fast track

CyberSOC: the human side of security

Security is not all about deploying the right technology. People and processes are vital in identifying and preventing modern sophisticated security threats from disrupting your business.

How to protect your business from IT security threats has changed over the past decade. Previously, if you put the right security devices and processes in place and kept everything patched, you could prevent the bulk of attacks. However, with the increase of targeted attacks and newer, sophisticated attacks, a technology-led approach is no longer enough.

Data exfiltration is often the target. For example, a user could go to an infected site and introduce malware, which targets confidential enterprise information, such as R&D results, the customer database or intellectual property. And, of course, threats don't just come from external sources; for example, an employee might download confidential documents in order to harm the organization, if they are about to be let go.

The CyberSOC can help you address these challenges by introducing a human element to your security. It manages risk across the business via a cycle of monitor, assess, advise and remediate. The CyberSOC is staffed with skilled security event analysts and offers incident handling, alert warning, risk analysis and business impact assessment.

Business Services

orange™

1. security is not just about technology: you need organization, skills and processes

To protect yourself from targeted attacks, you need to look beyond technology. The CyberSOC provides the people, skills and organization to identify anomalies and threats. For example, in the disgruntled employee example, you can protect yourself by matching downloads to the human resources database. This allows you to spot unusual patterns and calculate the risk to the business.

2. CyberSOC is a complement to the SOC, not a replacement

The CyberSOC complements the work of a security operations center (SOC), which manages the security infrastructure from a "technology standpoint." The SOC is staffed by security product specialists and offers services such as release management, configuration management and signature updates.

3. involve the business from the start

Remember that ensuring security is a business issue, not an IT project. The CyberSOC is essential in coordinating the involvement of the business in security right from the start. This is an ongoing process through all refinements of the security strategy to ensure that it still meets the objectives of the business.

4. work out your business objectives and how to achieve them

The CyberSOC can help analyze the risks to your business and determine what type of threats are likely. Different types of businesses have different requirements and risks. For example, a manufacturer's priority is to ensure that its intellectual property is not stolen, while an e-commerce company will be more concerned about the uptime of its customer-facing site.

5. focus on the resource that you're protecting

Don't only focus on how the attack will happen, focus also on the resource that you're protecting. The CyberSOC will work out what kind of actions could signal a problem, such as a large number of requests from one IP address, or port scanning. A combination of several suspicious activities can signal a potential problem that will need action.

to find out more about implementing CyberSOC-related services, contact your local account team or visit us at **www.orange-business.com**

6. gain skilled insight with the Orange CyberSOC

The CyberSOC is a good match for a specialist security service provider because it requires in-demand skills and must be operational 24/7. In addition, a specialist security provider can share CyberSOC insight across multiple customers, which is particularly useful in identifying any wider attacks or trends.

7. deploy a CyberSOC step by step so that you can achieve measurable results quickly

We provide four CyberSOC-related services to help meet your business objectives. Expand the scope of each service gradually, rather than trying to achieve everything with a "big bang" project.

our solution

- active prevention: monitor your infrastructure for intrusion, identify malicious traffic, alert for suspicious activity
- DDoS protection: prevent hackers from flooding your network or IT with traffic to take down your website or any other application
- cyber risk and compliance intelligence: audit servers to see if they are vulnerable, provide advice on actions, such as patching servers or turning service off
- security event intelligence: consolidate information from various equipment into one place to spot patterns and identify malicious activities

Business Services

orange™