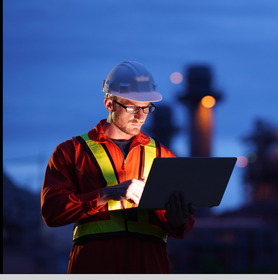
Cyberdefense

# Making Sense of Operational Technology Attacks



Over the past few decades, there has been a growing awareness of the need for improved cyber security practices in IT's lesser-known counterpart, Operational Technology (OT).
The increasing digitalization of industrial processes has made the security of OT a major challenge, and cybersecurity is a key enabler to success.

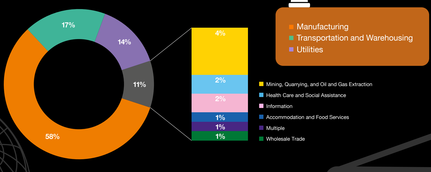
OT encompasses the systems and networks responsible for managing, monitoring, and controlling industrial equipment and physical processes. In this context, the security of OT devices has emerged as a paramount concern to avert service disruptions, safeguard against attacks compromising physical infrastructure integrity, and ensure the protection of critical data.

At Orange Cyberdefense, we are committed to offering advanced cybersecurity solutions, designed to defend OT systems against emerging threats and strengthen their resilience in an ever-changing digital landscape.
Let's dive into some figures from the Security Navigator 2024 regarding OT security and identify the key aspects of these systems.

## An integrated security strategy

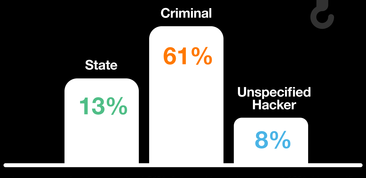
### Victims by sectors

**Proportion of victims of OT attacks by industry sector**




### Adversaries

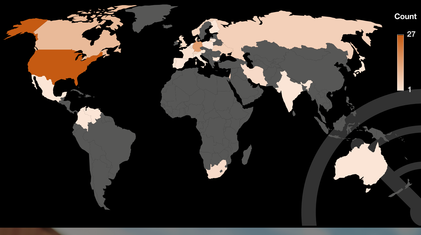
**Proportion of different types of threat actors (over time and in total)**




Criminal actors account for the majority at 61%, followed by state actors at 13%. Unspecified hackers and insiders each account for 8% of the total. Hacktivists make up 6% of threats, while contractual third parties and unknown actors each account for 2% of reported incidents.

### Geographic distribution of the victims

The geographic distribution of OT victims is quite broad. The USA saw the most victims with 23% of incidents. Russia also scores as the 6th most targeted country with 4% of incidents; its prominence is due to 4 hacktivist attacks shortly after their invasion of Ukraine in 2022. Germany saw 12% of attacks, and therefore enters the list of most impacted countries.




## Key recommendations

**1 Regular Security Assessments**
For now, our report shows that there are almost no sophisticated attacks specifically targeting OT. Instead, criminals overwhelmingly target IT assets. Implement periodic security assessments to identify vulnerabilities within the OT environment, especially when IT assets are connected to OT.

**2 Segmentation and Network Management**
Enhance network security by segmenting OT from IT networks, minimizing the risk of crossover attacks. Employ robust firewalls, intrusion detection systems, and strict access controls to regulate traffic and monitor network activity.

**3 Continuous Monitoring and Incident Response**
Develop a robust monitoring system that provides real-time insights into OT systems. Establish a dedicated incident response team trained specifically for OT scenarios to respond swiftly to any security breaches, minimizing potential damages.

## How Orange Cyberdefense can help

**Setting the right priorities for you is business-critical for us**

**Understand your environment**
Extending your security program to OT environments starts with understanding your assets, networks, threat landscape and attack surface.

**Protect your networks and assets**
Increasing connectivity of IT and OT requires secure network design and segmentation to protect and access assets in your network.

**Detect complex threats**
Detecting complex threats in increasingly connected IT and OT environments requires integrated threat detection capabilities.

**Prepare for security incidents**
Being prepared for security incidents gives you the best chance of minimizing the impact.

## Talk to an expert

To secure your Operational Technology systems, our team at Orange Cyberdefense is available to help you assess and strengthen the security of your critical infrastructures.

Contact us to find out how our customized solutions can effectively protect your business against current and future threats.

Take the first step towards robust IoT security.

**Contact us today**

## Sources

All data comes from the Security Navigator.
Click to see the full document.