Threat detection lessons...

...from hacking ourselves

Orange
Cyberdefense

orange™

Part 1:

Setting the scene

Cybersecurity spend has increased drastically over the last few years, with 2018 alone seeing an increase of 12.4% in wordwide spending on information security products and services, according to Gartner*. The market research firm predicts the market will grow a further 8.7% to $124 billion through 2019.

But despite this ever-increasing spend, data breaches and successful attacks only appear to be on an upward trajectory. The UK Government's Cyber Security Breaches Survey 2018, published in April 2018, discovered more than two-fifths of businesses (43%) experienced a cybersecurity breach in the previous 12 months.

As a result, research by the World Economic Forum found that cyber-attacks are businesses' number one concern and that they fear the actions of hackers will threaten their organisation over the next decade. At the same time, cybercriminals are improving their monetisation abilities and becoming more technically sophisticated and bolder in their attack methods.

When combined with progressively harsher sanctions being implemented by regulators, the threat of a data breach becomes more problematic and expensive for businesses. Delivering the always-on, highly specialised maintenance and monitoring required to prevent these increasingly sophisticated attacks is difficult and highly resource intensive. Businesses are therefore struggling to respond to the higher level of threat themselves. Indeed, the UK Government study found that around one third of businesses (30%) believe the staff responsible for dealing with cybersecurity are not capable of doing so.

One way to gain access to the highly skilled, around the clock expertise required to ensure defences stand up against cybercriminals' expertise is to work with a Managed Security Services Provider (MSSP). This approach can fill the gap, as a competent provider can offer the appropriate level of skills and experience to make the right choices and counter the threats. However, it may also require a significant paradigm shift.

Engaging with an MSSP requires a high level of trust in that organisation's capabilities and integrity. Furthermore, standardisation and regulation remains basically non-existent in the MSSP space, which can make it extremely hard for buyers to know whether to trust a provider. For example, it was alleged that Dell Secure Works may have played an accidental role in facilitating the data breach suffered by Marriott last year. While it's also been alleged that hackers working on behalf of China's Ministry of State Security breached the networks of Hewlett Packard Enterprise and IBM as part of a wider campaign deliberately targeting MSSPs. By establishing a culture of specificity and transparency – namely sharing exactly what they are doing, how they do it, and what results they are achieving – MSSPs can build a level of trust that becomes absolutely crucial to customers.

As an MSSP we believe in demonstrating transparency to our customers. And it's in this spirit that we decided to share the results of a recent 'red-team exercise' that we performed on our own environment – essentially hacking ourselves.

* Source: https://www.gartner.com/en/newsroom/press-releases/2018-08-15-gartner-forecasts-worldwide-information-security-spending-to-exceed-124-billion-in-2019

At a glance: Security

12.4% increase in cybersecurity spend in 2018

8.7% growth predicted through to 2019

$124 billion: predicted market valuation through 2019

43% of UK firms have experienced a cyber security breach in the last 12 months

#1: Cyber-attacks are the top concern for businesses according to World Economic Forum

Part 2:

What we learned from attacking ourselves

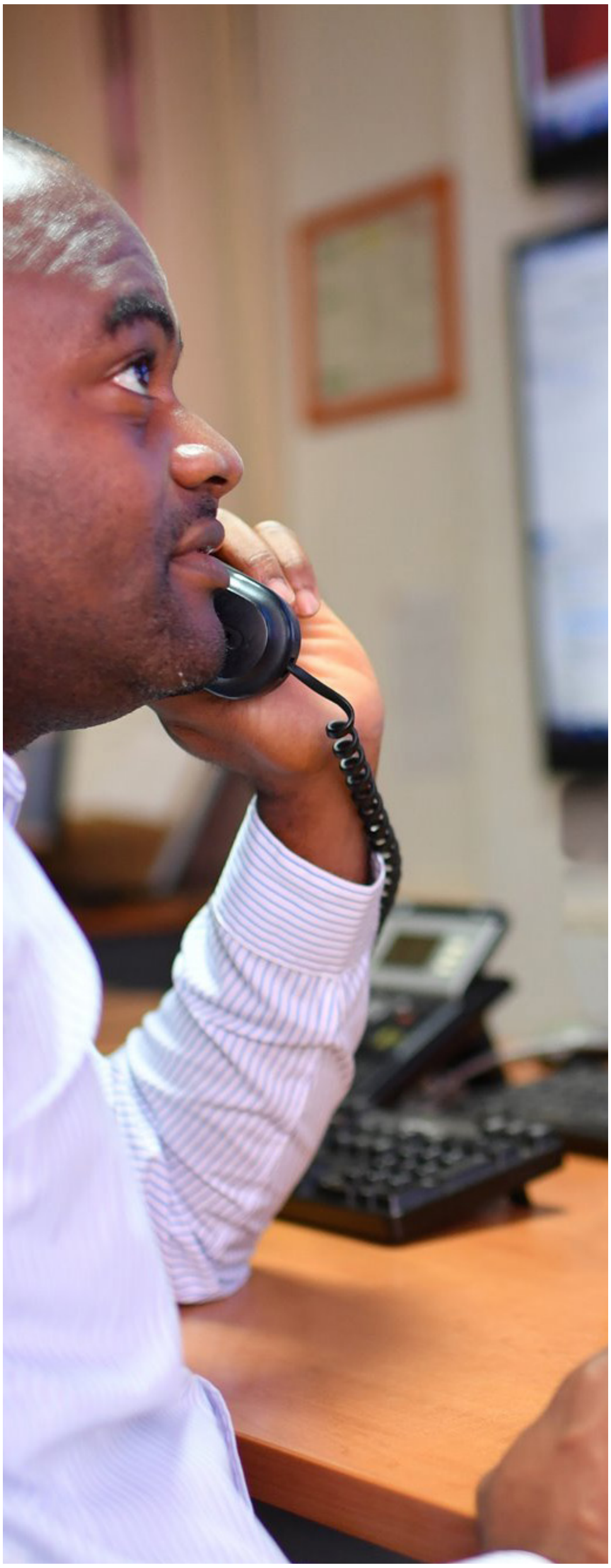
To investigate the ease with which attackers can gain access to corporate systems and how prepared businesses are for the inevitable, we're taking the unusual step of documenting the results of an internal 'red team' exercise of our own estate for our customers to review.

We wanted to verify how our systems would cope with an incoming attack and how successful someone would be if they came at us with malicious intent and share the experience with our customers, whom we believe face the same threats and challenges. We also wanted to assess how well our Managed Threat Detection (MTD) service would perform in the face of a compromise by a skilled adversary, and similarly share those findings for the benefit of our customers.

So we tasked our SensePost research and penetration testing team with the job of simulating the lateral movement and privilege escalation parts of an attack that commence after the perimeter has been breached. This kind of attack simulation makes the assumption that any network perimeter can, and eventually will, be compromised, and seeks to assess how robustly internal systems respond to an attacker who has found a route to the inside of an environment.

Having kick-started the process by granting the 'attackers' access to a machine with an IP address inside our network, the lateral movement process started with using open source data containing information about employees, such as LinkedIn, to build an initial list of Active Directory user IDs. With this list compiled, the attackers ran login attempts against our Windows Domain with a series of commonly used password formats and managed to find a match that provided access to one regular internal user's account. The user's credentials in turn enabled them to gain a list from Active Directory of all active users against which they again ran the login attempts, this time succeeding in obtaining access to an administrative user.

> **Our faux attacker was able to compromise an entire network by using a list of predicted template passwords to hack into the domain admin's account in less than a day.**



Our attacker was also able to gain access to our systems by infiltrating a disused machine that we presumed to be off the grid.

With this heightened level of access to our systems acquired, the ‘attacker’ turned to a popular hacking tool called Mimikatz, which enables intruders to quickly jump from account to account on a Windows Domain and thus spread their net inside an organisation.

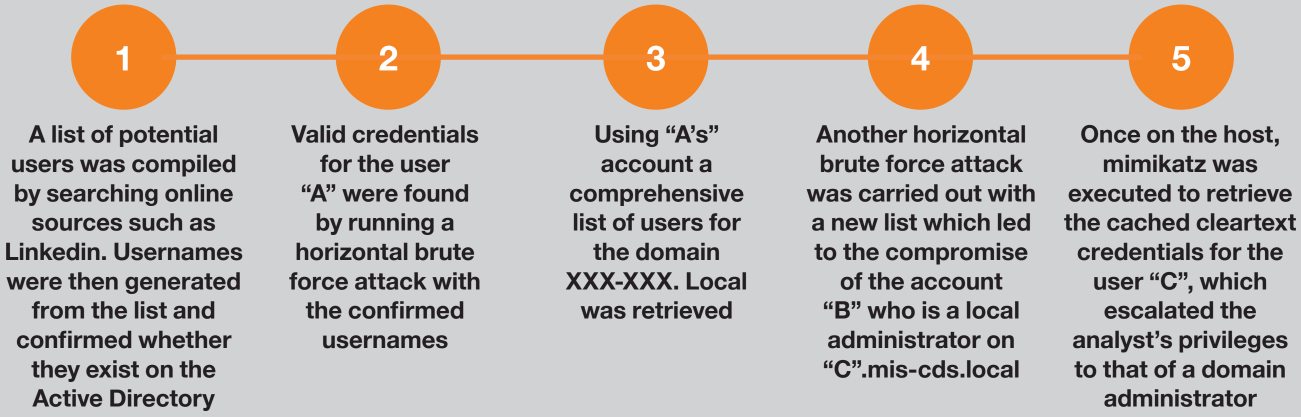
Mimikatz has shot to fame in recent times for its association with the NotPetya and WannaCry ransomware strains. In our case, Mimikatz enabled the SensePost hackers to extract password hashes and even clear-text cached credentials for a domain administrator account, effectively granting them full control over many of our internal admin systems.

Our faux attacker was therefore able to compromise an entire network by using a list of predicted template passwords to hack into the domain admin’s account in less than a day.

Analysis of hundreds of assessments performed by SensePost tells us that this is a typical scenario for enterprises running contemporary Windows environments with significant numbers of users. However, in our attack things were about to get a whole lot more scary.

Compromise of the domain administrator through weak passwords:

The 5-stage attack path taken to compromise the domain through weak passwords



1 A list of potential users was compiled by searching online sources such as Linkedin. Usernames were then generated from the list and confirmed whether they exist on the Active Directory

2 Valid credentials for the user “A” were found by running a horizontal brute force attack with the confirmed usernames

3 Using “A’s” account a comprehensive list of users for the domain XXX-XXX. Local was retrieved

4 Another horizontal brute force attack was carried out with a new list which led to the compromise of the account “B” who is a local administrator on “C”.mis-cds.local

5 Once on the host, mimikatz was executed to retrieve the cached cleartext credentials for the user “C”, which escalated the analyst’s privileges to that of a domain administrator

The above diagram shows attack via brute force and mimilkatz. Once a domain user’s account had been compromised through a horizontal brute force, a list of all domain users was retrieved using rpcclient with the following command: rpcclient XXX.XXX.XX.X-U ‘mis-cds.local\<redacted_domain_user>%May2018’ -C enumdomusers.

Lamenting legacy

Taking a different tact our attacker was also able to gain access to our systems by infiltrating a disused machine that we presumed to be off the grid. An old ticketing system that had been replaced, stripped of data, hadn’t been used in a while and was completely disconnected from the environment… or so we thought.

While the attackers were unable to take any data off the machine itself, they were able to use it to escalate their privileges across the domain.

This demonstrates how serious a threat legacy systems or machines can pose to your business. The old computer, printer or derelict laptop that’s been sitting in the corner of your office for months or even years collecting dust could easily be your biggest security vulnerability. And it could be an attacker’s route into your critical systems and data.

So no matter how inconsequential you feel a machine or network is, always ensure it’s patched so that you remove the threat.

Part 3:

How they do it

As the technology available to businesses increases in complexity and sophistication, so too does the arsenal available to their attackers. Cybercriminals are constantly evolving their tools, techniques and methods for that one opportunity that grants them access to a business' network.

Passwords

Passwords are a particularly perilous issue for businesses.

The obvious assumption was that the passwords belonging to our users were weak or obvious to guess. But on the contrary, we apply an ISO and PCI mandated strong password policy, just like most of our customers. Indeed, from an analysis of 600,000 passwords used by our customers, the vast majority were between 8 to 12 digits long and used combinations of letters, numbers and capital letters. All of which would adhere to the vast majority of even the most stringent security policies.

Indeed, our passwords weren't cracked because they were weak, but because they were predictable – as demonstrated in the graphic on the right.

Armed with a veritable plethora of password data available from publicly disclosed breaches, sophisticated cybercriminals are well aware of these common password trends, and use this information to build templates that form the basis of highly targeted attacks. These same password templates are used when conducting brute-force attacks directly against a log-in interface and when cracking hashes recovered by dumping hashes from the Windows cache.

In fact, the one actual password that our attacker was able to derive – by dumping the password cache on an already-compromised machine – was 8 characters long and included capital letters, numbers and punctuation marks. This demonstrates the importance of having measures in place to negate attackers' extraction and cracking tactics and understanding attackers' motives, as we shall describe later in this report.

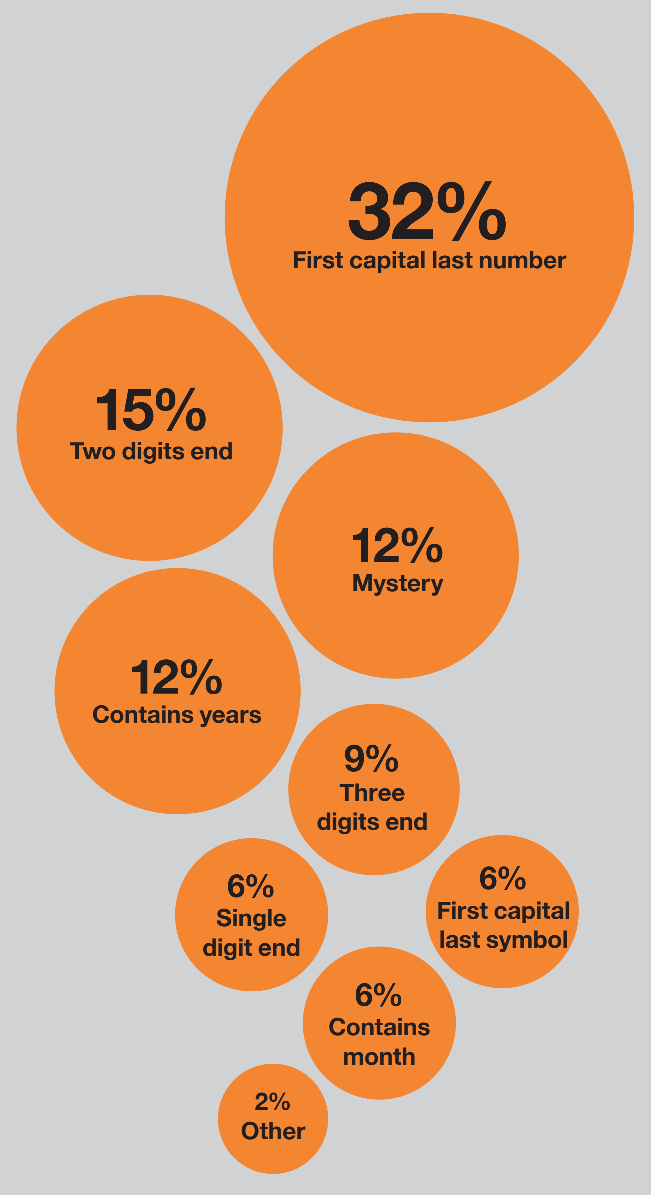
Malicious Attachments

An additional controlled experiment that we carried out saw our attacker breach an endpoint using native Microsoft Office DDE, which we enabled to evaluate how our detection technology would respond.

This began with an email attachment containing an embedded DDE object, which the attacker used to reach out to and evoke an external payload. This type of attack would present the end user with a series of common Microsoft Office error message boxes and queries about whether they want to enable editing, but no explicit security warnings. Upon hitting 'yes,' these trigger the download and execution of a PowerShell script that ultimately provides the attacker with full command and control of the machine.

With DDE enabled and the affected versions of Microsoft Office installed, this form of attack is devastatingly easy and effective. However, with the right kind of instrumentation, it's also easy to detect…

Passwords:
Weak passwords characteristics



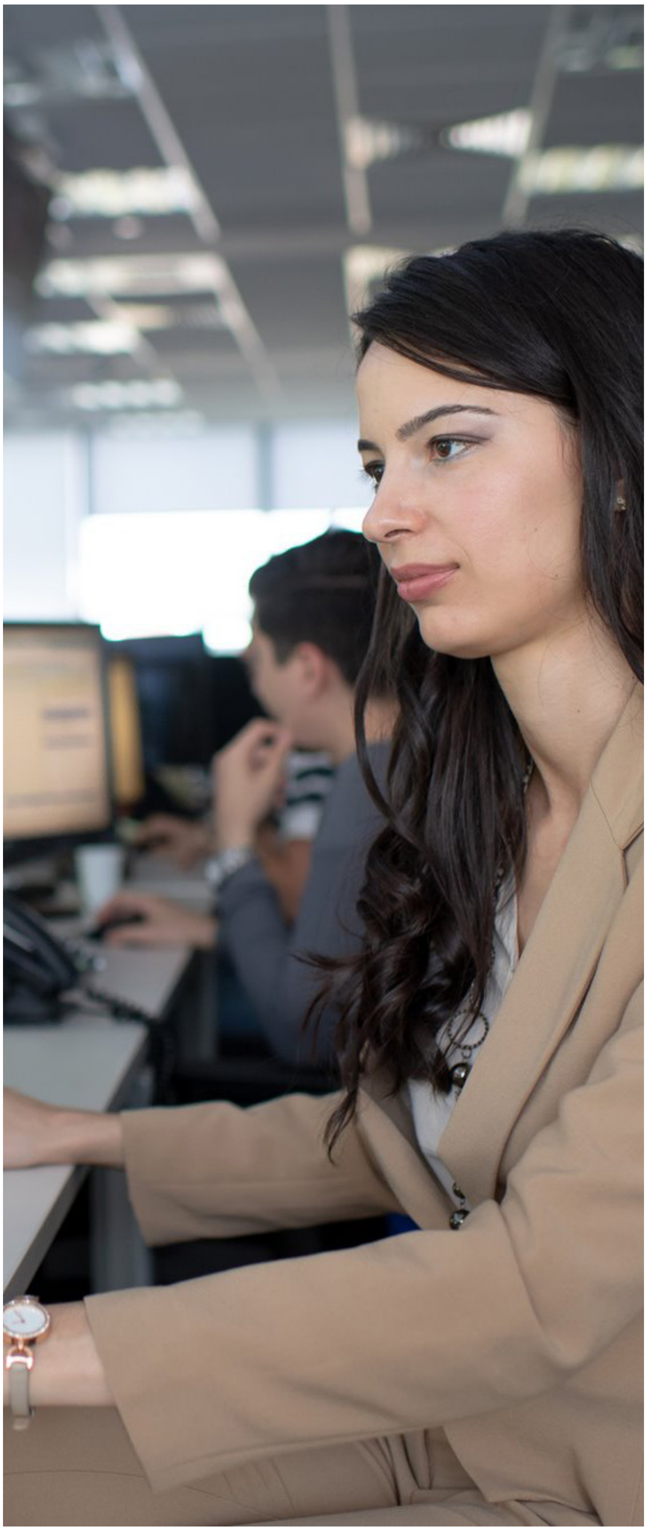
Kerberoasting

We also ran an attack path to compromise the domain through Kerberoasting, a common method that abuses service tickets on the network authentication protocol Kerberos, and resuses them to gain access to the targeted service. Once again online sources, such as LinkedIn , were used to compile a list of people possibly working for Orange cyberdefense. This was then used as a wordlist with an LDAP user enumeration tool to determine two things: whether a particular account existed on the domain; and the naming scheme of users.

After confirming the accounts existed within the domain, a horizontal brute force attack was launched against the SMB service using the password cracking tool THC Hydra. This resulted in discovering valid credentials for a domain user. Shortly after the attack, our defences discovered it and identified the account that had been compromised as we will describe later. However, for the purposes of this experiment we allowed the attacker to continue the compromise.

> **We also ran an attack path to compromise the domain through Kerberoasting, a common method that abuses service tickets on the network authentication protocol Kerberos, and reuses them to gain access to the targeted service.**

Once authenticated to the domain, the attacker could then use their Kerberos access to request tickets for specific resources on the domain, using the GetUserSPNs.py tool. This enabled the attacker to comfortably retrieve the cleartext passwords for the Administrator, BackupExec SRV_SQLSRV accounts in an offline brute force attack.



Part 4:

Fighting back against the attackers

A commonly held assumption is that attackers have the upper hand as they only need to get lucky once, whereas the defenders have to remain lucky all the time to prevent them. But by looking for clues in the right places, the defenders can exploit the assymetric advantage they have through their unique knowledge of their own environments, and therefore also only have to get lucky once.

To invert this common asymmetry we spread the net as wide as makes sense, and use a range of logs that alert us to specific kinds of behaviour or activity that could be clues or early indicators of unauthorised access to systems. We won't detect all the signs in attempts at a breach all the time, we only need to detect a single sign of a breach to trigger a threat hunt or incident response.

Judicious use of diverse log sources allows us to detect activity at various stages of the attacker's 'kill chain.' We have only to detect activity at a single stage to discern that something untoward is taking place. While we weren't able to detect everything the attackers did inside our network, our goal is to detect that an attacker is present and active, and be able to respond.

For example, the email-based attack described in the previous section exploited Office DDE, which isn't permitted on our system. We were able to detect a change in the registry our administrators made to enable the attack, which offered a first clue that a machine was being targeted. This activity was not in itself malicious, but it is a high fidelity indicator that something untoward is happening.

We could also reliably detect that the machine was attempting to 'talk out' to a suspicious external source. We could detect the use of PowerShell to communicate with the command and control system and easily identify much of the lateral-movement activity, including port-scans, brute force attacks and the use of Mimikatz techniques and other common tools.

Detection of Kerberoasting, meanwhile, is not an easy task as it could generate many false positives within the organisation due to the legitimate use of service tickets. However, this can be decreased significantly by implementing specific filters and discarding other benign requests.

Finally, we were able to detect attempted access to 'canary' user accounts, documents and folders specifically created to lure and unmask attackers – another clear and clean indicator that someone or something is up to no good.

Our blue and red teams both concluded that the attack was successful, but was detected in multiple places, successfully tracked, and could have been subverted if we had so chosen.

> **The email-based attack exploited Office DDE, which isn't permitted on our system. We were able to detect a change in the registry, which offered a first clue that a machine was being targeted and something untoward was happening.**

Part 5:

How we find and fight the bad guys

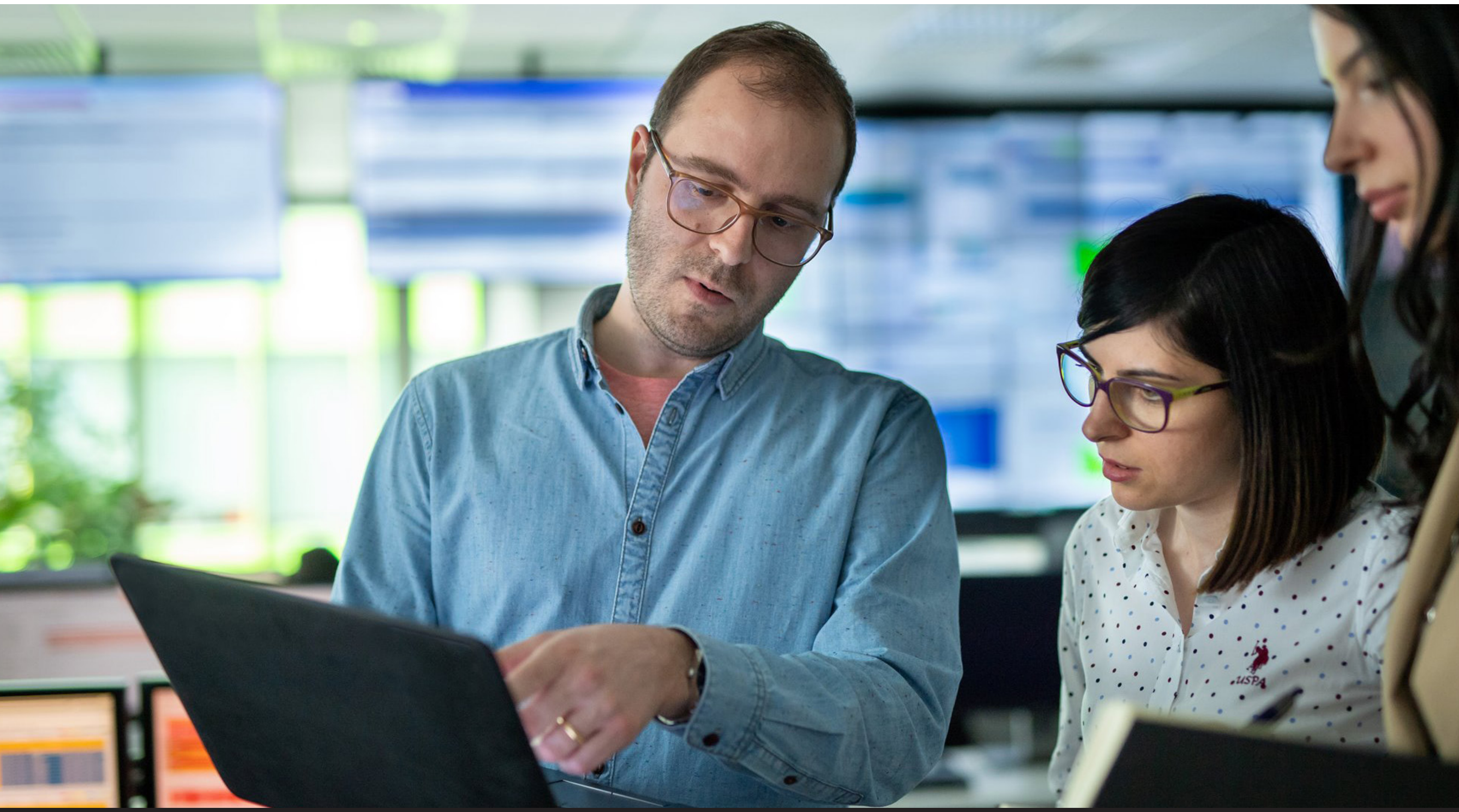
Modern cybersecurity operations and threat detection involves ingesting, processing and understanding a huge amount of information from diverse sources. This vast array of data points is used by security teams to make real-time decisions on how to deploy time and resource, and the wrong decision could leave the organisation critically exposed to a potential breach.

At Orange cyberdefense, we combine a deep view of customers' day-to-day network behaviour with continuous research on threats and vulnerabilities developing in the outside world and a thorough understanding of attacker tactics to build a comprehensive picture of their real-time security posture. We're able to sift through millions of security logs in real-time, transforming data into events that warrant further investigation to uncover malicious activity that could truly cause damage to businesses.

Our Managed Threat Hunting service helps businesses perform preemptive, active pursuit of potentially malicious activities within their networks. Businesses also receive immediate alerts on newly discovered vulnerabilities, exploits and attack methods being used in the real world, as well as relevant breaches and other developments, ensuring they're always as prepared as possible to recognise the unthinkable when this happens.

The service offers deep, far-reaching visibility of a series of events that, when stitched together, provide indicators of an active attack or potential compromise. This is drawn from a continuous stream of data through network and security devices and open-source and proprietary threat intelligence sources and proprietary knowledge gained during penetration tests. That's in addition to our ongoing research into the evolving threat landscape and the latest insight into tactics and techniques being utilised by cybercriminals and other malicious actors. This high level of threat and vulnerability intelligence provides the insight required to make important security decisions.

We deploy a team of skilled security analysts, ethical hackers and responders, who are tasked with understanding the signs of compromise and guiding the customer through response and mitigation. We assess the criticality, urgency and relevance of any potential threat and report what we see in easily consumed reports that are free of jargon and highlight any actions the business needs to take.



Part 6:

How we can help

Our approach to protecting your data and helping you understand the threats facing your business is three-fold. SensePost is our specialist 'offensive' team charged with rigorously testing the robustness of businesses' security defences, while Orange cyberdefense MTD offers Managed Threat Detection and Orange cyberdefense Labs is our specialised research unit.

The former boxing heavyweight champion of the world Mike Tyson famously said: "Everybody has a plan until they get punched in the face." We like to think that punching people in the cyber face is something that our SensePost research and penetration testing team does for a living.

Not only can we provide you with a deep understanding of the cybercriminal mindset, we can also expose your business to as close to a real-world attack as possible without causing actual damage – in exactly the same way we exposed our own systems and processes in the attack outlined previously. You'll uncover some pretty scary things, but can rest assured that we've discovered the vulnerabilities before the real bad guys could.

Our approach is fundamentally research-led, which is where our Orange cyberdefense Labs Team ensure we're always on top of the latest trends, threats and vulnerabilities facing businesses. We're constantly observing what's happening in the market by processing over 25 billion events per month, which provides unparalleled access to current and emerging threats. Using that information, we're able to help our customers evolve their defences, understand the cybercriminals' minds and drive change internally.

While the SensePost 'red team' provides the cybercriminal insight, the Orange cyberdefense team offers 25 years of expertise delivering managed services to some of the world's largest companies. We look beyond the technology to address cybersecurity as a whole, offering a range of integrated solutions that assess the risks, detect the threats and protect your assets.

We offer 24x7x365 monitoring and protection of your systems and data, as well as an around-the-clock hotline and on-site expert help. In addition to providing the expertise to understand how to prevent an attack and improve your defences, we'll also provide insight into what's been affected and ensure you limit damage, control costs and reduce recovery time should an attack occur.

We trust our customers to make sound choices that support their business goals, and believe they will trust us more if we are honest and transparent with them. If you'd like us to help you gain attack insights that will improve your defences, reduce your security risk and better understand the techniques of sophisticated attackers and common criminals, we'd love to help.

Why Orange Cyberdefense?

Orange Cyberdefense is the expert cybersecurity business unit of the Orange Group, providing managed security, managed threat detection & response services to organizations around the globe. As Europe's go-to security provider, we strive to protect freedom and build a safer digital society.

We are threat research, intelligence-driven, offering unparalleled access to current and emerging threats. With a 25+ year track record in information security, 250+ researchers & analysts and 16 SOCs distributed across the world and sales and services support in 160 countries, we can offer global protection with local expertise and support our customers throughout the entire threat lifecycle.

We embed security into Orange Business Services solutions for multinationals worldwide. We believe strongly that technology alone is not a solution. It is the expertise and experience of our people that enable our deep understanding of the landscape in which we operate. It is our people that make us different.

We are proud of our high-end security research unit, thanks to which we publish regularly white papers, articles and tools on cybersecurity which are widely recognised and used throughout the industry and featured at industry conferences including, Infosec, Manchester DTX, RSA, BlackHat and DefCon.

Orange
Cyberdefense

orange™