Orange Cyberdefense

The Orange Cyberdefense
CSIRT

Be prepared: emergency recovery services

The cyber security incident response team (CSIRT) is an elite pan-european team in Orange Cyberdefense that provides emergency consulting, incident management and technical advice to help customers handle a security incident from initial detection to closure and full 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 IT security incident, is the reaction time between detection and response. Many companies lack the infrastructure needed to react in a quick and secure manner. SecureRespond services by Orange Cyberdefense allow any company to react 24/7 to malicious cyber threats. We enable customers to complement existing resources with world class expertise, to safeguard their business.

The Orange Cyberdefense CSIRT

The Orange Cyberdefense CSIRT is an Pan-European team within Orange Cyberdefense Group, Europe's largest independent cybersecurity and Managed Security Service provider. The CSIRT can be deployed to provide expert consulting, incident management and technical advice to help you handle a security incident end-to-end from the initial detection to closure.

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.

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. Orange Cyberdefense's CSIRT continuously refine and update our methodologies and techniques. This allows our teams to handle security incidents with confidence and in an efficient manner. Using our combined knowledge to identify, contain, eradicate and recover from a range 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, in tried and tested methodologies used to manage the response.

Hotline:
+46 40 668 81 88

Find out more about our response services:
orangecyberdefense.com/se/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
- Incorporates a vast wealth of experience, cyber threat intelligence and a passion for quality service and customer satisfaction

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 times, 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

We collect Indicators of Compromise (IOCs) from every incident response engagement. Orange Cyberdefense have access to global threat intelligence from commercial and open sources, and our CSIRT team are closely linked to the Orange Cyberdefense Cyber Defense Centre (CDC). The two-way sharing of information between the CSIRT and CDC, 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 or series of incidents.

Containment

With outbreaks of ransomware and other malicious malware threatening industries of all types, containment is vital. With Orange Cyberdefense's strong partnership with leading threat detection and containment product vendors alongside a combination of in-house and commercial toolsets honed across years of IR work, we look to ensure that if your defences have been breached, the threat is prevented from escalation and damage is limited to a minimum.

Qualifications

All personnel working on incident response activities are certified to the CREST Registered Intrusion Analyst level at a minimum or equivalent certification/ experience. Experience and skill-sets, backed up by internationally recognised standards and methodologies (including a CREST certified methodology) give you the assurance that you are in good hands.

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.

Build a safer digital society

Orange Cyberdefense helps companies secure their activities and data. We provide integrated solutions that assess risks, detect threats, protect our customers' IT assets and respond to security incidents.

Working in cyberdefense means being part of an industry that is constantly evolving: what is true today can become obsolete tomorrow. To face this challenge, Orange Cyberdefense invests in its own research labs. Our goal: finding answers to emerging issues and developing our own expertise.

This mission requires the contribution of every member in our field. Orange Cyberdefense, as the industry leader in cybersecurity in Europe, is proud to be at the heart of this ecosystem.

For more information check
https://orangecyberdefense.se

Orange Cyberdefense
Stenbärsgatan 6, 212 31 Malmö

info@se.orangecyberdefense.com
+46 10 202 20 13