Orange Cyberdefense

The Orange Cyberdefense
CSIRT

Be prepared: incident response services

The Orange Cyberdefense cybersecurity incident response team (CSIRT) is an elite European team that provides proactive consulting, incident response and technical advice to help customers handle a security incident from initial detection to closure and recovery.

Focus of attention

Media reports of large data breaches used to be few and far between, hidden away inside the pages of the tech section of the news, or dedicated industry news sources. The reality now is that breaches are mainstream news, adding a PR-nightmare on top of the actual damage.

The key to mitigating the impact of any cybersecurity incident, is the reaction time between detection and response. Many companies lack the infrastructure, processes and people needed to react in a quick and secure manner. Incident response services from Orange Cyberdefense enable any company to call on our CSIRT as an extension of their security operations team. Our team is on-demand 24x7, allowing you to complement existing resources with experienced, multi-skilled specialists in digital forensics and incident response to help safeguard your business.

About the Orange Cyberdefense CSIRT:

- Part of Orange Cyberdefense CERT, with an extended team of 80+ people globally
- Large, multi-skilled CSIRT team with 20+ responders in Western, Northern and Central Europe
- Members of industry-recognised bodies for Incident Response including CREST, TF-CSIRT, FIRST and ENISA
- Highly experienced team including experience in handling nation state level attacks
- Analyst recognition including Gartner* and Forrester**

We will help you manage an entire incident, from a simple breach of policy to an estate-wide compromise working as a key part of your organisation's incident response plan and as a colleague within your own incident response team. The CSIRT follows the principles of the 'Association of Chief Police Officers' (ACPO) Good Practice Guide for Computer-based Electronic Evidence' for all aspects of evidence management, regardless of criminal circumstances or law enforcement agency involvement.

* Representative Vendor, Gartner Market Guide for Digital Forensics and Incident Response Services, December 2019
** Forrester NowTech report for European Cybersecurity Incident Response Services, Q1 2020

Once a breach is detected, it is vitally important to know how to respond. You typically require:

Expertise

Experience and skills make an impact especially in response to critical cybersecurity incidents. The CSIRT continuously refines and updates their methodologies and techniques. This allows our teams to handle security incidents with confidence and in an efficient manner. Using our combined knowledge to help customers identify, contain, eradicate and recover from a range of incidents.

Reliability

With ever increasing regulations such as GDPR and the emerging market of cybersecurity insurance, requiring assessment and reporting of incidents faster than ever before, a solid partner who can deliver on providing the expertise required time after time is crucial. In what is often most companies' greatest hour of need, you require someone you can trust.

Preparation

Pro-active services help you to plan, prepare, train and test your people, processes and technology so that when incidents do happen, the organisation is ready and confident, with tried and tested methodologies used to manage the response. The Orange Cyberdefense CSIRT helps you be as prepared as you possibly can be. We know what works and - more importantly - what doesn't.

Find your country's Incident Reponse Hotline on www.orangecyberdefense.com/global/csirt/

Find out more about our response services:
orangecyberdefense.com/global/response/

Benefits:

- Delivers high quality incident response when you need it (on-demand or on a retainer basis).
- Develops your internal skills, documentation and processes to allow you to be ready for a broad array of incidents.
- Get access to specialist skills across many different disciplines, with one of the largest CSIRT teams in Europe as well as access to the wider CERT team, all underpinned by our Intelligence-led security approach.
- Access to an adaptable, customer-centric team that passionately believe in what they do.

Working with us

Our CSIRT provides all of the key components for a world class incident response function:

Technical Experience

It is important to have experienced responders who are comfortable and confident in dealing with what are often high pressure situations. Orange Cyberdefense's CSIRT members have worked with some of the world's largest enterprises and responded to some of the most devastating and high profile cyber-attacks of recent years, including Petya and WannaCry.

Knowledge

Orange Cyberdefense know your business. Our incident response retainer services include an on-boarding risk assessment workshop to ensure our team have a detailed overview of the current position, to gain maximum insight before a response is required.

Intelligence-led Incident Response

We collect Indicators of Compromise (IOCs) from the Orange Cyberdefense Threat Intelligence backbone. Our CSIRT is closely linked to the rest of the CERT (including our Cybercrime Monitoring team) and our network of SOCs and CyberSOCs. The intelligence flowing into and out of the CSIRT fully utilises the cyber threat intelligence we have at our disposal, allowing us to better advise on preparing for future incidents and to provide focused context around an incident.

Containment

With outbreaks of ransomware and other malicious malware threatening industries of all types, containment is vital. The CSIRT team has built an incident response toolkit across years of IR work, that continuously evolves to ensure that if your defences have been breached, the threat is contained quickly, the source is identified and damage is limited to a minimum.

A pro-active approach

It is important to not wait for a cybersecurity incident to happen. Practice makes perfect and assurance is key. The Orange Cyberdefense CSIRT delivers services to prepare for the worst - from incident response consulting engagements such as incident reponse plan development and tabletop exercises, to compromise assessments that proactively look for signs of intrusion that are previously undiscovered.

Retainer

It is important that you have a guarantee of quality skills when you need them most; preparation is key. The Orange Cyberdefense CSIRT are available on retainer basis 24x7, 365 days a year with a guaranteed remote and responder to site SLA. Our retainer services are designed so that unused retained hours can be utilised for pro-active work such as testing, training and process review.*

*Depending on service level purchased.