The increasing importance of communication technologies across different industries has driven a growing integration of digital features that support the control and maintenance of physical processes. This intersection of the virtual and the physical has led to not only revolutionary connectivity and instrumentation, but also to significant safety and security risks.

It is becoming more important to proactively learn and share technical vulnerabilities and viable threat actor tactics, techniques and procedures (TTPs), so that cyber physical attacks can be anticipated and prevented.

FireEye Cyber Physical Threat Intelligence is a subscription service that provides context, data and actionable analysis around threats to cyber-physical systems, including operational technology, industrial control systems, Internet of Things and other equipment used to support physical processes in, for example, the telecommunication and medical sectors.

**What Your Subscription Offers**
For organizations tasked with maintaining the security and continuity of these systems, Cyber Physical Intelligence provides early warning on critical vulnerabilities, as well as the threat campaigns and adversaries targeting them. With Cyber Physical Intelligence, security teams can stay ahead of attackers and make better-informed decisions about the security posture of their cyber physical systems.

The Cyber Physical Intelligence subscription includes in-depth reporting on cyber physical-focused malware and malicious tactics, techniques and procedures, threat actors, threat activity, vulnerabilities and strategic insights. Table 1 lists the critical coverage areas where FireEye provides in-depth intelligence for teams tasked with defending these systems.
Table 1. Coverage areas of FireEye Cyber Physical Threat Intelligence.

<table>
<thead>
<tr>
<th>Coverage Area</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current Intelligence</td>
<td>Tactical and strategic analysis of threat activity, derived from FireEye Mandiant engagements, deployed FireEye technology and extensive network of FireEye sensors deployed worldwide.</td>
</tr>
<tr>
<td>Cyber Physical Reference</td>
<td>Review of terminology, network architecture, ICS ports and protocol security and cyber physical-focused threat actors.</td>
</tr>
<tr>
<td>Cyber Physical Vulnerabilities</td>
<td>Tactical reporting on ICS vulnerabilities.</td>
</tr>
<tr>
<td>ICS Network Activity</td>
<td>Analysis of network traffic on ICS ports based on firewall logs data.</td>
</tr>
<tr>
<td>ICS Security Roundup</td>
<td>Collection, analysis and implications of ICS publications in media.</td>
</tr>
<tr>
<td>FireEye Mandiant-Sourced</td>
<td>Ongoing review of Mandiant engagements that examines trending data and security best practices.</td>
</tr>
<tr>
<td>Tools and Research</td>
<td>Research and analysis of ICS-focused reconnaissance and attack tools.</td>
</tr>
</tbody>
</table>

Stay Ahead of the Next Generation of Threats

Cyber physical systems come with a complex set of benefits and risks. To anticipate and block threats that target cyber physical systems, you must maintain current information on the unique security requirements of these technologies:

- Increase awareness of relevant cyber physical security vulnerabilities and support vulnerability management efforts through FireEye vulnerability scoring and analysis of remediation options.
- Gain situational awareness of threats, campaigns and actors targeting your cyber physical systems.
- Educate your internal teams and external stakeholders with in-depth reference material and topical event coverage tailored to the cyber physical world.
- Make better-informed decisions about your evolving cyber physical security program and controls.
- Get actionable intelligence to help evolve your cyber physical risk management posture from reactive to proactive.

For more information about how FireEye Cyber Physical Intelligence can help your security team make better-informed security decisions, [www.FireEye.com](http://www.FireEye.com)