NEXT GEN’ PRODUCT, NO MATTER HOW SHINY THE VENDOR CLAIMS IT TO BE. TO BE BLUNT, THE SOLUTIONS THEY’RE SELLING ARE FIXING THE WRONG PROBLEMS."

DON’T BELIEVE THE HYPE

Getting to the point of why we presented this risk analysis, we’ve noticed that there’s still a very strong marketing push towards endpoint protection solutions. We’ve seen “next gen” vendors claim that their solutions can prevent targeted attacks. Some even foolishly claim that breach detection is irrelevant, since it’s already “game over” if a threat gets through perimeter defenses.

It’s all very misleading.

Targeted attacks don’t care about your “next gen” product, no matter how shiny the vendor claims it to be. To be blunt, the solutions they’re selling are fixing the wrong problems.

Given this huge marketing push from “next gen”, we’re not really surprised to see that very few companies we’ve spoken to are aware of the need for breach detection and response capabilities. And therein lies the problem. Organizations are way too distracted to realize that they should start investing in breach detection and response, instead of another layer of protection against commodity threats (although the adversaries would love you to do this). Let’s put it this way - would you rather have your next incident involve cleaning malware off a laptop in your sales department or dealing with a full-blown data breach?

But don’t just take our word for it. Gartner predicts that “by 2020, 60 percent of enterprise information security budgets will be allocated for rapid detection and response approaches, which is an increase from less than 30% in 2016.” So, ask yourself this: how much of your budget have you allocated to breach detection and response capabilities. And therein lies the problem. Organizations are way too distracted to realize that they should start investing in breach detection and response, instead of another layer of protection against commodity threats (although the adversaries would love you to do this). Let’s put it this way - would you rather have your next incident involve cleaning malware off a laptop in your sales department or dealing with a full-blown data breach?

BY 2020, 60 PERCENT OF ENTERPRISE INFORMATION SECURITY BUDGETS WILL BE ALLOCATED FOR RAPID DETECTION AND RESPONSE APPROACHES, WHICH IS AN INCREASE FROM LESS THAN 30% IN 2016.

Gartner ‘Special Report Cybersecurity at the Speed of Digital Business’ Paul E. Proctor, Ray Wagner, 30 August 2016, refreshed December 2017
Cyber threats are asymmetric in nature. An attacker only needs to succeed once to gain access to a network. Defenders must succeed one hundred percent of the time if they want to keep them out. You can’t rely on being successful all the time.

And yet this is what most companies are doing. Traditional perimeter defense technologies, such as firewalls and endpoint protection software do a good job at what they’re meant to do - namely detecting and blocking real-world and commodity threats. But you can’t expect these solutions to stop advanced adversaries. Any adversary worth their salt will craft an attack designed to bypass those defenses. And they won’t even need to use malware to gain a foothold in the organization (contrary to what you might have been told, skilled attackers rarely, if ever, use malware).

Cyber attacks commonly follow the same pattern. Attackers start by breaching the perimeter of an organization with spear-phishing, waterhole, or man-in-the-middle attacks. Sometimes attackers may gain entry by exploiting a vulnerability in a public-facing system, or even by purchasing access to an already compromised system. Once inside the perimeter, adversaries perform reconnaissance, elevate privileges (by exploiting misconfigured or vulnerable systems), hunt for domain admin access (such as Mimikatz), and move laterally onto password (using memory-scraping tools able systems), hunt for domain admin (by exploiting misconfigured or vulner

WHICH STRATEGY IS RIGHT FOR YOU?

Of all the challenges that organizations face while building breach detection and response capabilities, nothing really compares to the difficulty they face when trying to hire and retain good cyber security expertise. It is estimated that right now, there are at least two cyber security jobs for every one person working in the field. This problem is expected to become even more acute in the future. The only way you’re going to get valid data from an in-house intrusion detection system (IDS) is by having experts on staff. The same goes for keeping up on threat intelligence, configuring systems, red-teaming, and responding to incidents correctly. So, you’re probably going to need more than one or two experts on your payroll.

And while you could eventually develop your own in-house team, systems and expertise, in most cases it means taking on a lengthy and expensive project. Finally, operating your own 24/7 Security Operations Center (SOC) with adequately skilled resources may push the total cost of ownership to the level only the largest enterprises are prepared to invest.

With a lack of skilled defenders on their side, and with the difficulties and cost associated with building their own breach detection and response capabilities, companies are battling cyber attacks and losing. This is why F-Secure has spent the last few years developing and perfecting managed detection and response services for the varying needs of companies - to bring our world class cyber security expertise within reach of every organization.

Our services don’t just provide human expertise, though. They are built on top of threat intelligence, sample analysis, and decision-making technologies that have been developed in-house for over a decade. And while an organization could eventually develop their own in-house systems and expertise to the levels a very we’ve reached, it would take them a very long time.

Our managed detection and response services are available with different service levels and models to fit an organization’s needs, whether enterprise or midsize. We invite you to consider the following three alternatives.
OPTION 1:  
Do it yourself (with option to augment your team)

Many organizations have the resources to invest heavily in their own security teams and infrastructure. But even well-invested enterprises with their own SOC may find value in augmenting their own team with a vendor that exclusively provides cyber security services. An extended team working alongside your IT team can help you overcome the issue of hiring and retaining a big enough IT security team.

Not every company who handles detection and response in-house necessarily has staff working 24/7 protect their operations. Such organizations may find it useful to invest in an endpoint detection and response solution that helps their IT team identify attacks during business hours, and also provides coverage outside business hours with automated response to isolate attackers. Such an approach can be enough to quickly determine the scope of an attack, identify whether or not any personal data was affected, and be able to meet the regulatory requirements to report data breaches within 72 hours as required by the GDPR.

OPTION 2:  
Managed Detection and Response with F-Secure for 24/7

To overcome the difficulty of trying to hire and retain qualified cyber security expertise, F-Secure offers fully managed detection and response (MDR) services. What we mean by “managed” is that there’s a minimal installation process on your side to get things up and running, and after that, everything from breach detection to response is handled by us. Our teams of threat hunters, incident responders and forensics experts are available around the clock for a fully managed breach detection and response service we call Rapid Detection & Response Service (RDS).

With Rapid Detection & Response Service you will have the benefit of F-Secure’s world-class cyber security experts monitoring your network 24/7. They will review all detections within minutes and determine severity before alerting your team. False positive detections are flagged immediately to ensure your team only spends time on real threats. Working with our cyber security experts means all detections come with guidance and if needed, further clarification. The availability of human expertise means your team will spend significantly less time on detections.

Rapid Detection & Response Service doesn’t just provide human expertise, though. It’s a service that’s built on top of threat intelligence, sample analysis, and decision-making systems with machine learning and artificial intelligence capabilities that have been developed in-house for over a decade. And while an organization could eventually develop their own in-house systems and expertise to the levels we’ve reached, it would take them a very long time.

Augmenting your own team’s availability and skills with F-Secure’s Rapid Detection & Response Service help to easily reach 24/7 availability with 30-minute service level and receive expert guidance to respond whenever under an attack.

OPTION 3:  
Managed Endpoint Detection and Response with a Local Service Provider

An alternative approach to managed detection and response is an Endpoint Detection & Response (EDR) solution like F-Secure Rapid Detection & Response, which is delivered by certified and trained service provider partners.

F-Secure trains our local managed service providers to support you in everything from monitoring your IT environment’s health and security status, to detecting and guiding you in response actions in the case of a breach. The local service provider is backed by automation that can be used to extend their availability beyond covering business hours, and is also supported by F-Secure’s experts to handle even the most complex cases.

Many companies find a local managed service provider is the most suitable option to help keep their operating costs low. Based on our experience, these tend to be small and midsize organizations.

Even if your enterprise is a well-invested with your own SOC, you may still consider augmenting your own team with a managed detection and response service to reach 24/7 availability and below 30-minute detection to response time.

BUILDING IN-HOUSE BREACH DETECTION AND RESPONSE CAPABILITIES IS DIFFICULT

We’ve noticed that, for most organizations, setting up in-house breach detection and response capabilities tends to be a complicated, time-consuming, and expensive endeavor. There are multiple components that need deploying and configuring. All of them are expensive, so purchasing decisions take time and research. Different components may or may not interoperate well, so you have to figure that out, too. Then you need to select threat intelligence feeds, and there are dozens if not hundreds of those available. Deploying and configuring these systems is a complicated job. And at the end of all this, you’ll be left wondering if you’ve got everything covered and whether or not all the pieces are talking to each other properly. And that’s just the initial install. After that, systems, rules, and feeds need to be constantly improved and modified as the world changes.

Responding to a breach is usually also a lengthy and expensive process that requires expert data forensics and incident response work. A typical response scenario includes removing the adversary from the network, cleaning up or restoring affected systems, resetting compromised accounts, determining where the intruder has been, and determining what the intruder has done. Most companies don’t have the in-house expertise or capabilities to perform these types of activities, and so must call on a third party to help.
Because expertise, monitoring, threat hunting, and response capabilities are covered by F-Secure or our service providers, once you’ve decided to implement the service in your organization, all you need to do is install simple sensors on your organization’s endpoints. The time from initial deployment and configuration to actual breach detection and response capabilities is less than a week. In fact, we’ve been told by several customers that we have the easiest system they’ve ever worked with.

The alternative to deploying a managed breach detection and response service is a lengthy (in most cases 3-5 years) and expensive (multi-million Euro) project of purchasing, deploying, and configuring dedicated systems, and hiring and training a sizeable staff.

But a managed approach to detection and response isn’t just about a fast return on investment. We’ve seen many companies go to the trouble of building a SOC and setting up an IDS and SIEM, only to still not catch threats. This is because, in our experience, finding actual threats is like looking for a needle in a haystack.

To illustrate with a recent real-world example, in a 1000-node customer installation, our sensors collected around 2,000,000,000 events over a period of one month. Raw data analysis in our back end systems filtered that number down to 900,000. Our machine learning systems and Broad Context Detection™ mechanisms then narrowed that number down to 25. Finally, those 25 events were analyzed, where 15 real threats were discovered (and verified by the customer).

The thing is, if you go with your own IDS/SIEM solution, it’s your organization that will need to process those 900,000 events. And that’s why we’ve gone to countless customer sites and found threats on their network, despite those customers already running very well-known IDS solutions. Combing through the noise and false positives is difficult, and can cause fatigue in even the most diligent of analysts.

In order to process this volume of events, you also need reliable, up-to-date threat intelligence. At F-Secure, we have our own in-house sources. And after over 30 years in the business, we also have a massive historical sample collection that even gives us the ability to find relevant threats left undiscovered from currently active threat actors. Our researchers do both threat intelligence investigations and reverse engineering. This gives us both high-level knowledge of the global threat landscape and in-depth technical knowledge of the threats themselves. Instead of studying each threat independently, we identify relationships between threats, allowing us to understand the capabilities and motives of an adversary. We focus on the puzzle and not just on the individual pieces.
At the core of F-Secure’s approach to advanced threat protection is our Rapid Detection & Response Center (RDC), which is the base of operations for all of our detection and response services. At RDC, cyber security experts work on a 24/7 basis, where they hunt for threats, monitor data and alerts directly from our Rapid Detection & Response Service customer environments, flag anomalies and signs of a breach, and then work with our customers to respond to real incidents as they take place. They also support our certified F-Secure Rapid Detection & Response service providers when their expertise is needed to resolve the most demanding cases.

RDC staff have access to our own in-house, world-class analytical and threat hunting tools, all of our threat intelligence data, and a wealth of information and knowledge from both our Cyber Security Services and F-Secure Labs organizations. In fact, all of these teams work closely in cooperation with each other.

Staff at our Rapid Detection & Response Center are trained to handle a variety of tasks. We also train our managed service providers in many of these tasks. The main tasks fall into roughly three different roles - threat hunters, incident responders, and forensics experts.

Threat hunters
Threat hunters are our first responders. They monitor the service and hunt for threats. When a threat hunter discovers something suspicious, evidence is collected to verify the incident. If a real incident is discovered, it is given a priority. High-priority alerts are generated when there’s a strong indication of an ongoing breach, and in these cases, the customer is immediately contacted by phone. For non-critical cases, guidance is sent to the customer by email. Threat hunters also keep the customer up to date on any ongoing investigations.

Incident responders
Incident responders are assigned complex cases that customers are unable to handle on their own, and may assist the customer either remotely or on-site. Incident response personnel can assist with a range of technical and non-technical response activities, depending on customer needs. We are also familiar with collecting evidence for law enforcement purposes, should it be required.

Forensics experts
Forensics experts are specialists tasked with the most difficult of cases. F-Secure is one of the few organizations globally who have a very wide range of forensic tasks, ranging from internal network triage to deep reverse engineering of unique malware samples. This allows us to handle even the most complicated nation-state originated attacks.

F-Secure’s detection and response service capabilities are primarily developed using an iterative, red-teaming approach. In short, we have our guys attack systems, figure out what the service didn’t catch, and make improvements. Some improvements are made by hand. Others are learned by our backend systems during the red-teaming exercises. As part of this process, we document and visualize the various attack chains used, which allows the red-teams to come up with new, more devious attack methods.

Our first recommendation to customers who have just purchased F-Secure’s detection and response service is to bring in a third party and run a red-team exercise against our service. Not only does it help you verify that everything has been correctly set up, it allows you to see the process in action, which is a nice way to practice for a real incident.

On the subject of red-teaming, we’ve challenged third parties to bypass F-Secure’s detection and response services, but none have managed to do so yet. But there’s more. There are at least seventy companies out there that claim they can detect and remediate any targeted attack. In our experience, there are very few that actually can. How do we know? Well, so far, we have a flawless success rate on corporate exposure assignments (where a customer ordered a targeted attack from us). In every single case, we successfully breached organizations running our competitors’ products. And none of those products detected our attacks. We’re not going to name any names.

At F-Secure we recognized that protecting our customers from advanced threats requires more than world-class technologies built around artificial intelligence. The best way to provide an unequalled breach detection and response capability is not to build just an advanced threat hunting tool, it’s to combine both man and machine with machine learning systems and cyber security expertise.

We recognized early on the difficulties other companies had in building their own breach detection and response capabilities with a DIY approach, and decided to take the managed service route. We also recognize the different needs various organizations have, so we designed our managed services to be available with different service levels and models to deliver the service. F-Secure’s team is available 24/7 and can provide world-class services with a 30-minute response time after detecting a real threat. Our certified managed service providers also have different service levels, like availability only during local business hours supported by round-the-clock automation.

We recommend organizations calculate their return on investment (ROI) with alternative approaches before simply jumping into purchasing a piece of technology, or hiring a sizeable team required to operate the technology. It can be difficult to reach a positive ROI for building your own capabilities, especially after the necessary human expertise has been also considered.
When a targeted attack occurs, you will need a bigger picture than a detection from one impacted host can provide. In order to fully understand the true severity of each attack, you will need to discern the broader context, and to do it quickly.

To overcome the issue of having too many raw data events for a human to process, F-Secure has developed behavioral data analysis to narrow down the data, along with Broad Context Detection™ mechanisms to build context around all relevant events across impacted hosts. Broad Context Detection™ helps people easily understand the targeted attack by visualizing the set of circumstances around an attack, and even provides recommended actions for how to respond. Broad Context Detection™ is a prime example of F-Secure’s “man and machine” approach that empowers people to stop the attack swiftly, or even define automated response actions when the team is off work.

F-Secure’s detection and response services are also designed to look for the existence of newly discovered threats in historical data. Retrospective threat hunting is achieved when new detection algorithms are run against historical data collected from each of our customers. This mechanism is especially useful when dealing with attacks from more advanced adversaries (that may have gone hidden for some time).

F-Secure’s solution can be deployed during ongoing incident response work, and is used as a threat hunting service that can quickly gain visibility into a network that has already been breached.

Finally, the services continue to work outside of the corporate network. In a world where the classical security perimeter is crumbling, traditional IDS approaches have become ineffective (since they typically only work on the edge of the network). These traditional approaches cannot track threats when devices are outside of the corporate network, or when people utilize cloud-based services. Our endpoint sensor approach solves this problem rather effectively. What’s more, we’ve been working on extending the service capabilities into cloud services, such as Salesforce.
THREAT HUNTING AND DATA SCIENCE

Unlike the traditional approach of creating and applying a set of detections based on known “bad” behavior, we run actual attacks against our systems and train them on what “good” behavior looks like. We then flag everything else for further analysis and false-positive filtering. This, we believe, is the approach that most other breach detection vendors will also settle on in the future.

Threat-hunting systems need to be able to adapt to changes quickly. Everything in a monitored environment is in flux. People and devices come and go, operating systems and software get patched. New threats and TTPs emerge. Due to the nature of this flux, traditional IDS solutions tend to be “noisy” and prone to false alarms. These same traditional solutions are also always one step behind the threat landscape.

In order to tackle this problem, our data scientists, working alongside the experts at RDC, have designed and built a series of backend statistical analysis, machine learning, and expert systems to support our analysts. The core of F-Secure’s backend is very simple, and all of the complexity is embedded in surrounding algorithms. This approach enables very fast deployment times for new detection algorithms (in minutes) and allows us to adapt to changes quickly. With F-Secure’s detection and response service in place, there’s never a need to wait for the systems deployed on your own premises to receive updates — all the logic is in our backend systems.

Our analytics systems perform a number of tasks, from analyzing and learning behaviors in monitored environments to reducing false positives. Different analysis techniques are better suited for different tasks. For instance, an expert system is best suited to find the sort of behavior caused by common attack tools and by the TTPs employed by cyber criminals. These include PowerShell commands and malicious URLs and IP addresses. Machine-learning systems are designed to spot previously unknown bad behavior, such as DHCP hijacks, spoofing, and other stealthy evasion tactics. We also utilize different multi-level combinations of expert systems, statistical analytics, and machine learning.

We’ve found that simple statistical analytics are best suited for eliminating false positives, and by applying these methods, we currently eliminate approximately 80% of all irrelevant alerts. The way we’ve built these systems and the way they interact with each other is quite unique, and something we’ve not seen elsewhere in the industry.

This combination of artificial intelligence and cyber security specialists is about the most efficient and accurate configuration we could come up with for working with the event data we receive. And it allows us to spot attacks before they have a chance to do damage or access business-critical data.
 Nobody knows cyber security like F-Secure. For three decades, F-Secure has driven innovations in cyber security, defending tens of thousands of companies and millions of people. With unsurpassed experience in endpoint protection as well as detection and response, F-Secure shields enterprises and consumers against everything from advanced cyber attacks and data breaches to widespread ransomware infections. F-Secure’s sophisticated technology combines the power of machine learning with the human expertise of its world-renowned security labs for a singular approach called Live Security. F-Secure’s security experts have participated in more European cyber crime scene investigations than any other company in the market, and its products are sold all over the world by over 200 broadband and mobile operators and thousands of resellers.

Founded in 1988, F-Secure is listed on the NASDAQ OMX Helsinki Ltd.