# IT/OT Threat Hunting Services

**When it comes to ensuring operational integrity, no organization is 100% immune to cyber attacks. Once a breach is identified, the damage might be irreversible. OTORIO offers a proactive, Threat Hunting service to ensure that the customer network is clean from cyber threats.**

Many companies are not aware of attackers lurking in their OT and IT networks. In some cases, attackers were able to propagate through a victim network undiscovered for months. OTORIO has been partnering with many industrial companies on their path to identify and stop threats before they are carried out.

Threat hunting is a short term, proactive approach that looks for dormant malware and malicious activity in your OT network. If suspicious activity is identified, it quickly escalates to an incident response to mitigate the risk.

## Industrial Threat Hunting

Our threat hunting team identifies security gaps and deficiencies and later helps in the remediation process, thereby minimizing the chance of future incidents. Our tailor-made hunting is based on the customer's specific network and critical assets, thereby defending its trademark secrets and operations before anything happens to them.

Our team conducts state-of-the-art Threat Hunting in OT environments. We are equipped with the top signatures of the most recent OT related malware. Our unique approach of data acquisition and pre-prepared machine learning analytics protects your company from the next attack.

## Benefits

- **Conducts tailor-made threat hunting**
  We look at your network and critical assets and partner with you to defend your trademark secrets and operations.

- **Checks your external attack surfaces**
  We verify that your company's external attack surfaces are reasonably protected and updated.

- **Identifies existing threats**
  We make sure no threat actors or malware are currently in your network. If we identify a threat, we provide mitigation steps. We map all internet facing services without triggering any alerts by your SOC or blue teams.

- **Provides an automatic passive reconnaissance service**
  You receive a list of services connected to your company, prioritized based on ease of discovery, the complexity of the service's exploitation, and the severity of the potential impact. This runs with zero impact on the services themselves and requires no preparation by the customer's IT team.

## Proactive Threat Hunting

Launching a remote or on-prem hunting team marks security deficiencies and finds artifacts left by malicious activity.

With threat hunting, you can identify threats and vulnerabilities before they happen. We identify security gaps and deficiencies and then offer remediation assistance. You can maintain your vigilance against security breaches and improve your overall security posture. This minimizes the chances of future incidents.

## OTORIO - Industrial-native cyber and digital risk-management solutions provider

OTORIO combines the professional experience of top nation-state cyber-security experts with cutting edge digital risk-management technologies to provide the highest level of protection for the manufacturing industry. OTORIO's automated Digital Risk-based Maintenance solution aggregates threat data analysis to provide deep insights into industrial control systems, identifying risks and mitigating them before they can cause damage.

Our cyber experts work closely with our customers' cyber and operational teams to tailor solutions that address their specific industrial digital security needs, according to their level of digital maturity. OTORIO empowers industrial companies to implement, automate, and operate secure production, making way for a safer, more reliable and productive industry.