

Managed Threat Detection Intelligence

Getting ahead of the attack through smart visibility

Orange Cyberdefense helps organisations identify and manage their digital risk.

Comprehensively covering Open, Deep and Dark Web sources Orange Cyberdefense identifies potential cyber threats and breaches, as well as monitoring customer owned digital assets for brand, data and infrastructure exposure.

Providing targeted threat intelligence as a service

Threat intelligence is a broad term that can carry many meanings in the field of cyber security. The Managed Threat Detection Intelligence service, rather than focusing on technical threat intelligence and feeds of known IOCs, looks to provide a broader, more business-focused threat intelligence including:

- Operational threat intelligence, looking at identifying attacks or potential security incidents across the open web, as well as closed sources
- Tactical threat intelligence around common tactics, techniques and procedures (TTPs) used by adversaries, with a focus on customer-specific industry or systems
- Strategic threat intelligence, collected and distributed by our cyber defence center (CDC) and incident response (CSIRT) teams

Many companies already undertake these activities in their traditional “internal” networks but as digital transformation has become a global initiative for businesses of all shapes and sizes, managing digital risks outside of that traditional infrastructure has never been more important.

Looking at the latest trends, threats and digital risks and assessing the impact on our customers, their peers and their key 3rd party partnerships.

The primary goal of targeted threat intelligence should be to provide further context to security operations center (SOC) activities being undertaken already by an organisation such as security information and event management (SIEM) or vulnerability management.

Expertise in cyber threat intelligence

- 10 Cyber SOCs across the globe
- Over a quarter of a million security events processed in 2019
- Strategic partnership with Digital Shadows and their market-leading SearchLight™ platform
- CREST certified computer security incident response team (CSIRT) operating internationally with vast experience including military intelligence services
- Dedicated research team tracking threats, trends and adversaries continuously
- Cyber security advisory practice, aligned to customer’s digital risk management programmes

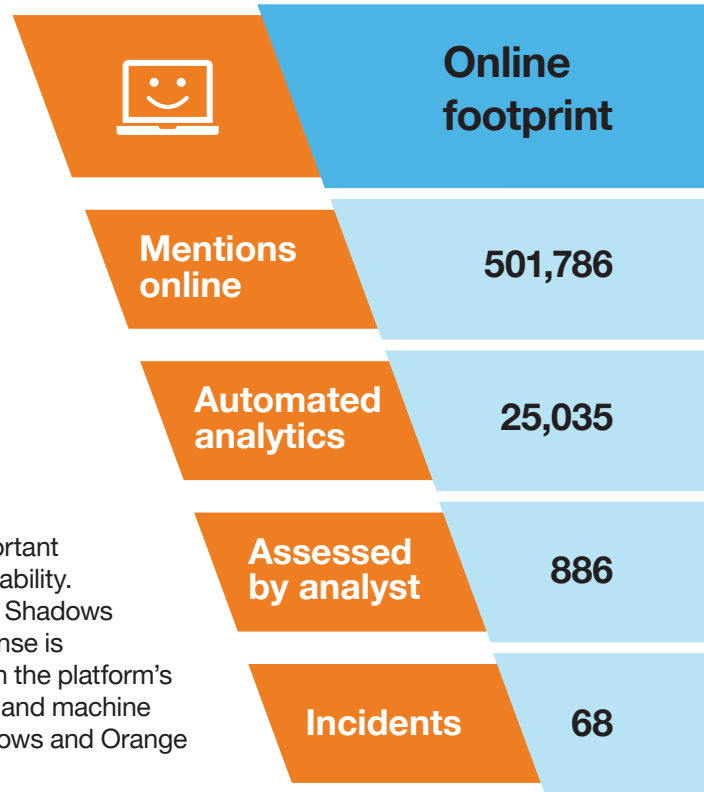


Managed Threat Detection Intelligence

The Managed Threat Detection Intelligence service (powered by Digital Shadows) enables you to minimise your digital risk by detecting data loss, securing your online brand, and reducing your attack surface.

An extension of your team

Whilst techniques such as natural language processing allow us to conduct a certain amount of automated analytics, the two most important facets of providing targeted threat intelligence are context and actionability. To get real value out of the targeted threat intelligence that the Digital Shadows SearchLight™ platform provides, human analysis and incident response is required. The Managed Threat Detection Intelligence service wraps in the platform's broad coverage of sources and the latest techniques in data science and machine learning, with industry leading intelligence analysts from Digital Shadows and Orange Cyberdefenses computer security incident response team (CSIRT).



Benefits:

- Search across open, deep & dark web
- Save queries and receive alerts
- Access threat intelligence feeds
- Search across bulk WHOIS information
- Access threat actor profiles
- Identify exposed credentials
- Identify exposed sensitive documents
- Identify exposed intellectual property
- Identify spoof domains
- Identify spoof social media profiles
- Identify spoof mobile applications
- Identify open ports
- Identify exploitable vulnerabilities
- Identify weak or expiring certificates
- Perform takedowns

an **Orange Cyberdefense** service powered by **digital shadows**

