RETHINKING RESPONSE

F-Secure

TABLE OF CONTENTS

This whitepaper is for CISOs, CIOs, and any security professional who needs to successfully manage and respond to incidents.

EXECUTIVE SUMMARY 1
A new era – and a new term 2

1. WHY RETHINK RESPONSE NOW? 5
VUCA: speaking in a language your board will understand 6
Volatility 7
Uncertainty 10
Complexity 16
Ambiguity 21
CISO summary – the VUCA checklist 23

2. HOW DO YOU STOP AN ATTACK? 24
Leveraging your investment in detection 25
The challenges facing security teams 26
The Continuous Response Methodology 28
Collaboration 29
People 30
Processes 32
Technology 34
Context 35
People 36
Processes 38
Technology 39
Control 40
People 41
Processes 42
Technology 44

3. WHAT THIS MEANS IN PRACTICE: CONTINUOUS RESPONSE CASE STUDY 46
How the attack unfolded 47
The investigation starts 48
How Continuous Response might have yielded a different outcome 50

CONCLUSION 52

EXECUTIVE SUMMARY

While you know you will be targeted by a cyberattack, convincing the stakeholders in your business is not straightforward. But it will be you that has to answer for a breach, should it happen.

The evolving threat landscape makes it highly likely that almost any organization will be the target of a cyberattack.

Over the past few years, attack detection has seen enormous investment and progress, making it now possible to detect even the stealthiest and most innovative of attackers faster than ever before.

But to actually stop attacks takes more than just good – or even great – detection. We have witnessed attackers achieving their objectives in days, hours, even minutes. These objectives continue to surprise – organizations that would never have thought themselves a target of a sophisticated attack are increasingly finding themselves attempting to recover assets, restore encrypted servers, and, ultimately, save their businesses.

This is due in part because – despite the strides made in attack detection – many organizations have struggled to adapt their approach to leverage new response technologies and capabilities. Incident response has traditionally been a post-mortem investigation that begins after the attack has been completed and the business has suffered impact.

Is it time for change?

A NEW ERA – AND A NEW TERM

F-Secure Countercept first launched to provide what was then a new and emerging idea: effective threat hunting. We defined threat hunting as proactive detection and response conducted by a skilled team trained in the attacker mindset. This meant 'assuming breach' and actively searching for indicators of anomalous activity that might not be caught with technology alone, and then containing those actions before business impact. Threat hunting, for us, was always about the human element of attack detection and response in an era when it was becoming crystal clear that even the best automated and AI-based tools in the world could be evaded and bypassed.

The emergence of threat hunting as a skillset fed the security industry's laser focus on attack detection. However, the ability to respond to a live attack as it is happening – while part of Countercept's vision from the beginning – has been a challenge for many to achieve. Many solutions offer the ability to detect attacks, but provide limited means to stop the attackers from achieving their objective, while the attack is happening. While certain actions can be taken, such as isolating the affected host or terminating malicious processes, these often serve to tip off attackers that they've been detected, forcing them underground, leaving little evidence of how they compromised the organization, and increasing the likelihood that they will be back with better, stealthier techniques to achieve their wider overall objective.

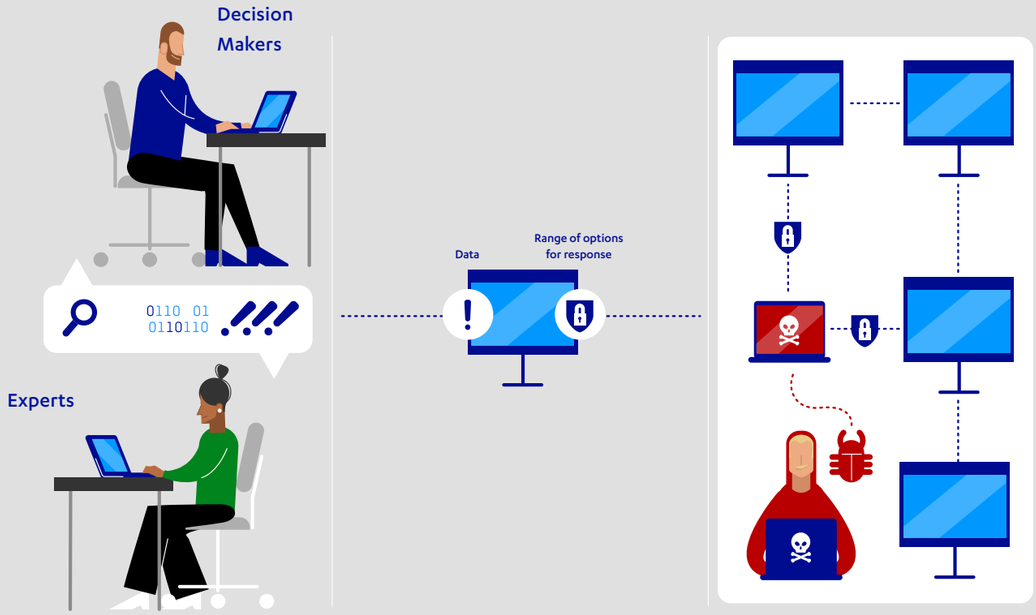
Let's put an end to the era when organizations only respond to a breach after the attacker's objective has been completed.

Instead, we can now catch attackers live, in action, executing critical decisions at speed while still collecting live forensics and artefacts. All of the intelligence normally relegated to post-incident investigations can be provided while the attacker is live on the estate, containing and limiting their access and preventing them from reaching their objectives while the full extent of the breach is assessed and eviction planned. In essence, we can buy time to respond effectively.

How do we do this?

With Continuous Response.

Our Continuous Response methodology puts the right people, in the right place, at the right time (Collaboration), equips them with the right information to make a decision (Context), and the ability to take the right action (Control).



Collaboration
between expert teams

Context
from the right data

Control
over actions

In the pages to follow, we illustrate how to defend your business against targeted attacks by live, human adversaries. We will:

- Equip you with the vocabulary to help your organization – including your board – to understand and action your threat profile, including who might target you, why, and how;
- Share our Continuous Response methodology that empowers the right people in your organization with the processes and technology to proactively defend your organization against the threats you face;
- Explain how the core elements of our methodology – **Collaboration, Context, and Control** – prepares the five essential factors for continuous response: people, data, decision-making, the ability to act, and timing;
- Show Continuous Response in action by applying it to a real, live incident.*

Are you ready? Read on.

*The name, sector, and geographical location of the company has been anonymized.

For years, security experts have vocally advocated the need for enterprises to invest evenly across Prediction, Prevention, Detection and Response.[1] From a survey conducted by MWR, prevention still takes the lead in investment, with 40% of enterprises naming it as their highest cost and 28% as the second highest.

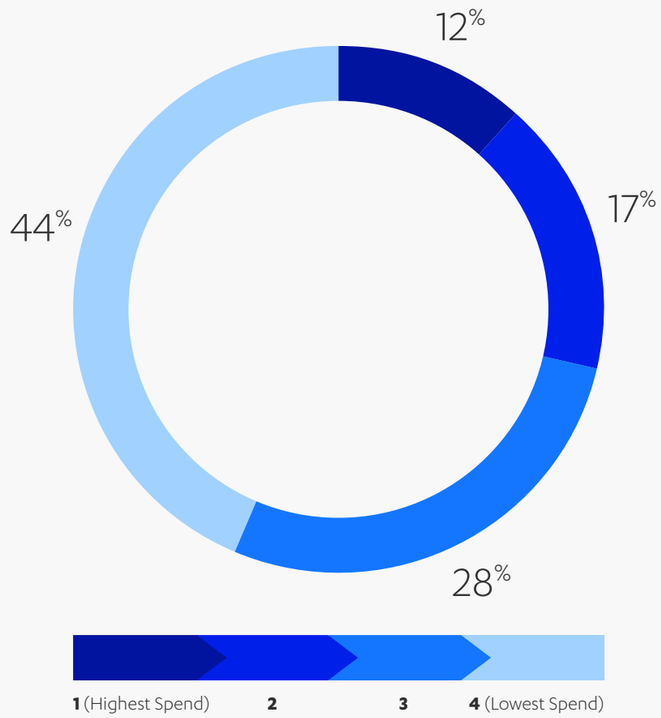
Detection is climbing up the priority list, coming in as second highest for 34% of enterprises, with just 17% of enterprises naming it as their smallest spend.

However, response is currently the lowest priority spend for 44% of enterprises.

Prevention tools can only be used effectively if they do not operate in silos. Innovations in connectivity between preventative tools and SOCs can allow for better data collection and enable better visibility into anomalous activity across your estate. However, with the average cyberattack now costing a single business over $1million,[2] is it time for enterprises to start investing more in incident response?

SPENDING RANKED FOR RESPONSE

Of the companies we surveyed, when it comes to investing in Prediction, Prevention, Detection and Response, only **12%** of companies identified 'Response' as their highest spend.



[1] https://searchsecurity.techtarget.com/news/2240223269/On-prevention-vs-detection-Gartner-says-to-rebalance-purchasing
https://www.gartner.com/en/newsroom/press-releases/2017-03-14-gartner-says-detection-and-response-is-top-security-priority-for-organizations-in-2017

[2] https://threatpost.com/threatlist-cost-cyber-attack/140870/

1. WHY RETHINK RESPONSE NOW?

A guide to the who, what, why, and how of the threat landscape, and how it affects your organization

WE LIVE IN A VUCA WORLD.[3]

VUCA – the acronym coined by the United States Army to describe the **volatility, uncertainty, complexity, and ambiguity** of the post-Cold War world – has been adopted in the corporate setting as a framework for preparing, leading, and even thriving in an unpredictable business, economic, and geopolitical environment. According to Forbes, "[VUCA] is gaining new relevance to characterize the current environment and the leadership required to navigate it successfully."[4]

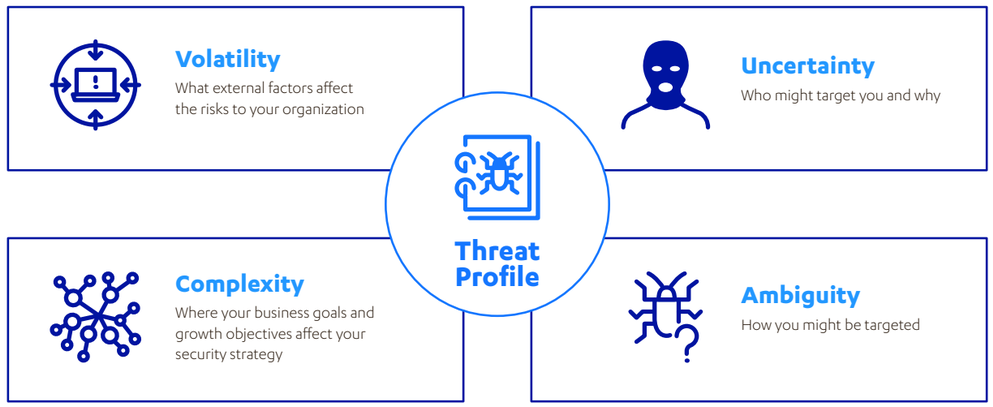
We believe that VUCA's roots in the challenges of the Cold War – battling an unseen and stealthy enemy with wide-ranging objectives that deploys unseen tactics, techniques, and procedures – make it a thorough and appropriate framework for guiding organizations as they craft their cybersecurity strategy. Assessing your organization through the VUCA lens ensures your security strategy is aligned with your leadership's needs and objectives, as well as with the unique threats you face.

In this section we will explain how the VUCA framework can guide discussions and decisions about the how, what, and why of the threats to your organization, and provide the basis for how our Continuous Response methodology can help you defend your organization against the threat landscape.

[3] https://en.wikipedia.org/wiki/Volatility,_uncertainty,_complexity_and_ambiguity

[4] https://www.forbes.com/sites/sunniegiles/2018/05/09/how-vuca-is-reshaping-the-business-environment-and-what-it-means-for-innovation/#5bb99417eb8d

VUCA: SPEAKING IN A LANGUAGE YOUR BOARD WILL UNDERSTAND



Defending your organization is not a one size fits all exercise. No single tool or magic box with flashing lights will solve this problem.

Understanding the threat landscape and where your organization sits within it is no easy task, but it is far from impossible.

We know a fair amount about the primary threat groups, their motivations, their targets, and their methods. However, it is not the case that all threat groups target all organizations, or even a few. The nature of targeted attacks is that attackers take weeks and months to plan an attack where they attempt to access and exfiltrate specific information or assets.

The VUCA framework will equip you to understand where you sit in the threat landscape, who might target you, why, and how. It will help you craft a security strategy that combines your knowledge of the threats you face, how you should structure and support your ecosystem for detection and Continuous Response, and align these with your board's overarching goals and objectives. It can guide the incremental improvements you make to continuously assess your security.

IDENTIFYING AND COMMUNICATING THE THREATS TO YOUR ORGANIZATION

Our aim is to provide you with the vocabulary, visuals, and a practical checklist to help you lead discussions in your organization to identify why, how, and by whom you might be targeted. These findings will enable you to craft a security strategy that combines the people, processes, and technology required to protect your organization.

VOLATILITY:

THE EXTERNAL FACTORS THAT AFFECT THE RISKS TO YOUR ORGANIZATION

Volatility applies to the changing motivations and shifting components of the threat landscape, and how they affect your security posture. While some aspects of the threat landscape are more within an organization's control, volatility focuses on the influencing factors that are beyond your power.

ADVANCED, PERSISTENT THREATS ARE NOT WHAT THEY USED TO BE

Let's start with a somewhat provocative statement: we need to stop using the acronym 'APT' to describe state-sponsored cyberattack groups.

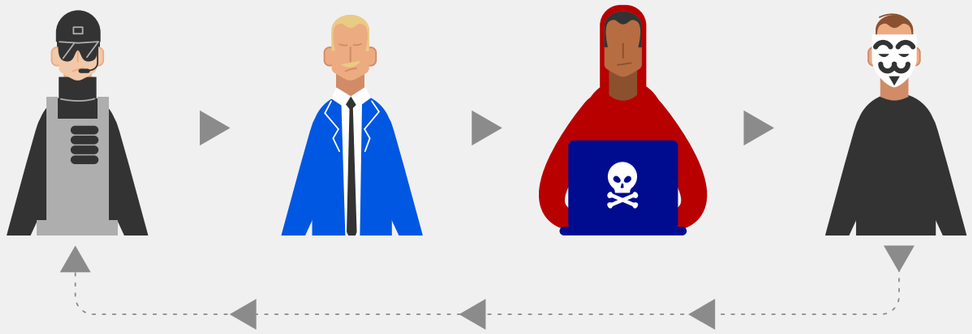
Why?

Appropriating the acronym APT – advanced persistent threats – to only state-sponsored groups belies the fact that the threat landscape has moved on; as state-sponsored capabilities trickle down and become more widely available, it gives other hacking groups the ability to be as advanced and persistent as those historically called APTs.

This means that state-sponsored capability is rampant throughout other groups. Many criminal groups, individuals, and hacktivists eventually deploy the same tactics, techniques, and procedures, with variants of state-sponsored malware and zero days being deployed throughout the threat landscape. In addition, this trickle-down effect is motivating state-sponsored groups to innovate in in order to stay under the radar.

What does this all mean? That anyone – from a state-sponsored group to a capable individual willing to invest the time – can execute a targeted attack on your organization, leveraging some of the most advanced tools, techniques, and procedures of the trade.

Increasingly, anyone can be an APT



State-sponsored groups develop and deploy **advanced** tactics, techniques, and procedures (TTPs).

Advanced criminal groups adopt or create variants of these TTPs, enabling them to be **persistent.**

The TTPs trickle further down to cybercriminals, hacktivists, and individuals, making them a genuine **threat** to organizations, targeting them for financial gain, to make political statements, or to cause business impact.

State-sponsored groups respond to their tools being leaked and widely used by innovating and developing new TTPs, to stay under the radar. Fundamentally, anybody can acquire the capability to be an advanced, persistent threat.

EVERYTHING IS (GEO)POLITICAL

There are many examples of how geopolitics drives the threat landscape.

In 2010, China released its five-year plan for 2011-16, outlining its intent to address the country's key challenges around urbanization, environmental protection, and increased domestic consumption. Research and development – particularly around developing the efficiency of nuclear power and renewable energy technologies – was high on the country's agenda.

In 2012, APT1 – China's state-sponsored cyberattack group – targeted several key industries globally, with a specific focus on cyberespionage where English was the primary language. The United States Department of Justice brought charges against members of APT1 for this, stating that: "The perpetrators stole trade secrets that would have been particularly beneficial to Chinese companies at the time they were stolen."

Increasingly, this kind of compromise could have been the objective of or achieved by any hacker or hacking group, as the tactics, techniques, and procedures used in an attack such as this are available to anyone with the time and inclination to use them. This also shows that attack objectives are nuanced and unexpected, although with the right geopolitical and business knowledge, they are easier to predict than you might think.

FROM THE ZERO TO THE 'N'

At the time of writing, the most used browser in the world has an n-day vulnerability.* As you read this, many people are still unlikely to have patched.

It's hard to quantify the effect of this type of vulnerability being exploited. We know they can be divided into two camps: the flaw that provides an entry into your IT estate, and the flaw in business critical applications and software, which affects the ability of your business to continue as normal. Both are equally hard to manage. The latter, for example, requires clear updated contacts and roles and responsibilities to handle effectively.

Attackers move quickly when a zero-day becomes an n-day; organizations need to move faster still. Notably, Equifax sent out a notice to patch an n-day flaw; however, it went to a member of staff who had recently left the business. The result? The most expensive cyberattack in history, to date.

*We refer to zero-day vulnerabilities as security flaws that exist, but have not been publicly disclosed; the n-day is the time between disclosure and patching.

YOUR SUPPLY CHAIN

We are well aware of the difficulties in trying to control the security of your suppliers. You can vet them, but they face the same challenges in securing their organizations as you do, often with much smaller budgets.

The surge in supply chain attacks over the last two to three years is astounding. As large, established organizations bolster their security capabilities, attackers continually turn to smaller, less secure companies in the supply chain to gain access to the companies they service.

But we have seen many companies, understandably, struggle to grasp the vastness of their supply chains, and the vulnerabilities that they create. Even the new printer installed last week can provide an entry to your estate.

SUMMARY

These are just some examples of how external factors beyond your control are constantly shifting in a way that directly affects your threat profile. There are many other elements that create **volatility** in your business environment and it is worth cataloging as many as you can so that you can keep track of them and, with them, the emerging risks surrounding your business.

UNCERTAINTY:

WHO MIGHT TARGET YOU AND WHY? WHAT WOULD THE IMPACT BE? WHAT (OR WHO) IN YOUR ORGANIZATION WOULD BE OF VALUE TO STATE-SPONSORED HACKERS OR CRIMINAL GROUPS?

These answers are not obvious or easy to know. Uncertainty, by definition, is caused when the availability of information or predictability in events is unknown. In this section, we will describe the main players in the threat landscape, what in your organization might be of value to them (and why it might not be what you think), and how it might impact your organization overall.

BEHIND THE HEADLINES

Despite the enormity of the cyberattacks that make the headlines – British Airways, Maersk, Sony Pictures, for example – the majority of compromised companies rarely become part of the public vernacular, giving the false impression that it is only a small handful of companies with obvious assets of value that are breached.

For those that do make the headlines, it is rarer still for the attacks to be attributed to any particular group, making the threat landscape seem intangible and nebulous, when it is anything but. Lack of attribution also means that motivations and objectives are seldom revealed or even speculated. This leaves a void of information regarding what the attackers were after, whether or not they were successful, and what might be their larger intentions, feeding the misconception among many that their company isn't of interest to sophisticated attackers.

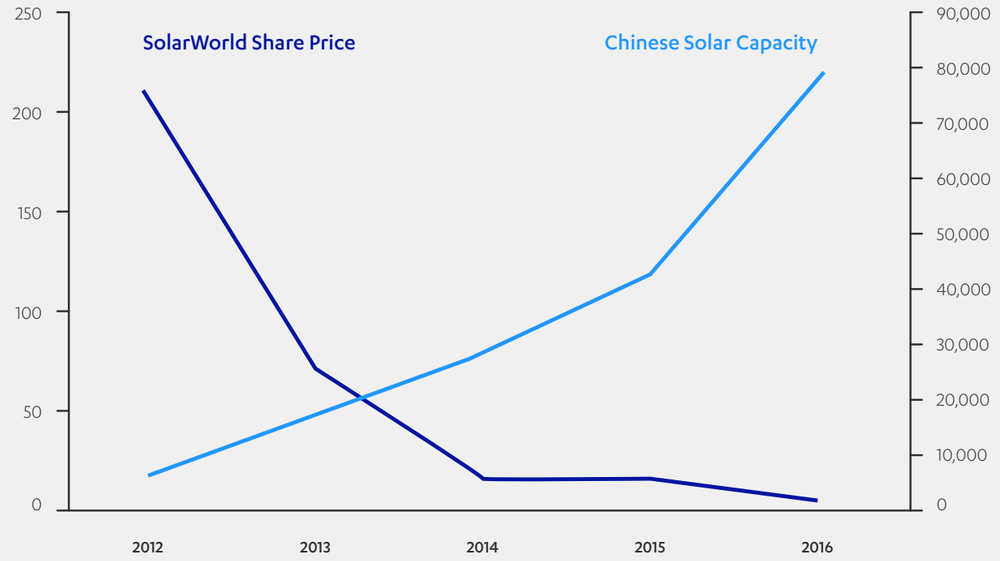
ONE OUT OF MANY

In the previous section, we mention APT1. One of their targets, SolarWorld, was then the world leader in solar panel production, turning over €750 million a year, holding key contracts and intellectual property. It was well positioned to take advantage of a rapidly growing industry with global demand.

But the effect of the APT1 compromise was profound. As Ben Santarris, Director of Strategic Affairs for SolarWorld was quoted at the time: "There were thousands of emails exfiltrated, many with sensitive data that would pose to serve all kinds of unfair advantages." Those unfair advantages included intellectual property (IP), sensitive pricing information, and even ways for Chinese competitors to bypass United States-based regulations in flooding the market.

In August 2017, SolarWorld was officially declared bankrupt, with Chinese market saturation in solar production – commencing at the time of the APT1 attack of 2012 – bringing the company to a swift end. China has since cemented its place as the world's leading solar nation, smashing its 2020 solar targets three years ahead of schedule.

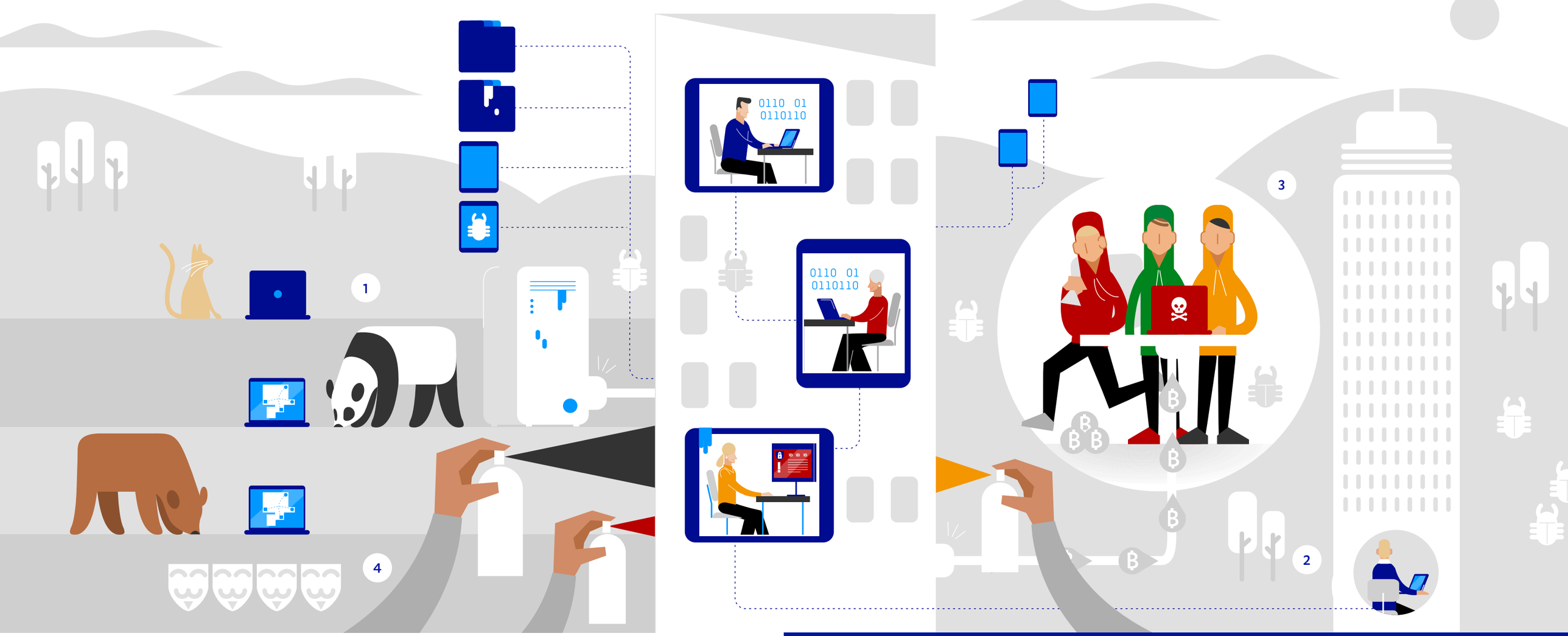
At exactly the same time, China announced the cancellation of 134 coal projects, in line with the 'future energy development' goals of the 13th five-year plan of 2016-2020.



Chinese success stories and the SolarWorld insolvency were announced in the same month, a cruel twist of fate that only serves to highlight their inversely linked fortunes since the APT1 attack.

SolarWorld is rare in that its full story – who targeted it, what was taken, and the eventual impact on the company – is in the public domain.

Disclosed even less frequently are the long-term consequences of being breached, such as gradual erosion of the bottom line, and – like SolarWorld – going out of business. We have experienced this firsthand; many incidents we have investigated have not been reported or fully covered by the media.



ATTACKERS AND THEIR MOTIVATIONS

In order to protect your organization against cyberattacks in all their forms, it is essential that you go beyond the headlines to know who might target you, and why.

1. STATE-SPONSORED GROUPS

A range of geopolitical objectives, all in support of the state. Will steal, extort, or sit on IT estates to observe. They don't stop until they reach their objective.

2. ORGANIZED CRIMINAL GROUPS

Motivated by money. Direct theft and invoice fraud. While state-sponsored groups steal IP to use for the state, criminal groups will steal IP and sell it on.

3. CYBERCRIMINALS

Will cause damage or leak information either from inside an organization or from the outside, either for monetary gain or for personal political objectives.

4. SCRIPT KIDDIES & HACKTIVISTS

Capable of causing disruption for the sake of it.

THE TOP OF THE ATTACKER PYRAMID

State-sponsored groups are the behemoths of the threat landscape, with the largest pool of financial and technical resources. While their objectives in targeting government and commercial information are well documented, we have seen other, less obvious assets be targeted, such as human resource files.

These attacker groups are proving that they can move at lightning speed, driving to achieve their objective before they are detected. For example, F-Secure recently acquired a client where a state-sponsored group had moved from a phishing email to full server access within 72 hours.

During an attack, a state-sponsored group can often be identified by the characteristic that they do not stop an attack until their objective is reached. This involves a high level of sophistication on the attackers' side; attacks are organized in shifts where work is handed off from one group to the next and objectives are tracked centrally to ensure cohesion.

For us, 'not stopping' is often the first indicator of what kind of group we're dealing with. If they carry on until they get to their target, they're state sponsored; if they give up, they are a crime group – the latter tend not to spend endless amounts of time, effort, and money if their objective is made harder to achieve.

UNDERSTANDING THE OBJECTIVES OF CRIMINAL GROUPS

Criminal groups are next in the food chain, and again, their objectives are often misunderstood. Many organizations would not see themselves as a target.

For example, a company may think that if they make a widget at 0.20 per unit it would be of little interest to any type of cybercriminal. But it's not so much the widget itself as who it is sold to – an attacker with access to your finances could, among many other things, create fraudulent invoices under your name, redirecting to criminal accounts. This is the kind of compromise that isn't detected until much later in the process, and can result in the loss of millions.

There is further blurring of the lines between crime groups and state-sponsored groups – North Korea's state-sponsored groups, for example, have historically deployed ransomware to generate funds for the state.

THE CRIMINAL IMPACT YOU MIGHT HAVE MISSED

Organized crime group dubbed MoneyTaker conducted over twenty successful attacks on financial institutions and legal firms in the US, UK and Russia since May 2016, which included 16 attacks on organizations in the United States (one bank had documents successfully exfiltrated twice), three attacks on Russian banks, and one attack on a bank in the United Kingdom. Attackers stole documentation related to the interbank payment systems (e.g. SWIFT), which appeared to have been obtained in preparation for further attacks.

- The Cobalt cybercriminal group conducted synchronized ATM heists across Europe, CIS countries (including Russia) and East Asia in 2016, and recently expanded its targets to North America, Western Europe and South America, particularly Argentina. Also, while banks are still targeted, other targets included stock exchanges, insurance companies, investment funds and others;
- Since 2013, FIN10 has compromised networks, stolen sensitive data, and extorted victims into paying large ransoms of up to $620,000. For victims that did not give into the demand, FIN10 escalated their operation by destroying critical systems and leaking stolen data to journalists;
- FireEye published a report on "FIN7", a group that targeted specific personnel involved with US Securities and Exchange Commission (SEC) filings at various organizations across insurance, investment, card services, loans, transportation, retail, education, IT services, and electronics. It is speculated that these attacks were aimed to support insider trading schemes (via securities fraud), using information gathered from these victims before it was provided to and published by the SEC;
- Members of organized criminal groups were behind half of all breaches in 2018, with state-sponsored or state-affiliated actors involved in 12%. (Verizon DBIR 18).

CYBERCRIMINALS – GROUPS AND INDIVIDUALS

There are many capable attackers whose motives are less about financial or geopolitical disruption and more about making a statement or disrupting the state of current politics and affairs. Those who would carry out this kind of attack are more than just disgruntled individuals in bedrooms – the 'political-insider-as-attacker' could be someone in government with the means and motivation to cause damage or leak information from the inside.

YOUR MOST VALUABLE ASSETS MIGHT NOT BE WHAT YOU THINK

It can be hard to read into the objectives and goals of state-sponsored and advanced criminal groups. We have taken a holistic view of what we have seen targeted, and have put them into these three categories below:

1. If you provide a service to another company, you may be a target for a supply chain compromise. Take a look at your clients – even though your business may not have any IP or assets of interest, does anyone on your client list? As large organizations spend millions to bolster their security, attackers look to compromise via the supply chain;
2. If you create invoices – and let's face it, most companies do – then you are potentially a target for fraudulent invoicing. This is defined as a threat actor gaining credentials that enable the creation of fraudulent invoices with altered payment details. The company often doesn't know the invoice was created;
3. If you hold any confidential information on your customers – names, birth dates, bank details – you may be targeted by criminal groups seeking to either sell these details on the black market or state-sponsored groups wishing to compromise your company's internal data.

However, to put this down to the micro level, here are some real-life examples of what we have recently seen within our Incident Response team:

- A healthcare provider became aware of unusual activity on one of its development servers; our investigation found that a state-sponsored group had been trying to exfiltrate a 30-gigabyte human resources file, and had also accessed information relating to IP of consumer goods;
- A local government office contacted us because of a suspected breach; our investigation found that a state-sponsored group had been active on the office's environment for three years;
- Fraudulent invoicing does not discriminate based on sector or size of the company. We recently responded to an incident where invoice fraud was first revealed when a member of accounting noticed an invoice had gone out requesting payment in Hong Kong dollars instead of in United States dollars.

SUMMARY

This section has outlined the key types of players in the threat landscape and how their motivations vary, from the SolarWorld example of devastating IP theft for geopolitical advantage, to bedroom hackers with an agenda, to the many attacks perpetrated by criminal groups for immediate financial gain. Although attacker motivations are hard to predict, keeping up to date with current trends, and reconsidering what your organization holds of value in light of this perspective, may prove very revealing.

COMPLEXITY

WHERE YOUR BUSINESS GOALS AND GROWTH OBJECTIVES AFFECT YOUR SECURITY STRATEGY

Complexity focuses on the internal elements that affect your security posture – i.e. the interconnectivity and interdependence of multiple components and the number of unknown variables they create. Understanding – and communicating – the complexity of your organization is about detailing the entirety of your IT estate and the people that rely on it, and identifying the crucial assets on your estate in order to craft strategies – and secure budget – for how you protect them, and factoring security into all plans for digital transformation.

SECURITY FROM THE START

Your board is likely to know where and how technology fits in your long-term business and growth strategy. Crucially, you need to factor in how these plans affect your risk profile. Giving ample time to integrate security into the process of choosing, implementing, and maintaining the technologies being added to your IT estate is an essential element of your long-term security strategy. In our experience, it is one which other business stakeholders can easily forget to factor in as plans are made and deadlines are set.

THE VASTNESS AND COMPLEXITY OF YOUR IT ESTATE

It is common security parlance that one of the best ways to secure your organization is to maintain as small an attack surface as possible. Turning off unused functionality in applications, reducing the amount of code running so that less code is available for exploitation, and reducing entry points are just some of the ways to do this.

However, for many global enterprises, achieving and maintaining a small attack surface is simply not feasible. Business critical functions rely on lines of code, multiple entry points, and an array of services, as well as the people that use them.

MANAGING ATTACK SURFACE FLUIDITY

Adding to the complexity is that your attack surface is fluid. Every time new endpoints, hardware, software, and even people are added to it, these new vulnerabilities need to be tracked and managed. For a large, global enterprise, tracking and monitoring activity on IT assets, adding and subtracting endpoints and programs, plus the unalterable fact that people in your organization – whether new or seasoned – are still your greatest vulnerability, all create challenges.

THE COMPLEXITY OF DIGITAL TRANSFORMATION

Emerging technologies are the backbone of many organizations' growth strategies. But implementation of these need to be managed with security in mind. We have compiled some statistics to illustrate the magnitude of the associated risks and opportunities.

INTELLIGENT AUTOMATION

64%

64% management and financial tasks could be automated by 2020 (thoughtonomy)

52%

52% of sales processes could be automated by 2020 (thoughtonomy)

40%

Forrester has predicted that by the end of 2019 more than 40% of enterprises will create state-of-the-art digital workers by combining AI with RPA[5] (Process Excellence Network)

45%

Forrester recently found that 45% of AI decision makers say trusting the AI system is challenging[6] (AI Business)

ARTIFICIAL INTELLIGENCE (AI)

450%

The share of jobs requiring AI has increased by 450% since 2013 (Adobe)

77%

77% of CEOs say AI and automation will increase vulnerability and disruption to the way they do business (PWC)

61%

About 61% of companies with an innovation strategy are using AI to identify opportunities in data that they would have otherwise missed (Narrative Science)

"We expect the growing use of AI systems to lead to the expansion of existing threats, the introduction of new threats and a change to the typical character of threats." (Malicious AI Report)

[5] https://www.processexcellencenetwork.com/rpa-artificial-intelligence/articles/putting-process-back-in-to-rpa

[6] https://aibusiness.com/trust-ai-rainbird-ceo/

CLOUD

94%

By 2021, 94% of data will be handled through cloud platforms[7] (Cisco)

66%

When asked about adopting an enterprise cloud computing platform, 66% of IT professionals say security is their greatest concern (LogicMonitor)

21%

Of all files in the cloud, 21% include sensitive data which has increased by 17% in the last two years[8] (Tech Target)

51%

An average of 51% of organizations publicly exposed at least one cloud storage service (RedLock)

24% 24% of organizations have hosts missing high-severity patches in the public cloud (RedLock)

IoT

80billion

IDC found that there will be 80 billion connected devices in 2025, helping generate 180 trillion gigabytes of new data that year[9] (Velocity Business Systems)

2020

The amount of data from the Internet of Things (IoT) that is analyzed and used to change business processes will be as big in 2025 as the amount of all the data created in 2020 (IoT Innovation)

48%

A survey of 950 companies that both make and use IoT technology found that 48% of companies that use IoT devices in the workplace don't have mechanisms in place to detect if any of their devices are hacked or not (Gemalto)

78%

78% of IT decision-makers think it's somewhat likely that their organizations will experience data loss or theft enabled by IoT devices within the next two years (IoT Innovation)

[7] https://www.business.com/articles/cloud-computing-enterprise-data/

[8] https://searchcloudsecurity.techtarget.com/tip/The-problems-with-cloud-based-email-security

[9] http://www.vebuso.com/2018/02/idc-80-billion-connected-devices-2025-generating-180-trillion-gb-data-iot-opportunities/

COLLABORATION TOOLS AND REMOTE WORKING

81%

81% of CIOs said their company had experienced a Wi-Fi related security incident in the last year

46%

Only 46% of enterprises were confident that mobile workers were using a VPN (all iPass)

57%

57% of CIOs suspect their mobile workers have been hacked or caused a mobile security issue in the last year

38%

Only 38% of the respondents thought of data security when collaborating externally

51% of the participants use public document sharing tools for work collaboration; only 16% did not use such tools since they were not approved for use at the workplace (both Queens University)

UNINTENTIONAL OVERSIGHTS ARE QUICKLY EXPLOITED

1.4billion

1.4 billion people a year are now interacting with chatbots (Oracle)

80%

80% of businesses reported that they already use or plan to use chatbots by 2020 (Oracle)

265billiion | **30%**

Per year there are a reported 265 billion customer requests, with businesses spending nearly $1.3 trillion to service these requests; using chatbots can cut these costs by 30% (chatbotslife.com)

SUMMARY

Your organization no doubt has plans – for growth, for staying ahead of the competition, for digital transformation – all with the goal of meeting the objectives of the board and your stakeholders. Cybersecurity needs to be put at the center of every business decision in order to enable your organization to meet its overall objectives.

AMBIGUITY

HOW YOU MIGHT BE TARGETED

While we have hopefully helped start discussions of who might target you and why, the next step is to consider how. Obviously, this is not easy. Ambiguity is caused when something is unclear even when an appropriate amount of information is provided. Here, we attempt to break down how attacker tactics, techniques, and procedures manifest across multiple cyberattacks, equipping you with a vocabulary to explore these with your corporate and technical teams.

SOCIAL ENGINEERING TACTICS – AND THE PAYLOADS THEY DELIVER – HAVE DIVERSIFIED

Phishing emails have always been the most effective attack vector – many red team exercises result in full domain compromise, simply by luring someone to click on an email. The act of luring has crossed over into a relentless territory, with attackers using any and all personal information at their disposal to achieve their objectives.

In addition, attackers are extending the range of payloads delivered via this mechanism, from remote access trojans to ransomware, from worms to malware, from shortened URLs to Unicode URLs leading to websites that download malicious programs.

IN-MEMORY ATTACKS CONTINUE TO EVADE AND EVOLVE

There is currently no end in sight to exploitation of legitimate functions, including .Net, reflective DLL loading, dynamic loading of code within an existing process, and the trickling down and re-use of legacy tools. Stealthier techniques are making memory resident implants harder to find.

There are also a number of tools that are developed for legitimate purposes by defensive teams that have been leveraged by threat groups, such as PowerShell Empire and Cobalt Strike.

MALICIOUS ATTACHMENTS ARE OFTEN USED AS DECOYS

Malicious attachments have historically been a primary method for attackers to get a foothold within an organization. As detection of these attachments has become smarter and more mature, sophisticated actors now use attachments as decoys to mask the use of malicious LNK files or other equivalents.

For example, an analysis of the Iran-linked OilRig group recently uncovered a weaponized delivery document that was downloaded on exploitation alongside a decoy Excel spreadsheet. Cisco's Talos group also identified the Cobalt gang using malicious Word documents running VBA code, which kicks off the infection chain while displaying a non-malicious decoy document that is dropped to the hard disk.

WHAT YOU'RE UP AGAINST

Attackers have more time than their targets

Attackers will take months to plan their attack, performing reconnaissance on email filters, determining which employees fall for social engineering tactics, testing for whether or not known vulnerabilities have been patched, and amassing state-sponsored grade tools and techniques, among other activities.

Attackers only need one hit

During an active compromise, attackers will try any number of maneuvers in the knowledge that they need only achieve one success. Defenders – by contrast – need to succeed at every move. This asymmetry during a live compromise means that defenders and responders need to have the skills, expertise, and knowledge of the attacker mindset to be one step ahead.

Unintentional oversights are quickly exploited

More enterprise companies have vast IT estates with millions of servers and endpoints across multiple geographies. The sheer size of some IT estates makes it difficult to keep on top of all endpoints and the software running on them. Many groups lie in wait for a zero-day to be revealed, ready to perform searches for which companies have not responded to them.

Errors were at the heart of almost one in five (17%) breaches in 2018. That included employees failing to shred confidential information, sending an email to the wrong person or misconfiguring web servers. (Verizon DBIR 2018)

SUMMARY

Ambiguity speaks to the range of methods that attackers might deploy as they seek to compromise your business. While tools, tactics, and procedures continue to evolve, at their core many of them have remained unchanged, exploiting human error and manipulating legitimate tools to mask a malicious purpose.

CISO SUMMARY – THE VUCA CHECKLIST

The VUCA framework serves to guide how you craft your cybersecurity strategy and communicate it to your board. It can help remove the guess work when assessing who might target you, how, and why, supporting the case for what in your organization needs the most protection and how this is best achieved. We have summarized what we have covered so far in the following checklist:

VOLATILITY – WHAT EXTERNAL FACTORS AFFECT THE RISK TO YOUR ORGANIZATION

- The trickle-down effect – is your team ready to battle state-sponsored grade tools, no matter who is using them?
- Zero days – what protocols do you have in place for when an unknown vulnerability is revealed in software, hardware, and firmware?
- Supply chain: what is your process for vetting your suppliers?

UNCERTAINTY – WHO MIGHT TARGET YOU AND WHY

- How does your organization and your core business activities fit the stated objectives of state-sponsored groups, such as China's Five-Year-Plan?
- What in your organization is of value to any attacker seeking monetary gain, such as invoices, IP assets, M&A data, or personal details of customers?
- Who counts you as a supplier?

COMPLEXITY – WHERE YOUR BUSINESS GOALS AND GROWTH OBJECTIVES AFFECT YOUR SECURITY

- Digital transformation – while essential to growth and competitive edge – increases your attack surface. How is this continuously managed, and by whom?
- How do you manage the fluidity of your attack surface – i.e. updates and upgrades?
- Which elements of your attack surface are business critical and how would you manage them if they were compromised or forced offline?

AMBIGUITY – HOW YOU MIGHT BE TARGETED

- Phishing and social engineering
- In-memory attacks and their continuous evolution
- Malicious attachments as distractions

Consider:

- Some attackers will plan attacks for months – or even years
- Attackers need only one hit

2. HOW DO YOU STOP AN ATTACK?

The threat landscape dictates that we always need to be ready to respond to an incident.

Our Continuous Response methodology puts the right people, in the right place, at the right time (Collaboration), equips them with the right information to make a decision (Context), and the ability to take the right action (Control).

No matter where you are in your detection and response journey, our methodology can help. It was developed to guide organizations to manage incidents as they arise, provide a framework for fast decision making, offer a thorough understanding of the impact of certain actions, and cultivate the ability to gather evidence, intelligence, and forensics as the attack is happening.

In short, it's about making you ready to respond to an attack in its earliest possible stages, whenever it might hit.

But first, let's have a look at why detection – although essential – only gets you half of the way to securing your organization.

LEVERAGING YOUR INVESTMENT IN DETECTION

Attack detection has come on leaps and bounds. Over the past five years, the market has exploded. F-Secure Countercept was at the forefront of this evolution, developing our managed detection and response (MDR) solution to counter what we then saw as a massive gap in the market: as red teamers, we found the job of compromising organizations far too easy, and sought to bring the capabilities of the opposing blue team on par.

We also saw clear evidence that – despite the millions being spent on security tools – modern day attackers were devising creative and stealthy ways to bypass traditional detection. While automation went a long way in defeating automated attacks, there was a human element that was missing from attack detection. In short, we needed people to defeat people.

However, detection is not enough. And many detection offerings – despite including an 'r' for response in name – do not provide the ability to properly respond to an attack as it is happening. In addition, many solutions do not provide the necessary telemetry nor are they constantly fed with new threat intelligence as it is received, meaning that many teams are still only defending against known threats.

As we mentioned in Section 1, attacks are increasingly difficult to detect, due in part to unknown tactics, techniques, and procedures trickling down from the most sophisticated actors to a variety of threat groups, with many now possessing the capability to compromise an organization and achieve their objectives in mere minutes, without being detected by traditional prevention technologies. According to CrowdStrike's 2019 Global Threat Report, Russian state-sponsored attackers were logged at 18 minutes and 49 seconds to lateral movement after achieving initial foothold.

THE CHALLENGES FACING SECURITY TEAMS

TEAMS ARE DROWNING IN NOISE

79%

79% are overwhelmed by # of alerts[10]

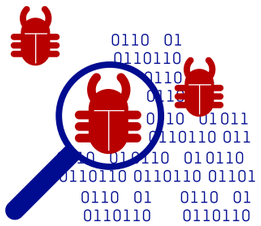
61%

61% of banks receive over 100,000 alerts per day[11]

50%

False positives are 50% of alerts[12]

ATTACKS ARE GETTING HARDER TO DETECT



28%

28% of attacks involving insiders are hard to detect due to legitimate access[13]

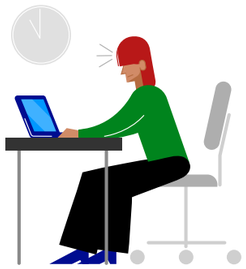
50%

50% of attacks involve criminal groups[13]

12%

12% of attacks are state sponsored[13]

DETECTION TAKES TOO LONG,THEN RESPONSE IS SLOW



100+days

On average it takes 100+ days to detect a breach[14]

46 days

On average it takes 46 days to resolve an attack with the cost of €18,689 per day[14]

€18,689 per day

[10] https://bricata.com/blog/how-many-daily-cybersecurity-alerts/

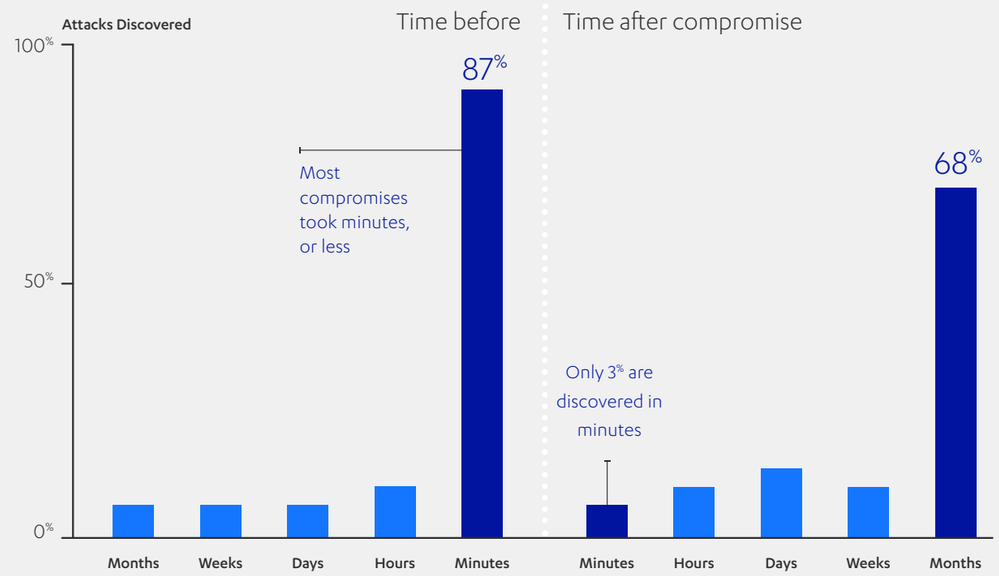
[11] https://www.americanbanker.com/news/alert-there-are-too-many-cybersecurity-alerts

[12] https://www.ponemon.org/local/upload/file/Damballa%20Malware%20Containment%20FINAL%203.pd

[13] Verizon: "2018 Data Breach Investigations Report" www.verizonenterprise.com/industry/public_sector/docs/2018_dbir_public_sector.pdf

[14] https://www.ibm.com/downloads/cas/861MNWN2

The industry is still struggling to detect and respond



68%

of attacks went undiscovered for months or more*

46 days

On average it takes 46 days to resolve an attack**

This does not mean that your detection investments thus far haven't been worth it. Continuous Response is only possible with good detection. It means elevating your detection capabilities to enable you to battle attackers when they are live on your estate, defeating the attacker early in the killchain, before business impact. Good detection feeds Continuous Response, constantly pushing attackers off your estate before they get a chance to persist. We will now explain how.

* Verizon 2018 Data Breach Investigations Report

** Ponemon 2018 Cyber Security Trend Report

THE CONTINUOUS RESPONSE METHODOLOGY

After decades of collaborating with internal and external teams to detect and battle live attackers, and still more years of developing our F-Secure Countercept technology stack and service, we have devised a methodology across people, process and technology, which any business can follow, regardless of their security posture or maturity.

We call it Continuous Response.

Continuous Response puts the right people, in the right place, at the right time (Collaboration), while equipping them with the right information to make a decision (Context), and the ability to take the right action (Control).

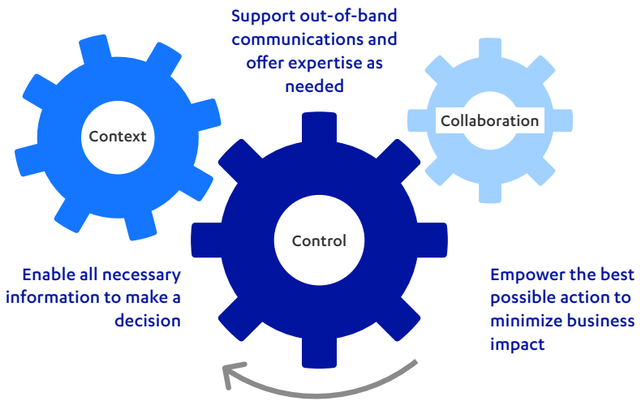
In more depth, it provides the three Cs:

Collaboration: Support for communication and cooperation between a pre-defined team of experts and decision-makers, both internal and external as needed, and providing the roles, remit, and responsibilities that enable expedient decision making.

Context: Access to all relevant business intelligence coupled with the most pertinent data and telemetry from across your estate so that teams can quickly understand and respond to the threat at hand.

Control: A range of options to contain a live attack and ensure the least possible business impact, while gathering live forensics and performing remediation.

How does Continuous Response work?



WHAT PUTS THE 'CONTINUOUS' IN CONTINUOUS RESPONSE?

Continuous Response supports ceaseless searching for signs of malicious activity, then facilitates a series of live response actions at the earliest indications of compromise. It aligns detection with response so that there are no delays when an attack is identified. Instead of response actions being taken only after a breach has happened, **Continuous Response** deploys subtle, tailored response measures early in the killchain, empowering an intelligent human response to a live human attack.

COLLABORATION

You need people to defeat people. When an attacker is live on your estate, you need skilled individuals with clear processes and technology to battle them.

Defined roles and responsibilities are the hallmarks of Continuous Response. The minute an attack is detected, multiple people across your organization need to work together. Collaboration is essential to enable fast decision making, with clean lines of remit across your IT estate, and the ability to escalate where required.

So how can you enable good Collaboration when you are under attack?

People

When an attack has been detected, you need a team of different skill sets – some you may have in-house, some may be outsourced. No matter where they are, there needs to be a clear chain of command. This needs to start with a primary contact.

PRIMARY CONTACT

The primary contact is the single port of call for the incident. Their job is to be the liaison between your organization, your security partner, and your supply chain (if applicable). They should have the mandate – and training necessary – to:

- Make and escalate decisions;
- Release budget;
- Provide management oversight;
- Manage the incident for the first 48 hours.

Crucially, they should have a thorough understanding of the **impact of certain actions**. For example, if the server with your customer data or payment processing is compromised, do you pull the plug? Do you have a back-up?

THREAT HUNTERS

Threat hunters – whether in-house or outsourced – are a core element of Continuous Response. While the term 'threat hunting' has seen many industry iterations since it was coined, for us it has always remained the same – threat hunting embodies a team of highly skilled and curious individuals, trained in the attacker mindset, using their knowledge and acumen to research and discover indications of compromise that cannot be identified with technology alone.

Threat hunters should do more than just detection – ours play equal roles in response. This can encompass pulling logs from the network, performing in-memory analysis, decompiling malware, and writing disruption scrips to slow the attacker down.

YOUR IT TEAM

Your IT team is instrumental in Continuous Response. No one collectively knows your estate better. For **Collaboration**, it is crucial that your entire estate is represented by a person or persons who have the day-to-day responsibility for each element. This can include responsibility for:

- Hardware;
- Software;
- Servers;
- Applications;
- A map of your estate and all the programs running on it.

Assigning a team member to know each element and all its facets can save hours and sometimes even days or months during an incident. It is worth noting that if the employees allocated to incident response perform business-critical functions in your day-to-day, it is suggested that they have a back-up team member to handle their business-as-usual responsibilities when they're called on to an incident.

YOUR SECURITY PARTNER

We can list many reasons why organizations should engage a security partner ahead of an actual incident. To start, it means you have established who you will call the second an incident has been identified; you will not waste valuable time googling 'who do I call when I'm under attack?' It means that you can build the crucial foundations for **Collaboration**, ensuring ahead of an incident that you and your partner have agreed processes, playbooks, roles, tools, and responsibilities. It can also mean that your business can test how you apply the Continuous Response methodology and get feedback on its efficacy.

When deciding how to best support Collaboration in your organization, consider:

- Who would head up the team that responds to an incident and liaise with your security partner? Would they have the remit to shut down servers in the middle of the night?
- When resourcing a team of technical experts, each with responsibility for your particular parts of your estate, is all your hardware and software covered?
- What's the process for when new assets are added?
- Who owns the program to communicate response readiness throughout the organization?
- Who will monitor and respond to simple anti-virus (AV) alerts?

Processes

During an incident, there can be a lot of unknowns. While this can make it hard to plan for on the surface, we cannot overemphasize the importance of establishing a basis for **Collaboration**. From the threat hunters who collect data and telemetry, to the principal contact having a dedicated conference line for the duration of the incident, to plans for backing-up or pulling the plug on infected servers and machines – all of these require pre-determined processes, signed-off by senior management. In our experience, the best place to start is with a playbook.

THE IMPORTANCE OF A PLAYBOOK

Your response playbook(s) may be the most important document that senior management ever signs. It helps you understand what you've got, where it is, and then articulate the processes for how you are going to protect it. During an incident, it expedites response, shortens conversations, and puts everyone – literally – on the same page.

However, one size does not fit all. While templates are useful, it is essential that your playbook fits with the roles, responsibilities, and objectives of your organization. It should be a collaborative effort with the entire IT team to ensure all assets, programs, and endpoints are logged, backed-up, accessible, and able to be investigated.

Part of the exercise involves thinking though worst-case scenarios, for example: who gets the call at in the middle of night? What if someone is on holiday? Is there a process for when certain people can't be contacted? Where will your data come from? What are the internal and external communications plans? Who takes the lead? What if it's your payment server that is compromised and needs to be shut down? Who has the authority to make that decision? How will you communicate that to your customers? Who will handle the press enquiries? Incident management often stretches far beyond security operation center (SOC) and IT teams.

HOW TO ENSURE THE SUCCESS OF YOUR PLAYBOOK

TEST YOUR PLAYBOOK. THEN TEST IT AGAIN. AND AGAIN.

Think of your playbook as a living document that must be continually fed. Assume that your company, as it grows and evolves, will undergo changes that must be reflected in your playbook for it to be an effective document. But before it is signed off, it is crucial that you test it to ensure all participants are clear on their role and that all processes can run as smoothly as possible. Think of it as similar to testing your disaster recovery scenario.

TEST EVERY PERSON IN EVERY ROLE

We have talked about the importance of clear roles and responsibilities. But this can and should be taken further so that every person in the core team is trained and tested in every role required. This ensures that all eventualities – and absences – are ready to be handled.

CONTINUOUS EVALUATION IS KEY

In any organization, things change – and they change quickly. This can lead to any number of oversights in existing plans – for example, when corporate restructuring occurs, something as simple as a contact list of who is responsible for certain processes could quickly become obsolete (for example, the Equifax breach occurred because the instructions to patch a known vulnerability went to an outdated list of recipients). Your incident response plan needs to be continuously re-evaluated, especially if your organization has undergone any kind of restructuring, merging, and even after any new incident to make sure your plan reflects your security posture and your evolving understanding of how and why you are targeted. The bedrock of **Collaboration** is having all network maps, mailing lists, and more up to date.

Technology

Part of knowing ‘who owns what’ is documenting – and making readily available – what assets are on your IT estate, but equally crucial is building a comprehensive technology stack that assists your IT teams and partners to perform Continuous Response. The specifications for such a stack are justifiably lengthy, but in our experience the mandatory elements are:

THE TECHNOLOGY SHOULD BE PROGRAMMED BY THE PEOPLE THAT USE IT

At F-Secure, we are constantly updating tooling based on the tactics, techniques, and procedures our threat hunting team discovers, both as part of their allocated research time and from battling attacks on our clients’ estates. Our threat hunters continually program in new hunts and hypotheses, and the team that develops our tooling sits alongside them.

THE RIGHT COMBINATION OF MACHINE LEARNING AND HUMAN UPDATES

The average IT estate of a multinational company generates millions of lines of data an hour. While we celebrate the necessity of the human element in attack detection, there is also a great deal that machine learning can do to identify known malware and executables. Machine learning and statistical analysis should help filter the noise and highlight anomalies so that threat hunters are able to spend their time investigating the most suspicious incidents, rather than wading through data.

COMMUNICATION

It goes without saying that during an incident communication is vital. Ideally, there should be a portal or central communication platform to enable all teams to get clear, instant transparency into the status of the attack. It is also worth exploring out-of-band communication options, as normal channels and connectivity may be compromised.

Now you have the basis for **Collaboration**, how do you start to amass the information necessary to battle an attack? With **Context**.

CONTEXT

When an attack is detected, it is crucial that we quickly gather data to inform decisions. But how do we gather the right data and ensure its integrity?

Context is about providing the right environment for collecting data to provide as much information about the incident as possible. You need trained specialists that have the right tools to distill datasets down to what is most useful. Where do you start?

With threat hunters.

People

When an attack hits, a wide group of people will be required to feed in relevant information around the wider business context and potential impact of various actions. (You can read more about how best to account for this need in our **Collaboration** and **Control** sections dealing with playbooks.) Preparing your teams and partners with ongoing training, readiness exercises, and consultancy engagements – such as threat modelling, purple team exercises, and attack path mapping – will also help give your team the knowledge and experience to make well-judged decisions at speed, accounting for all of the relevant business context and knowing what information is going to be most important.

However, when an attacked has been detected, equally important is establishing clear chain of command. This needs to start with a primary contact.

THE THREAT HUNTING SKILLSET

Threat hunting – while becoming more established – is still an emerging field and it can be challenging to find experienced hunters for your team. F-Secure Countercept is no exception to this, which is why we value our team so much.

However, we have learned that years of experience isn't always necessary – there are a myriad of skills, personality traits, and background that indicate whether an individual would make a good threat hunter. Years of experience and a relevant degree are not necessarily essential. Instead, you want your team to look outside convention and forge a path that should sometimes goes against the traditional InfoSec flow. They should be more than threat hunters – they need to embody the traits and skills of red teamers, incident responders, and data scientists.

Threat hunters should be:

FASCINATED AND INSPIRED BY SECURITY

This can be demonstrated in a number of ways, such as building a test network at home to simulate attacks, reversing malware in their spare time, maintaining an active Github account, and attending security conferences. Look for demonstrative evidence that they live and breathe security.

TECHNICALLY BRILLIANT

Threat hunters must know computers at a very deep level – how they work, how they break, and how they are used and abused. They also need to understand operating system (OS) fundamentals and internals, networking fundamentals, and have an innate understanding of how machines talk to each other. Having good knowledge of programming and scripting can also be invaluable when dealing with multiple systems, large datasets or forensic artefacts to speed up analysis and integration.

CHALLENGING AND QUESTIONING

Threat hunters should be innovative in how they approach problems and should solve them in new, creative, and constructive ways. Threat hunters should never be satisfied with the status quo and should always use their knowledge to drive improvements in how attacks are detected.

ABLE TO ADOPT THE MINDSET OF AN ATTACKER

Part of the job of a threat hunter is to know how attackers operate, anticipate an attacker's next move, and discover future techniques before the attackers themselves. Threat hunters should be capable of executing simulated attacks against your detection tooling to ensure that the correct telemetry is collected, allowing them to do their job effectively.

GIVEN TIME TO RESEARCH

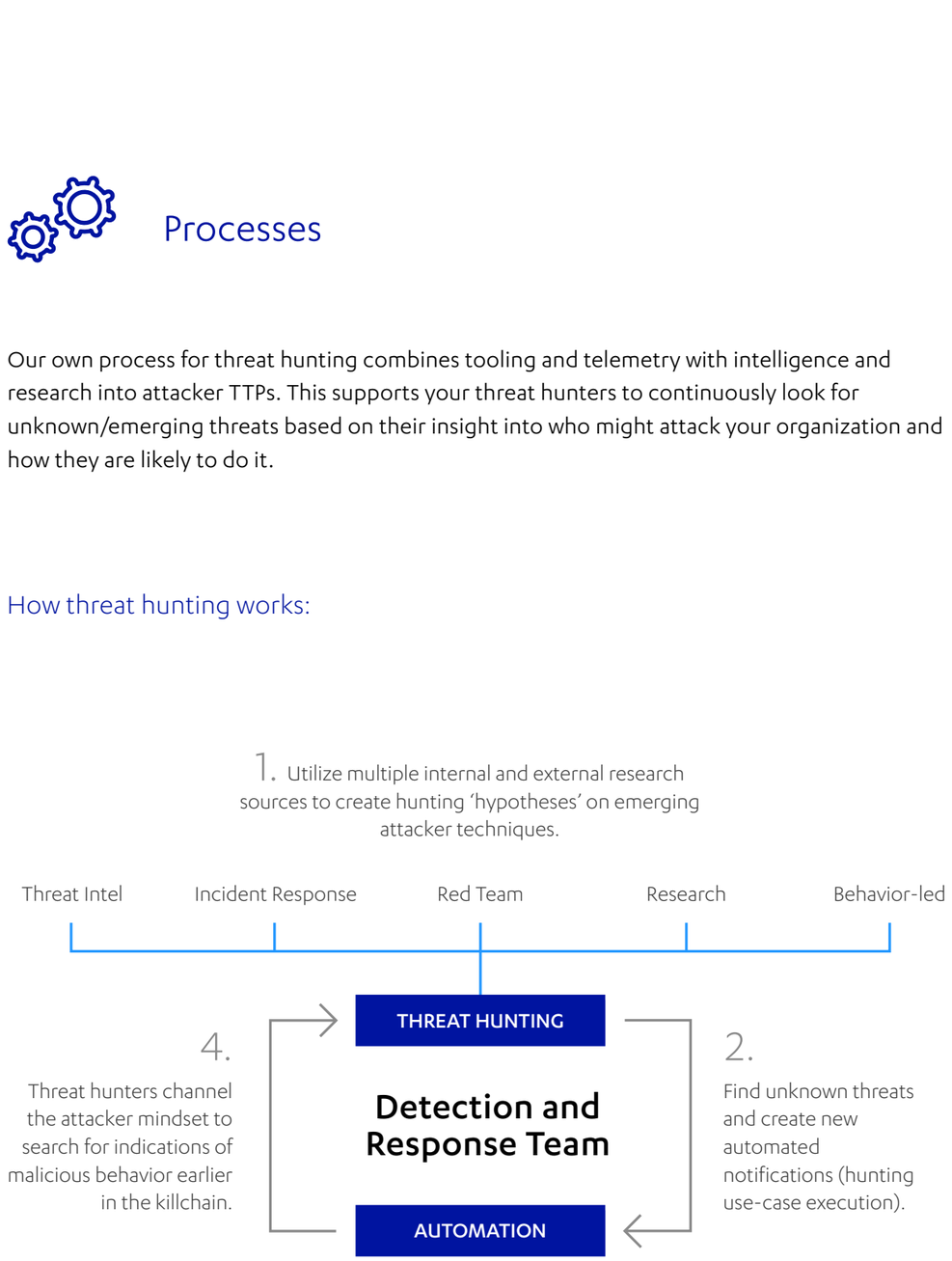
We give our threat hunters dedicated time to research new attacker tactics, techniques, and procedures, alongside testing both proprietary and open source defender tools and developing open source code and tools to distribute to the wider security industry. This – coupled with the fact that our hunters perform threat hunting across estates of all sizes, industries, and geographies – keeps them at the forefront of attack detection.

Processes

Our own process for threat hunting combines tooling and telemetry with intelligence and research into attacker TTPs. This supports your threat hunters to continuously look for unknown/emerging threats based on their insight into who might attack your organization and how they are likely to do it.

How threat hunting works:

1. Utilize multiple internal and external research sources to create hunting 'hypotheses' on emerging attacker techniques.



2. Find unknown threats and create new automated notifications (hunting use-case execution).

3. Automation of discovered threats reduces false positives and increases the time available to seek out and research new attacker TTPs.

4. Threat hunters channel the attacker mindset to search for indications of malicious behavior earlier in the killchain.

Technology

THE TOOLING THAT THREAT HUNTERS NEED

Threat hunters perform an essential first step in helping organizations battle a cyberattack: by detecting it in the first place. To detect a live, hands-on keyboard attack requires innovative and constantly updated tooling that reflects threat intelligence and known threats to better enable the threat hunter to establish if an attack is authentic and hunt up the killchain. This is equal parts process and technology.

EDR

Endpoint detection and response (EDR) agents are the essential foundation for detecting and responding to attacks on your organization. They ensure that all endpoint activity is captured and logged, and should contain a rich suite of features to enable Continuous Response.

The process of EDR deployment – when done prior to an incident – is often an illuminating and clarifying exercise to identify the exact number and location of endpoints in your organization, enabling teams to look at possible attack paths an attacker might exploit to access your critical assets, and eliminate those paths as part of the deployment.

Other telemetry should include logs and network data.

DATA ANALYTICS

Information gathered via your EDR should be analyzed by threat hunters – either internal or outsourced – to discover anomalies that provide early warning signs of malicious activity, such as persistence mechanisms, memory manipulation, process information, user sessions, and many more data sources.

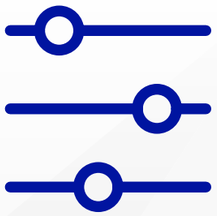
THREAT INTELLIGENCE

As new threats are identified, they should be added to the intelligence feed; they then become known threats, so that any attack with the same signature will be flagged. Not only does this help eliminate false positives, it enables threat hunters to create use cases from indicators of compromise seen in the wild.

COLLATING THE 'RIGHT' DATA

When an attack is suspected, the agent should help reduce the threat hunter's dataset as much as possible. People, processes, and technology should combine to ensure that you are able to group data based on, for example, how anomalous the data is, as well as the ability to filter data to look for specific files and processes.

Now that you have the data, the business can make informed decisions to take the next step and take **Control** of the incident.



CONTROL

Direct the attack instead of letting the attack direct you

Control encompasses the investigation, containment, and remediation actions that enable Continuous Response during an attack.

Response can be performed by one person or multiple people depending on your organizational size and budget, but the core skills involve taking the data collated during the **Context** phase to contain the incident while gathering live forensics and artefacts.

People

THE VALUE OF FIRST RESPONDERS

Having 'first responder' expertise embedded throughout the team – from defender to incident responders – significantly increases the success of later investigative activity. This enables your team to make collaborative, informed, and critical decisions that will affect the business continuity of your estate. Having dedicated first responders allows you to perform the acquisition tasks that enable experienced investigators to conduct analysis and investigate much sooner. Think of it like the fire marshal at your office – i.e. someone who knows what to do in the event of a fire and how to make sure everyone gets out safely, but doesn't replace the fire brigade.

Time is of the essence when there is an active threat actor on your estate. Your first responders can greatly reduce the time that hostiles remain in control and ensure optimum containment and remediation.

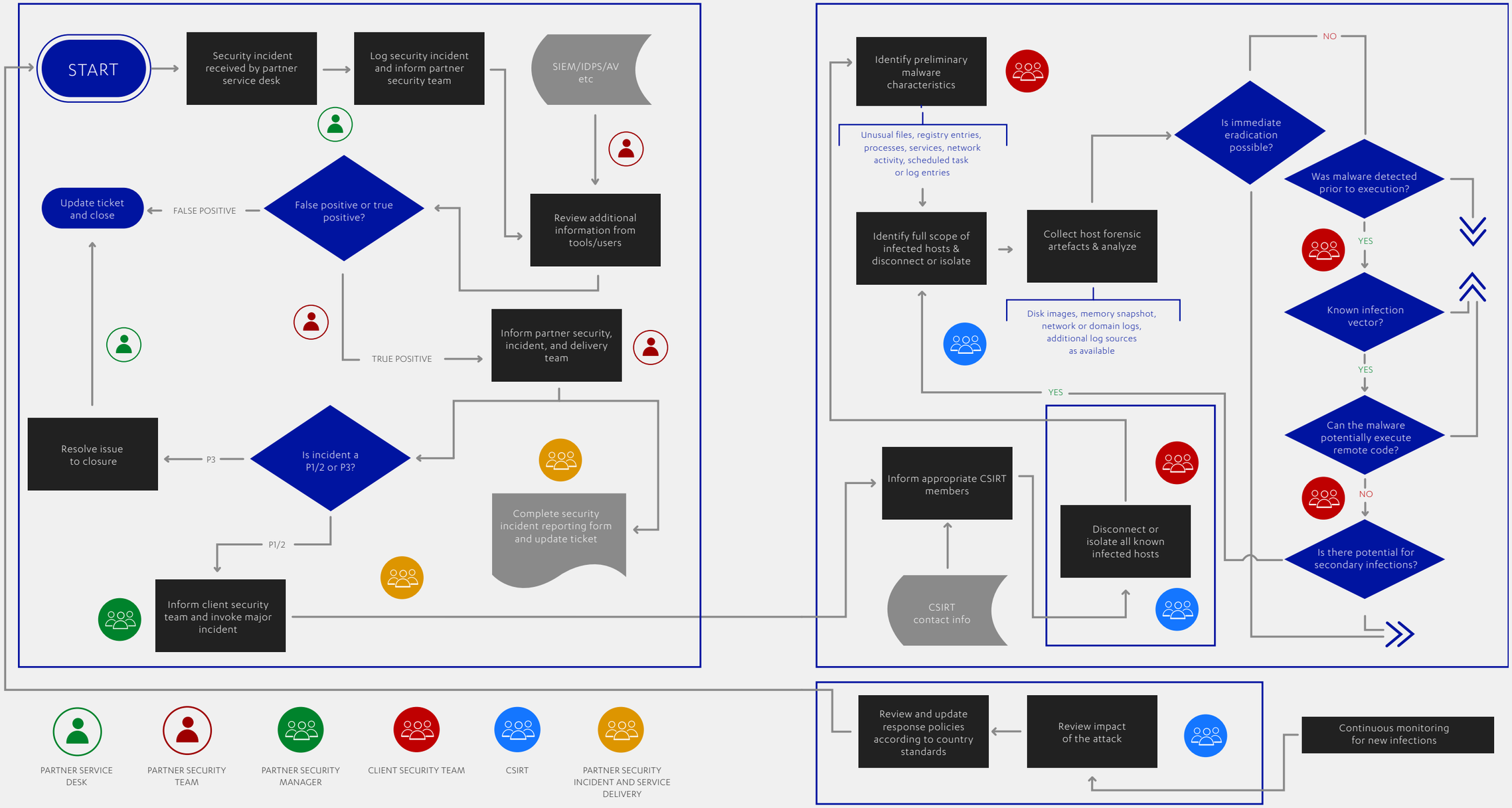
Your team should have, at minimum:

- Knowledge of your organization's policies and procedures for evidence handling;
- The ability to pull data from memory, disk, network, and logs;
- Methods for tracking evidence, analysis and triaging;
- The ability to manage an incident for the first 48 hours after detection, alongside the primary contact.

Processes

SAMPLE PLAYBOOK: GETTING EVERYONE ON THE SAME PAGE

This is one of many playbooks for a client and their security partner. While we have not illustrated the entire process, it will hopefully give you an idea of how much detail is required for documenting processes, ahead of an incident.



Technology

TOOLING FEATURES FOR CONTINUOUS RESPONSE

Response tooling should allow for rapid triaging of suspicious activity and the ability to perform a deep investigation on the suspicious activity identified from the attack detection data and other sources. It should help the responder pinpoint when an attacker gained a foothold on the network, how the attack evolved, what tools and techniques they used, and many other details. This information is invaluable as it helps when tracing an attack path, taking measures to stop it and/or preventing another compromise occurring again via this method.

Responder tooling should have the capabilities to:

- Capture forensic data – such as memory or disk artefacts and sending them to the team for further analysis;
- Actively sweep multiple endpoints for the existence of particular indicators of compromise (IoCs);
- Use the data from **Context** to trace the timeline of the compromise;
- Find key artefacts in the compromised machine's file system;
- Capture all event logs from the target machines.

Responders should be able to have the technology to:

- Perform actions on the registry, scheduled tasks, services and files on a target endpoint to ascertain if a foothold has been obtained;
- Have visibility of network-related activity on the target endpoint to detect any malicious outbound connections – for example, to a command-and-control (C&C) server owned by a malicious actor – as well as other suspicious events;
- Retrieve a specific file or folder from a desired endpoint, including registry hives and master file tables. This is especially useful in cases where a known malicious or suspicious file has been detected on a host and retrieval is necessary to perform further offline analysis;
- Delete a scheduled task, service or registry key, making it possible to stop a known malicious persistence mechanism further executing.

ACTIVELY PREVENT ATTACKERS FROM CONTINUING TO OBTAIN THEIR OBJECTIVE

During a live, hands-on keyboard attack, the ability to thwart the attacker's actions – without making them aware that you are doing so – protects your assets while giving responders time to analyze the activity and contain the threat.

There are different levels of sophistication to this capability: basic and advanced, as explained below.

BASIC

Blocking the network connection will cut the connection between the host and a malicious domain. In cases where simple degradation is not enough, blocking specific connections can result in the attacker being unable to use specific endpoints.

Isolating the target endpoint(s) is the most powerful of the active defensive tasks, as it isolates the target endpoint from the network and blocks all connections except the ones to the responder, therefore allowing the threat hunter or responder to still continue performing defensive and investigative actions on the host. This can be used both to contain a known threat or to contain a known target of the attackers to prevent them from reaching their goal.

ADVANCED

Degrading the quality of a network connection can slow down attackers and hamper their efforts. Responders can limit the transfer rate of both outgoing and incoming packets to and from a given IP address range for a given endpoint. This results in the attacker's actions taking longer to perform particular data exfiltration, buying the response team valuable time to get a full picture of the compromise.

Contain and disrupt the attack by degrading the C2 channel of the attackers, while not alerting them that they've been detected.

3. WHAT THIS MEANS IN PRACTICE: CONTINUOUS RESPONSE CASE STUDY

Our Continuous Response methodology is not just about battling live attackers, although this is a large part of it. The rest is about response readiness permeating every aspect of an organization to ensure that – in the event you are breached – there are multiple facets (and people) ready to be deployed and distributed.

In this section we are going to illustrate the compromise of a global financial organization. (This real event has been anonymized to protect the organization's identity.) We will first describe the incident as it unfolded, then illustrate how Continuous Response might have yielded a different outcome.

HOW ATTACKS UNFOLD

One of the most common ways to describe an attack is via a concept known as the killchain. This is often shown as a linear process, with the attacker following a set number of steps at each stage to reach their goal, such as reconnaissance, initial exploitation, lateral movement and data exfiltration. The reality is that modern attackers are rarely this linear in their methodology, instead adopting a more flexible approach to the process of information-gathering, exploitation, and privilege escalation.

The attack in this case study is no exception. However, for the purposes of illustration, we will use the traditional killchain to describe how the attack unfolded.

HOW THE ATTACK UNFOLDED

RECON

A global financial organization had a well-established incubator for smaller fintech start-up companies, some of which it would acquire. This was well documented on the organization's websites.

A state-sponsored attack group targeted one of these soon-to-be acquired companies, which at the time had a two-person IT function, with administrator rights shared by the small team.

DELIVERY

The attacker executed a watering hole attack via the website of a law firm frequented by the fintech company's legal team. The malware was dropped in such a way that it would only target this particular company – anyone else from another organization who accessed that law firm's site would not have been affected.

PERSISTENCE, CONTROL, PRIVILEGE, LATERAL MOVEMENT

Because all employees had administrator rights, lateral movement was easy for the attackers to achieve. They quickly moved through the estate, searching for fileshares and dropping further tools and back doors.

OBJECTIVE 1

Over six months the attackers had moved through the entire estate, targeting the source repository, staging and exfiltrating source code as they went through.

However, this was just the beginning.

OBJECTIVE 2

The fintech company was unaware it had been compromised when it integrated into the financial organization's estate. The organization had a well-established cybersecurity program that included threat hunting, as well as time-honored integration procedures. Everything from the fintech company should have been wiped and rebuilt as part of the financial organization's protocols, but because of timing it was a straightforward move and reboot. The attackers – effectively – moved with the fintech company.

THE INVESTIGATION STARTS...

ATTACK DETECTED

24 hours after the integration had begun, the global financial organization's internal security operations center (SOC) witnessed some suspicious traffic from the endpoint gateway intrusion detection systems. However, because of the expedited nature of the integration, none of the financial organization's cybersecurity controls were rolled out to the fintech company.

ENGAGE SECURITY PARTNER

At the start, the SOC fairly assumed the communications might be standard for the fintech company, but they chose to play it safe and engage an incident responder.

Because of the expedited nature of the integration, none of the financial organization's company's security controls were rolled out to the acquired company. Our team deployed EDR to the fintech company to enable telemetry gathering, where possible.

MALICIOUS ACTIVITY IDENTIFIED

Hours later, with our team on-site, malware was beaconing over DNS to establish communications.

REVERSE ENGINEER MALWARE AND REDIRECT COMMUNICATION

It was at this point that our team took control of the C2 channels to "chase the beacon" and ascertain where the attackers were headed, redirecting the C2 to infrastructure under our control, in order to capture the encrypted traffic. In tandem, our team at F-Secure LABS began reverse engineering a sample of the malware and its encryption routines.

LOCATE AND ISOLATE

Once this was completed, we were able to decrypt the captured C2 traffic, work out the exact number of machines that were beaconing, and then isolate them.

AN IMPEDED INVESTIGATION

By this point, the company had lost a great deal of data, both from the fintech and the financial organization.

A CHALLENGING INVESTIGATION

There were many other elements that made the engagement challenging. We had a series of phones calls from the organization – who were understandably panicked – but in contrast, we often found it difficult to get hold of the right people. The team or individuals we were able to talk to often didn't have the authorization to make decisions or sign-off budget.

SO, HOW COULD CONTINOUS RESPONSE HAVE YIELDED A DIFFERENT OUTCOME?

HOW CONTINUOUS RESPONSE MIGHT HAVE YIELDED A DIFFERENT OUTCOME

There are a number of ways that Continuous Response might have yielded a different outcome to this compromise:

COLLABORATION

INVOLVING SECURITY PERSONNEL IN KEY DECISIONS

While the expedited integration was not an ideal scenario, it should have been workable had security teams been more involved in the decision to not follow normal M&A protocol. The security team could have executed other actions if the deadline was immovable, such as rolling out EDR to the fintech company ahead of the integration.

A VIEW OF THE ENTIRE ORGANIZATIONAL INFRASTRUCTURE

Part of the Continuous Response methodology provides companies with the three Cs of their own infrastructure, so when an attack occurs, teams can ensure that the entire estate is mapped. The containment component of this investigation suffered due to the estate not being fully mapped. The three Cs ensure that organizations are taking continuous assessment and inventory of their estate, which gives them better control of their business.

STANDARDIZED ROUTE OF ESCALATION AND PROCEDURES

The Continuous Response methodology guides defining processes for as many eventualities as possible, including those which are unexpected. This includes a standardized route of escalation and procedures for communicating sensitive topics ahead of mergers and acquisitions (M&A).

A PRE-DETERMINED METHOD OF COMMUNICATION

A good Continuous Response platform will provide dynamic means for communicating, escalating, and authorizing certain actions. The ideal world of Continuous Response has a live platform that shows who is online, what their authority is, and sends messages when certain actions have been taken.

CONTEXT

STREAMLINED METHODS FOR COLLATING AND DISTRIBUTING DATA RELATED TO THE ATTACK

Only part of the financial organization had EDR rolled out, with the fintech company having none. This made it difficult to immediately trace the attack path. In addition, while the SOC team were quick to detect the attack, there wasn't an established routine for providing data from across the estate to aid the investigation.

CONTROL

DETECTION, WITH BASIC REMEDIATION IN-HOUSE

The financial organization had a well-established SOC with threat hunting capabilities that extended only to detection. The SOC had plenty of talented people looking at alerts, but a more ideal scenario would include all team members being trained in containment, remote investigation, and the ability to scale the response.

CONCLUSION

This whitepaper has aimed to make the case – and provide the methodology – for bringing your organization into a new era of response. We have seen the worst of the threat landscape to date and believe passionately that Continuous Response is crucial for how organizations defend themselves, their employees, and their shareholders.

We know it is not an easy endeavor. It requires a great deal from security leadership, teams, and senior management.

No matter where you are in your journey to defend your organization, whether you already have threat hunting teams, an EDR, or a response retainer, our purpose is to enable businesses to operate without the impact of a cyberattack.

A more secure world benefits us all.

Join the conversation. We are keen to hear your questions and feedback.

www.f-secure.com

Connect with us