Whitepaper

WITH secure

Automating advanced threat identification with Broad Context Detection™

Contents

Paradigm shift in detecting cyber attacks

Every company is a target. Small businesses increasingly face the same cyber security risks as larger companies, with most organizations experiencing a data breach at least once a year. Any organization not running a breach detection solution or not having performed a recent investigation must, in this day and age, assume they're in a post-breach state. It can be difficult for organizations to match the pace at which attacker groups evolve their techniques, tactics, and procedures, without them adopting a technology that automates threat identification.

Cyber security is in the midst of a paradigm shift. Targeted attacks are outmaneuvering the prevention and detection mechanisms that companies have in place. Endpoint protection solutions are incapable of detecting fileless attacks that are defined by behavior and the use of legitimate OS tools, rather than by a malicious program being installed on a machine. Detection technologies certainly detect suspicious events, but too often they fail to filter out noise from critical incidents, generating overwhelming numbers of alerts that have no hope of being processed.

According to a 2017 EMA study,[1] 79% of security teams reported being overwhelmed by high numbers of threat alerts. And it's no wonder: for example, a study by Ovum found that 37% of banks receive more than 200,000 alerts per day, and 61% receive over 100,000.[2] The Ponemon Institute reports that nearly half of all security alerts are false positives.[3] Of the rest, a large share is inconsequential and easily remedied. With the possibility to examine only a tiny fraction of alerts, overstretched security teams are forced to let the majority of alerts triggered on a daily basis go without attention. Teams are left frustrated. EMA found that 52% of operations personnel feel high levels of stress, with 21% of them stating that "not enough manpower" is a stress driver.[1] The cyber security skills shortage itself is well-documented, with a 2017 ESG/ISSA finding it worsening and impacting 70% of organizations.[4]

Despite having cyber security high in our collective awareness, and companies are still struggling with breaches. The average breach dwell time is reported to be 100 days, or more depending on the industry and study.[3] Companies are still being caught off-guard with breaches exposing their networks, and their customers.

All the while, the intruders continue, concealed by a sea of alerts.

1 Enterprise Management Associates. A Day in the Life of a Security Pro (2017).

2 American Banker. There are too many cybersecurity alerts (2017).
3 Ponemon Institute for HPE. Cybersecurity Trend Report (2016).
4 Information Systems Security Association International. ESG Survey Results (2017).

Context is everything

Everything. In life, and in cyber security. A key turns the lock on your front door. It matters whether the person holding the key is your spouse, or a burglar. A person emerges from a department store carrying a large bag of merchandise. It matters whether or not that person has completed a payment transaction before doing so. A complicated Powershell command is executed from a user's machine. It matters whether it is executed as a part of system maintenance, or by Microsoft Word.

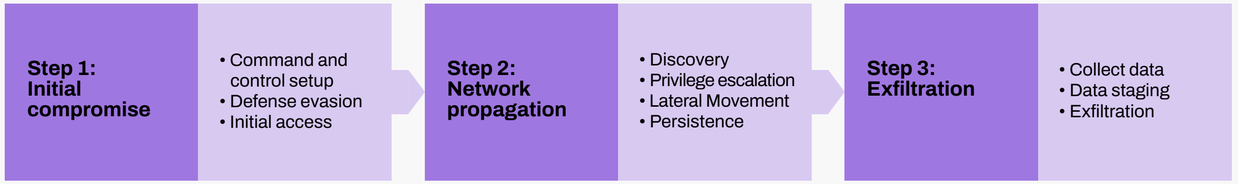
Lack of context, conversely, is lack of, well, almost everything one needs to know[5] to make a judgment. Without context, single isolated events are meaningless. It is only when connecting the dots between related events that a full picture can emerge.

Lack of context is a primary contributor to alert fatigue. Many intrusion detection systems today still produce isolated alerts that are in and of themselves anomalous, but when connected with other related events, are found to be innocuous.

This means false alarms clutter the stack, increasing the workload for security teams who are already strained to the max, and decreasing the likelihood that actual incidents will be uncovered.

5 The MITRE Corporation. Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK™) knowledge base (2019).

How a real targeted attack looks: Case Gothic Panda



To demonstrate an advanced and targeted cyber attack, we use the example of the advanced persistent threat (APT) group known as Gothic Panda from MITRE's Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK™) knowledge base and model for cyber adversary behavior.[5] The adversaries in this example attack are interested in exfiltration of documents and intellectual property, often industrial in nature. Gothic Panda's process can be broken down into three main phases as shown below.

In the initial compromise phase, attackers aim to achieve successful code execution and control of a system within the target environment. The goal of the second phase, network propagation, is to identify and move to desired systems within the target environment with the intention of discovering credentials and documents for exfiltration. In the final phase, the goal is to collect the data, compress it into an easy-to-transmit package while in the target environment, and then proceed with exfiltration by hiding in other outbound network traffic. The exfiltration is likely the most noticeable phase.

That's why from a detection point of view, the first phase is naturally the most important one, before the attacker gains persistence and moves to high value systems within the target environment. Well-prepared organizations use a preventive layer like endpoint protection platforms to block commodity malware threats such as and ransomware, which prevents most malicious code execution in the target environment. However, advanced attackers are able to remain undetected by using low and slow attacks, eventually finding a way around the preventive layer. That's where detection and response comes into the picture.

Man & machine

From a mindset perspective, we must let go of the notion that cyber security is about products and services. It's about skills. Experience. Competence. No matter what products and solutions you have in place, it comes down to proactively managing a highly complex and everchanging environment and threat landscape. That requires skills. Unfortunately, there's shortage of the needed skills, and this shortage will become ever more pressing as digital capabilities become a more important part of value creation for all.

But perhaps even more important is that skills alone are not enough. Just as technology has boosted our capabilities when it comes to everything from productivity work to engineering, we must develop technologies that boost our skills and help us scale our efforts when it comes to cyber security. We must develop technologies that can learn to do what human security analysts do, but at lightning speed – connect the dots, placing events into a proper overall picture in order to make an accurate judgment.

Game change

From the defender's point of view, this paradigm shift changes the game. It's not an option to give a boost to an existing endpoint protection solution and market it as a new technology. Cyber security vendors need to build new solutions from the ground up that are specifically targeted for the new era and new problems we face. This means a shift from single-shot and point detections with binary on/off responses to event flow and context-based detections and multi-faceted, risk-based responses.

To put the enormity of this change into perspective, in the traditional endpoint protection world our systems analyze over a million samples every day to decide whether they are malicious or not. This is an impressive number, resulting from already having tens of millions of endpoint clients out there that send these samples.

However, in the new era of trying to detect malicious, hidden attacker activity from the small individual events that attackers trigger when executing their Tactics, Techniques and Procedures (TTPs), the game is totally different. In a single midsized customer environment we have to analyze 70 million behavioral events a day.

Artificial intelligence and machine learning is obviously the only scalable solution that can be applied. But again, AI alone is not the answer – by itself, AI is little more than a glorified false positive generator. Rather, what's needed is the perfect combination of data science and cyber cybersecurity experts.

Detective-like piecing together of the facts

Detecting broader context is perhaps most easily explained to non-technical people in plain English with a real-world analogy. Imagine a car is found, crashed at the base of a cliff. Was it an accident, or was there a crime involved? Was there someone in the car? These are important questions that need to be answered in order to understand how to respond to the discovery.

Forensics investigators are called to the scene of the crash. They study the site to piece together the sequence of events that led up to the crash. They study the tire tracks at the top of the cliff to determine whether the car accelerated, or whether brakes were applied. They check the speedometer to see if they can determine how fast the car was traveling. They check the temperature of the engine to try to determine how long the car has been there. They run a license plate check to find out who the car is registered to and scour the site for any sign of a human being. They look into events that happened during the preceding weeks, such as whether the vehicle owner received suspicious phone calls or whether his or her browsing history reveals a map service search around the cliff, to rule out anomalies in normal behavior.

On their own, each of these factors - speedometer, engine temperature, events of weeks prior the crash, etc. - would appear to be meaningless, but when placed in proper context, a story emerges that will help investigators determine what has happened and whether a crime has been committed.

Taking shape

The idea for a context-aware, expert-tuned technology came about after discussions with our customers. We asked them what they were missing in their organization. They told us they have systems in place to stop the commodity malware files that make up the 99.9% of threat volume an organization faces. What they needed was a tool to stop the other 0.1% of threats that use non-traditional means to infiltrate an organization.

These are the threats that do the most damage – fileless threats that generate events that are almost indistinguishable from events an ordinary user would generate. It is only by connecting the dots between events that a malicious pattern emerges. Connecting the dots is the point where the security analyst usually need to step in.

Our advanced managed threat hunting service, WithSecure™ Countercept, puts our world-class cyber security experts at the service of organizations. Our threat hunters monitor our customers' environments 24/7. When an anomaly is detected, our experts investigate it and once they determine it's a real threat, they alert the customer, all within minutes of detection, or respond with Continuous Response methodology which merges people, process, and technology to battle live, targeted attacks.

There's just one problem with this service: these highly skilled experts are in limited supply. We realized that we needed to find a way to bring the knowledge and skills of our Detection and Response Team to any company. So we got to work on technology that comes as close as we possibly can to what our human experts do: investigate the context of an alert to determine if it's a real incident. The result is something we call Broad Context Detection™.

Innovation at its best

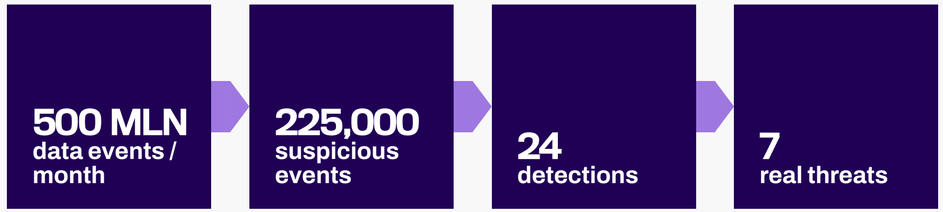
Spotting misuse from proper use is like looking for a needle in a haystack. It requires collecting vast amounts of behavioral events. Broad Context Detection™ is designed to take this sea of events and narrow it down to a trickle of meaningful incidents.

For example, a midsized organization with 650 sensors typically generates roughly 1 billion events every month, but only about ten detections require containment and remediation actions. The role of Broad Context Detection is to enable us to hone in on the few incidents that matter. It does this by analyzing myriad numbers of events, flagging suspicious ones, then relating similar events together and classifying these related events into a group that pertains to an incident. Broad Context Detection then displays the group events in a chronological timeline to give a complete picture of the incident that has taken place.

With Broad Context Detection™, as the calculated risk score increases with each detection based on the adversary's actions, the captured behavioral events of the initial compromise will be revealed and the manager of the target environment alerted. The broader context of the attack becomes instantly visible on a timeline displaying all impacted hosts and relevant events, along with recommended response actions.

As result, the attacker can be isolated from the network early, before propagating into the network and exfiltrating data from servers storing customer or other personal data, confidential or otherwise sensitive business documents and intellectual property.

Broad Context Detection™ in action



In a 325-node customer installation, our sensors collected around 500 million events over a period of one month. Raw data analysis in our back end systems filtered that number down to 225,000 suspicious events.

Suspicious events were further analyzed by our Broad Context Detection™ mechanisms to narrow the number of detections down to just 24.

Finally, those 24 detections were reviewed in detail by human experts and only 7 detections were confirmed as real threats.

Focusing on fewer and highly accurate detections allows response to be faster and more effective when under an actual attack.

How it works

When incident detection is based on providing alerts, it's no wonder the false positive rate is so high. WithSecure™ and other EDR vendors Broad Context Detection takes detection technology further than ever, by filtering alerts down into actual incidents. Using context, we narrow down a long list of alerts to a shorter list of detections, and that to an even shorter list of actual incidents that's clear and actionable for security specialists to respond to.

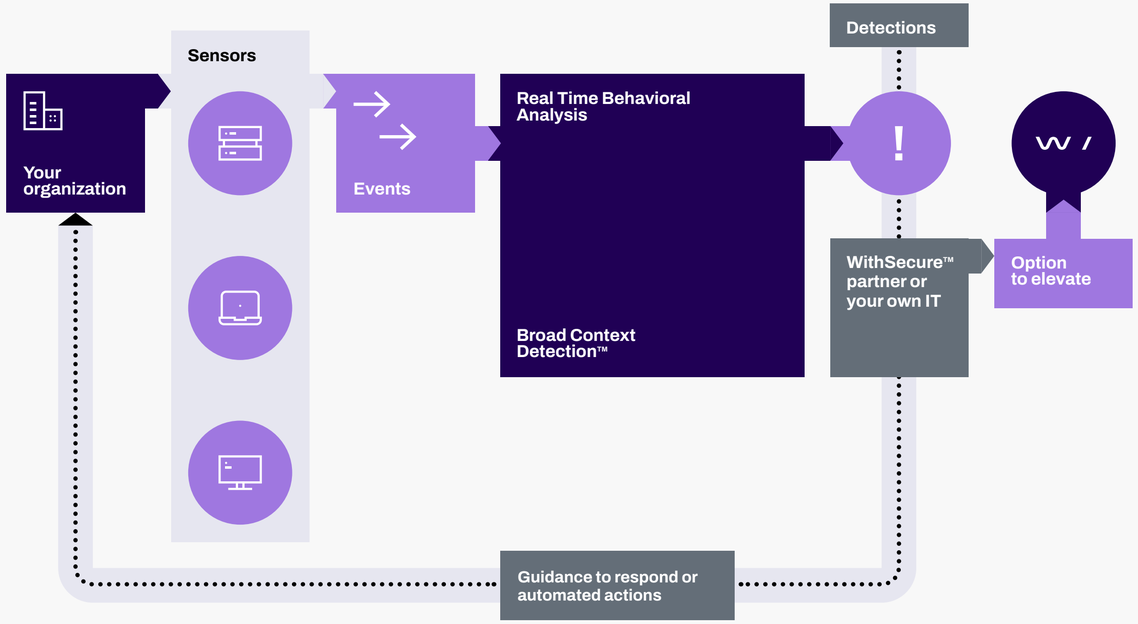
First, simple events are streamed to our behavioral analytics engine, which scans for suspicious behavior and moves suspicious processes into more detailed monitoring. In this monitoring stage, we take into account the greater context, allowing us to identify events that would be prone to false alarms if analyzed by themselves. We can now identify suspicious and hostile behavior reliably, and ignore behavior that is acceptable.

The stream of alerts then enters an alert aggregation engine, which begins to build the contextual picture by grouping together multiple related alerts. Based on the more comprehensive picture that is formed when grouping alerts together, judgments are made for actual detections, with a near zero probability of false positives. Finally, these detections are streamed to an incident detection engine that confirms real incidents. Again, the false positive rate is near zero.

From the now much more manageable comprehensive list of detections, a timeline is built, placing the detections in chronological order so analysts can see the full set of circumstances surrounding the incident. Detections are also prioritized by severity according to their risk level, the host criticality, and the prevailing threat landscape.

With this approach, IT teams are provided with a relatively short list of confirmed detections, each flagged with distinct priority levels and recommended response actions. So not only do teams know what to focus on first, but they also know how to respond and can do so quickly and decisively.

WithSecure™ Rapid Detection & Response



1. Lightweight sensors monitor endpoint activities and stream behavioral events to our cloud in real-time.
2. Real-time behavioral data analysis flags and monitors both the processes and other user behavior that have triggered those events.
3. Broad Context Detection™ mechanisms further narrow down the data, placing related events in context with one another, quickly identifying real attacks and prioritizing them with respect to risk level, host criticality, and prevailing threat landscape.
4. Visualized broad context and descriptive attack information make confirming a detection easy. Your WithSecure™ Partner or your own IT team manages the alerts, with the option to elevate tough investigations to WithSecure™.
5. Following a confirmed detection, our solutions provide advice and recommendations to guide you through the necessary steps to contain and remediate the threat.

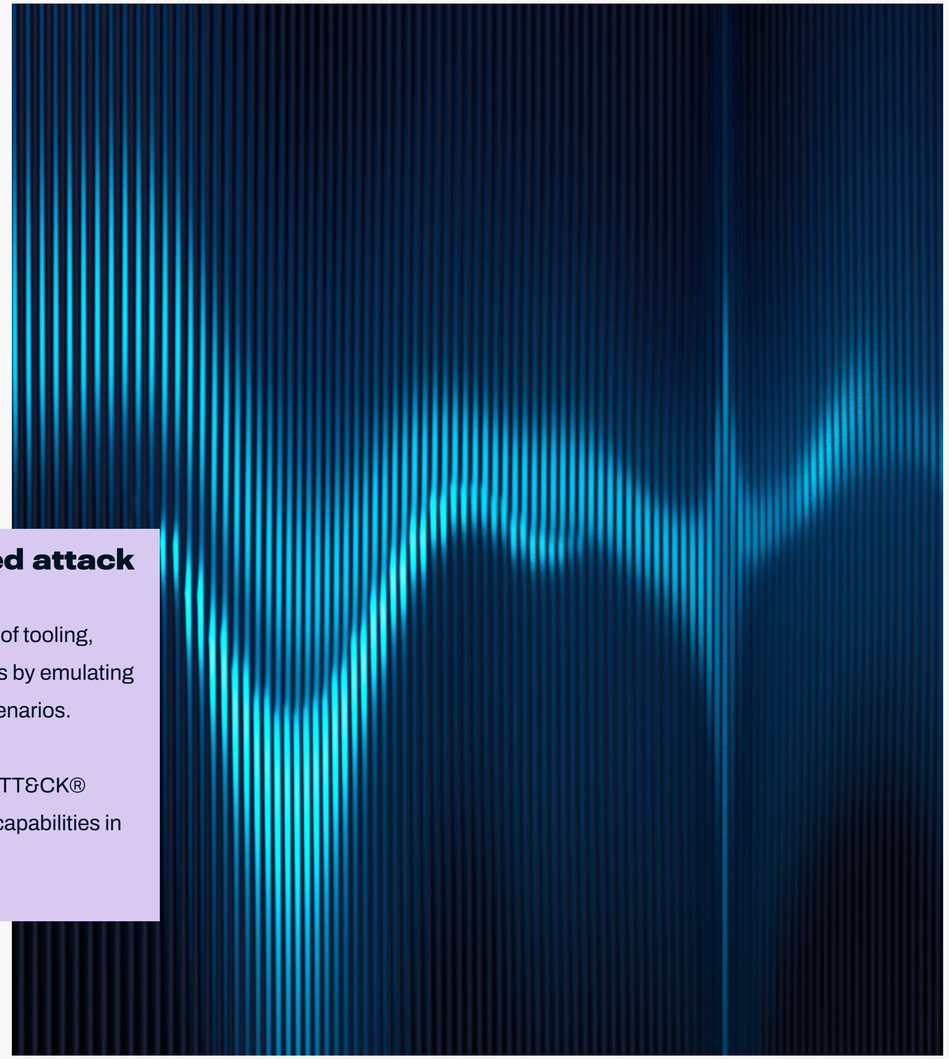
Detections and behaviors

Broad Context Detection™ flags indications of possible breaches by alerting admins of Tactics, Techniques and Procedures (TTPs) used in targeted attacks. This could include the following possibly suspicious actions:

- Abnormal activity of standard programs
- Calls to running processes from non-standard executables
- Running of unexpected scripts
- Unexpected running of system tools from standard processes

Broad Context Detection™ flags TTPs used to achieve the following objectives:

- Persistence
- Privilege Escalation
- Defense Evasion
- Credential Access
- Discovery
- Lateral Movement
- Execution
- Exfiltration
- Command and Control



Independent evaluation of advanced attack detection capabilities

To help provide organizations with a more detailed analysis of tooling, MITRE conducted independent evaluations of EDR vendors by emulating the Gothic Panda (APT3) and the Dukes (ATP29) attack scenarios.

Learn why should you care about MITRE and how MITRE ATT&CK® evaluations have confirmed WithSecure's industry leading capabilities in detecting advanced attacks at withsecure.com/mitre

Leveraging machine learning to the max

The use of machine learning and AI that's constantly tuned by human experts means that our systems keep getting smarter. Unlike traditional approaches of merely training the machine on what bad behavior looks like, our basic approach is centered around atypicality modeling. That means we teach our systems what normal, "good" behavior looks like, and then we flag everything that's different from what we expect. This allows us to be open to a much wider array of possibly malicious behavior.

This approach means we are not limited to typical attack detection methods, which are based on factors such as unusually high permissions and rapid patterns of operations. Competent attackers have caught on, choosing to employ minimal permissions and so-called "low and slow" attacks, meaning they carry out attacks gradually,in steps paced out over time. This way they can fly under the radar of conventional monitoring tools, because these attacks do not match the patterns that were used to train the tools.

The advantage of machine learning is that we can train machines to learn from everything, even from their mistakes (which is something even humans don't always do). When the machine pinpoints an alert that turns out to be a false positive, the machine learns why that was the case, and takes this into account next time, ensuring it won't flag the same type of alert again. This is one of the reasons our rate of false positives is so low.

While real-time detection is the basis of our solution, sometimes it's necessary to detect something after the fact. With machine learning, we can easily take new rules for detections that our experts have just identified and apply them to old data, picking up on activities that may have been passed over the first time around.

Broad Context Detection™ makes understanding the scope of a targeted attack easy by :

1. Combining real-time behavioral, reputational and big data analysis with machine learning
2. Taking into account risk levels, affected host criticality and the prevailing threat landscape to provide comprehensive insight into an incident and its severity
3. Presenting only relevant detections with actionable visualization for risk-based and multi-faceted responses

Prevention makes the attackers' lives harder

Those advanced attackers may have the skills to get into your network no matter what, but there's no need to roll out the red carpet. By putting effort into pre-compromise prevention, you're making it a little harder for these attackers to breach your network. When they're forced to put in more effort, their cost structures increase, which helps work as a deterrent.

Early prevention helps smooth your detection and response processes and reduces your workload. But not only that, it's actually the most cost-effective way to protect the network. The longer an attack persists, the more costs build up. Prevention from an early stage – and if that fails, detection as quickly as possible – keeps costs low and your team efficient.

Companies usually don't realize the importance of prevention until it's too late. Having strong postcompromise detection and response capabilities in tandem with pre-compromise preventive measures is the best way to protect your business from targeted attacks.

Conclusion

Cyber security is about skills and experience. But the defender's dilemma reminds us that we need to have the resources to be vigilant all the time, whereas our adversaries can strike at will. And with the current shortage of trained experts, the adversaries are winning the game.

What's more, skills and experience alone are not enough. It takes technology to leverage that expertise to monitor an entire organizational network and detect the tiny clues that indicate an attack is underway. And it takes superior technology to do so with precision, without activating unnecessary alerts that consume time and resources that security teams should be devoting to actual incidents.

Broad Context Detection a central feature of WithSecure's Rapid Detection & Response solution, which provides companies with the advanced capabilities they need to defend themselves from targeted attacks. With the power of machine learning trained and constantly tuned by elite cyber security experts, Broad Context Detection ensures WithSecure's solutions pinpoint only the incidents that matter. It's the perfect combination of man and machine, bringing world-class cyber defense within reach of every organization.

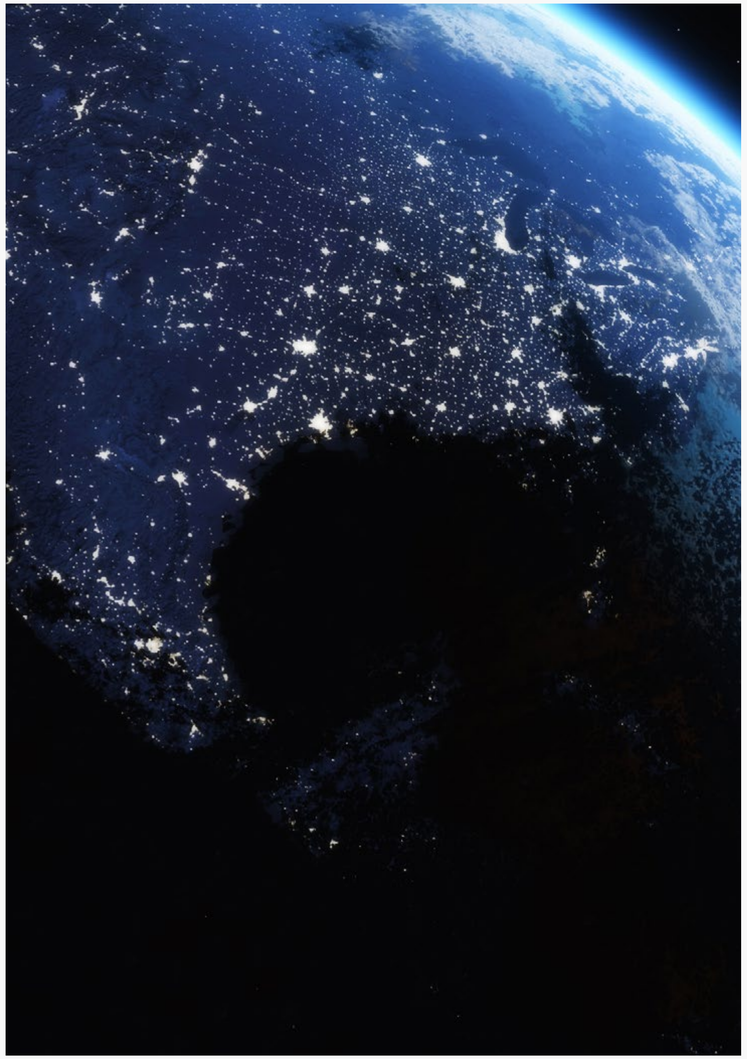
With Broad Context Detection, your company can detect targeted attacks that were previously undetectable. Now go fight to win.

For a video about Broad Context Detection™ go to: withsecure.com/RDR

Learnings from advanced managed threat hunting service

Our system is constantly being fine-tuned and analyzed by our experts. The fact that it's the same engine we use to provide WithSecure's advanced managed threat hunting service means that it's not just blind data analysis based on learning data. We use the system to provide managed detection and response (MDR) services to even the most demanding and highly targeted customers, and then constantly incorporate learnings from those customer environment back into the solution to provide a much higher quality and more finely tuned solution than the typical vendor who only produces the solution.

More about WithSecure's advanced managed threat hunting service for detecting and responding 24/7 to skilled human adversaries conducting live, hands-on keyboard attacks at withsecure.com/countercept



Who We Are

WithSecure™ is cyber security's reliable partner. IT service providers, MSSPs and businesses along with the largest financial institutions, manufacturers, and thousands of the world's most advanced communications and technology providers trust us for outcome-based cyber security that protects and enables their operations. Our AI-driven protection secures endpoints and cloud collaboration, and our intelligent detection & response is powered by experts who identify business risks by proactively hunting for threats and confronting live attacks. Our consultants partner with enterprises and tech challengers to build resilience through evidence-based security advice. With more than 30 years of experience in building technology that meets business objectives, we've built our portfolio to grow with our partners through flexible commercial models.

WithSecure™ is part of F-Secure Corporation, founded in 1988, and listed on the NASDAQ OMX Helsinki Ltd.

WITH secure