Threat intelligence

Detect, investigate and respond to cyberthreats more effectively

Orange
Cyberdefense

Increase your visibility into cyberthreats

Threat intelligence is indispensable in understanding and managing business risk in a connected world. It powers detection through data relationships, enables patch management and ensures ongoing monitoring of your digital assets. Threat intelligence also provides insights into nascent threats and cybercrime to help defend your organization and improve overall security.

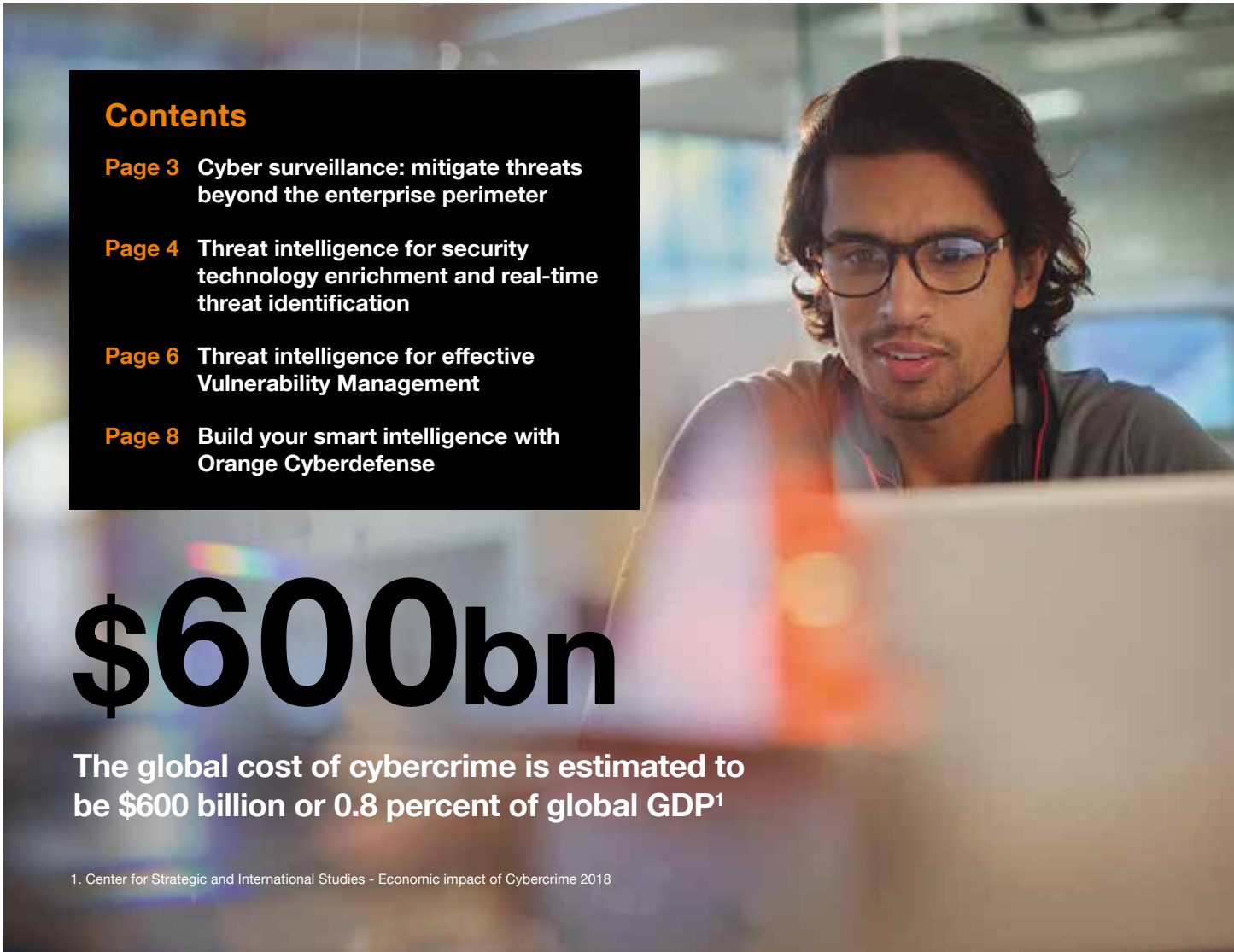
The growth of digital business and the scale of the internet is making it harder to defend yourself against multiple threats, while making it easier for cybercriminals to hide. In addition, the decreasing cost of technology and tools is making it far cheaper to launch sophisticated cyberattacks. This is leaving security teams struggling to sift through gargantuan amounts of data to identify damaging incidents, while at the same time avoiding being led down time-wasting trails of false positives.

By utilizing threat intelligence that pinpoints Indicators of Compromise (IoC) you get a clearer picture of the threat landscape. This increases accuracy in qualifying alerts that could indicate an attack. Threat intelligence gives you both a 360-degree view of your IT estate and a window on what is happening outside its perimeter.

Anticipation and knowledge – the keys to threat intelligence – didn't exist in cybersecurity strategies a few years ago: now they rank as a primary function. Orange Cyberdefense can help you accurately track the latest threats and vulnerabilities, so you can deploy the right protective and corrective measures to keep your organization as safe as possible.

Read on to find out more about our threat intelligence services and expertise.

Contents



Cyber surveillance: mitigate threats beyond the enterprise perimeter

Protecting your brand and intellectual property in the digital world is paramount. Orange Cyberdefense's Cyber Surveillance Services manage threats outside your organization's perimeter by continuously monitoring the internet, deep and dark web for digital fraud and data leaks.

Brand abuse by malevolent actors is at epidemic level in the digital world, destroying reputations and denting bottom lines. The impact can be enormous, from legal action and regulatory fines to damaged customer loyalty. The techniques used by attackers change as fast as the attack landscape and most threats come from organized and sophisticated cybercriminal networks with global reach.

In addition, many scenarios have resulted in the unwanted dissemination of information on the internet from using data sharing apps in cloud mode, distribution of a compromised website database, data mistakenly published by an employee and so forth.

Orange Cyberdefense continuously monitors the internet, visible web and deep dark web to identify and remediate beyond the enterprise perimeter. Cyber surveillance includes data leakage and stolen data monitoring, fraud monitoring, reputation monitoring and mobile app monitoring.

Our fraud monitoring service helps detect newly created suspicious domain names, fraudulent websites, phishing campaigns against customer brands, fraudulent profiles on social networks or any fraudulent usage of the brand or trademark. It takes a median time of around four hours to close a fraudulent site and we currently take down around 20,000 rogue websites each year.

The Orange advantage

- Orange Cyberdefense's services include in-depth qualification by multilingual experts, who are available 24/7/365 following the sun. They monitor more than 10,000 brands.
- Our proprietary, hidden web crawlers and bots specialize in analyzing huge numbers of pages on the open internet, the deep web and the dark web seeking out potential threats against your organization's brand and IP addresses.
- Our in-house Customer Emergency Response Team (CERT) is recognized as the top European private CERT. It has relationships with 20 law enforcement agencies across multiple continents including the FBI, Interpol and Europol.
- Our CERT can undertake in-depth cybercriminality investigations tailored to specific sectors and other bespoke monitoring as required.

The dark web

The dark web is a small part of the world wide web, which is hidden and inaccessible through standard web browsers. It doesn't take part in the DNS system, so can't be crawled by traditional web crawlers or indexed by search engines. This inherent anonymity makes it a breeding ground for illegal activities such as selling stolen intellectual property (IP), sensitive company information and customer lists, for example.

146 bn

Data theft to jump 175 percent from 2018 to 2023 – from 12 billion to 146 billion records[2]

2. Juniper Research: The Future of cybercrime and security 2018

Threat intelligence for security technology enrichment and real-time threat identification

Orange Cyberdefense's proprietary threat intelligence database is an essential part of our threat management portfolio. To build a comprehensive real-time picture of all threats facing enterprises, we collect information from public and private sources worldwide. Additionally, as a network operator, we have the advantage of visibility at the first signs of attack.

The data in our threat intelligence database is verified and correlated in real time against security logs to minimize false positives and maximize data quality. We look at the entire threat landscape including malware, phishing, ransomware, leaks and cryptohacking. We thoroughly qualify incidents to make sure you don't miss any threats.

Our threat intelligence database contains information on malware identified from over 500 qualified sources. These sources include Orange's tier-1 operator internet backbone, closed and open-source threat intelligence feeds, customers and partners including Europol, the European Union's law enforcement agency, and other CERTs.

The database is enhanced by exclusive direct flows from our Signal Intelligence and Epidemiology Lab, next generation sandbox, network backbone and public email inboxes for advanced persistent threat (APT).

Embedded or as-a-service

The Orange Cyberdefense threat intelligence database is available via our managed solution or as a service.

- **Managed threat detection:** benefit from our embedded proprietary threat intelligence as part of our managed services.
- **Datalake:** if you have an in-house or third-party managed SOC, you will be able to benefit from our unique Datalake threat intelligence-as-a-service comprising actionable threat intelligence and Indicators of Compromise (IoC) feeds.

20k

malware items

analyzed each day by Orange Cyberdefense.

Threat intelligence for security technology enrichment and real-time threat identification

Orange Cyberdefense Datalake: threat intelligence-as-a-service

Orange Cyberdefense Datalake is an intelligence database available via a single easy-to-use web portal that provides you with a one-stop shop for threat intelligence-as-a-service, supported by our team of experts.

The gargantuan volume of data that needs to be tracked to provide threat intelligence is resource-hungry and ongoing. The complexity and burden of aggregating this data is huge. Datalake does this job for you by providing accurate, consistent data sources directly to your organization in an easy-to-consume way. This provides invaluable intelligence for your security teams to act on and saves time and money that would otherwise be wasted chasing down false positives.

Orange Cyberdefense Datalake is hosted at Orange data centers. It is easy to deploy and requires no time-consuming configuration installation, additional skills or capex investment. The web portal can easily integrate with your application programming interfaces (API) and can be adapted to work with your current tools.

> **“With insight into the Orange tier-1 internet backbone and backed up by a team of cyber experts, Datalake provides unmatched threat intelligence on demand.”**

The Orange advantage

Access to Orange’s tier-1 operator internet backbone provides an additional unique and rich intelligence source. Initial signals and emerging threats we see on our internet backbone provides us with early visibility of the first signs of an attack with much shorter lead times.

Orange Cyberdefense uses a powerful co-relation engine and proprietary algorithms to correlate and evaluate data in the cloud.

Our CERT analyst teams further qualify and enrich the Datalake threat intelligence by evaluating the reliability of information and relevance of the indicators.

Our proprietary threat intelligence database is proven to minimize false positives, and used by our own CyberSOC teams to power effective threat detection for our managed detection customers.

Threat intelligence for effective Vulnerability Management

Threat intelligence is central to Vulnerability Management

Keeping up-to-date with vulnerabilities and patching accordingly in your environment is an important part of security housekeeping.

Looking at vulnerability data in isolation, however, limits your ability to safeguard your infrastructure. With the number of vulnerabilities rising, it is impossible for organizations to address every single vulnerability alert.

Our holistic Vulnerability Management service is underpinned by four components: Watch (vulnerability threat intelligence feeds), Detect (vulnerability scan), Ethical Hacking (including penetration testing) and Code Check (technical audit). These services, powered by tools and support from our cyber experts, allow reporting on newly identified vulnerabilities, regular vulnerability scans on networks, systems and applications, and punctual identification of other vulnerabilities in the IT system and applications prior to their release.

By keeping up-to-date with the latest vulnerabilities, you can ensure visibility and effectively remediate gaps in your security before they are exploited by bad actors.

Our solution: vulnerability intelligence

- We provide vulnerability intelligence feeds to help you prioritize actions for vulnerability remediation, and focus resources on what really matters to a proactive defense.
- Each day, our experts collect and analyze relevant information and share contextualized and actionable vulnerability intelligence.
- Our Orange Cyberdefense CERT offers access to real-time vulnerability feeds for more than 4,000 security products.
- Our experts analyzed and qualified more than 3,000 vulnerabilities in 2018.

Malware: a major cyberthreat

Locating and patching vulnerabilities is vital to stop malware spreading in your organization

Malware or malicious software is an umbrella term for malicious programs or code that can invade, damage or disable systems, networks and mobile devices. Malware can be delivered by a variety of mechanisms including phishing campaigns with texts and emails, compromised websites, software and network vulnerabilities and physical media such as USB memory sticks.

The Ponemon Institute[4], for example, estimates that 35 percent of malware attacks last year were fileless and this is increasing. These fileless attacks make it easy for bad actors to conceal themselves in systems undetected, allowing attackers to stay alive in your infrastructure for longer.

Cybercriminals know the techniques that organizations are using to block attacks and are coming up with increasingly clever versions.

4. The Ponemon Institute: State of Endpoint Security 2018

Threat intelligence: malware epidemiology

Malware epidemiology is a key part of threat intelligence, because it prevents malicious software from compromising your organization. This makes our unique Signal Intelligence and Behaviors Lab research capabilities the reason why our intelligence services are so sought after by enterprises globally.

Our team of dedicated cyberscientists study and profile malware in our labs to identify mutations and new strains. This research is fed into our CyberSOC and threat intelligence database. It is a unique enabler that provides advanced intelligence to determine in real time indicators of surveillance to support infrastructures' monitoring.

You will have undoubtedly noticed an alarming increase in the amount of malware attacks on your organization, and it shows no sign of slowing down. Why? Because advanced malware has mastered the art of evasion, making it difficult for traditional security solutions to pick up.

The Orange advantage

We have developed a unique methodology that expands the detection spectrum. By adding relationships or indicators of surveillance to our monitoring capabilities, we can augment our IoC-based processes – allowing for a highly predictive approach.

The intelligence offered by our threat intelligence database benefits from the following market differentiators which customers can access via our managed detection services or stand-alone via Datalake threat intelligence-as-a-service.

- Signal Intelligence and Behaviors Lab Services uses a balance of people, processes and advanced tools, fully supported by our team of experts.
- The Orange Cyberdefense library of threat intelligence indicators enables us to identify an anomaly up to 50 days before publicly published IoCs provided by other sources.
- Our in-house research and development teams are continually innovating to keep ahead of the changing threat landscape.

Advanced approach to stopping malware attacks

1. Studying malware behaviors

We transmit indicators of surveillance to follow malware families via a backbone of incubators for long periods, which allows us to analyze strains for signals via the internet. Malware that is mutating or changing needs external orders from the attacker. These are typically disseminated via vulnerable systems on the internet, which can include IoT and smart devices.

The objective of our research is to map malware families and come up with relationship links between them that will help us identify their characteristics and possible future strains and mutations.

2. Malware profiling

Our experts profile the malware including its domain name, who created it, its IP address, and the bandwidth required to draw up an identikit of the bad actors and the infrastructure being used. We can also spot patterns between different malwares and how they are related. By having a deep understanding of a particular strain of malware we can stop updates and advanced persistent threats.

3. Malware sandboxing

We have also developed our own unique sandbox to analyze malicious malware in our labs. This allows us to run and test malicious code in an isolated environment, understand how it works in the system and allow us to rapidly recognize similar malware. Our hypervisor-based sandbox analyzes thousands of malware a day, including mobile malware, and sees everything that has been altered on a system, from files opened to keys touched.

Build your smart intelligence with Orange Cyberdefense

Orange Cyberdefense, the Orange Group's expert cybersecurity business unit, has extensive experience providing threat intelligence to customers around the world, securing their business, safeguarding critical data and protecting their brand image against cyberattacks and abuse.

Our in-house CERT team and unique threat intelligence enable us to monitor the latest threats and vulnerabilities, so that our customers can rapidly deploy preventative and remediation measures. Our threat intelligence helps customers manage threats outside their infrastructure perimeter, continuously monitoring the internet, along with the deep web and dark web, for malicious activity.

Effective threat management requires coordinated anticipation, detection and response. Threat intelligence now plays a critical role in this ecosystem. With our unique threat intelligence offering we can help you better secure your organization now and into the future against current and emerging threats.

Contact us to find out about threat intelligence from Orange Cyberdefense at https://cyberdefense.orange.com/en/

Why Orange Cyberdefense

- **Unique proprietary threat intelligence database that maps cyberthreats in real time**
- **Analyze over 30 billion security events every day via our managed detection and reaction solutions**
- **Threat intelligence automated decision support tools**
- **Access to 500 plus public and private intelligence sources**
- **18 years of experience in cybercrime and forensics with a strong knowledge of hacker communities and communication channels**
- **Over 200 cybersecurity experts working on innovations at Orange Labs, an Orange R&D entity**
- **1,500 plus Orange Cyberdefense experts delivering 24/7 services across the globe**
- **In-house team of ethical hackers from Orange Cyberdefense and assistance from SecureData Group and its subsidiary SensePost, now part of the Orange Group**

Orange
Cyberdefense