

# OT-based Security Incident Handling Toolkit

Listed below are some of the tools that help incident handlers in responding to OT-based security incidents.

OT-based Security Incident Handling Tools	
Category	Tools
OT Incident Management Tools	<ul style="list-style-type: none"><li>Operational Technology Management (<a href="https://www.servicenow.com">https://www.servicenow.com</a>)</li><li>ETAP ADMS (<a href="https://etap.com">https://etap.com</a>)</li><li>Flowmon (<a href="https://www.flowmon.com">https://www.flowmon.com</a>)</li><li>Info360 Insight (<a href="https://www.autodesk.com">https://www.autodesk.com</a>)</li><li>LogRhythm (<a href="https://logrhythm.com">https://logrhythm.com</a>)</li></ul>
OT Network Monitoring and Threat Detection Tools	<ul style="list-style-type: none"><li>SCADAfence (<a href="https://www.scadafence.com">https://www.scadafence.com</a>)</li><li>Microsoft Defender for IoT (<a href="http://www.microsoft.com">http://www.microsoft.com</a>)</li><li>OPSWAT OT Platform (<a href="https://www.opswat.com">https://www.opswat.com</a>)</li><li>Rhebo (<a href="https://rhebo.com">https://rhebo.com</a>)</li><li>Forescout (<a href="https://www.forescout.com">https://www.forescout.com</a>)</li></ul>
OT Malware Analysis Tools	<ul style="list-style-type: none"><li>CyberX's ICS Malware Sandbox (<a href="https://cyberx-labs.com">https://cyberx-labs.com</a>)</li><li>FortiGuard Inline Sandbox Service (<a href="https://www.fortinet.com">https://www.fortinet.com</a>)</li><li>Steppa Malware Analysis Solution (<a href="https://steppa.ae">https://steppa.ae</a>)</li><li>VirusTotal (<a href="https://www.virustotal.com">https://www.virustotal.com</a>)</li><li>IDA Pro (<a href="https://www.hex-rays.com">https://www.hex-rays.com</a>)</li></ul>
Tools for Detecting Network Traffic Anomalies in ICS networks	<ul style="list-style-type: none"><li>Flowmon (<a href="https://www.flowmon.com">https://www.flowmon.com</a>)</li><li>Malcolm (<a href="https://malcolm.fyi">https://malcolm.fyi</a>)</li><li>Forescout eyeInspect (<a href="https://www.forescout.com">https://www.forescout.com</a>)</li><li>Industrial Defender (<a href="https://www.industrialdefender.com">https://www.industrialdefender.com</a>)</li><li>Dragos Platform (<a href="https://www.dragos.com">https://www.dragos.com</a>)</li><li>Nozomi Networks (<a href="https://www.nozominetworks.com">https://www.nozominetworks.com</a>)</li></ul>
Tools for Passive Discovery and Analysis of OT Network	<ul style="list-style-type: none"><li>LogRhythm NDR (<a href="https://logrhythm.com">https://logrhythm.com</a>)</li></ul>
Tools for Analyzing IIoT Traffic	<ul style="list-style-type: none"><li>NetworkMiner (<a href="https://www.netresec.com">https://www.netresec.com</a>)</li></ul>
Tools for Analyzing Modbus/TCP Traffic	<ul style="list-style-type: none"><li>Wireshark (<a href="https://www.wireshark.org">https://www.wireshark.org</a>)</li></ul>

<b>Tools for Acquiring Evidence</b>	<ul style="list-style-type: none"><li>▪ Belkasoft Live RAM Capturer (<a href="https://belkasoft.com">https://belkasoft.com</a>)</li><li>▪ Registry Recon (<a href="https://arsenalrecon.com">https://arsenalrecon.com</a>)</li><li>▪ MAGNET RAM Capture (<a href="https://www.magnetforensics.com">https://www.magnetforensics.com</a>)</li><li>▪ X-Ways Forensics (<a href="http://www.x-ways.net">http://www.x-ways.net</a>)</li><li>▪ Volatility Framework (<a href="https://www.volatilityfoundation.org">https://www.volatilityfoundation.org</a>)</li><li>▪ CAINE (<a href="https://www.caine-live.net">https://www.caine-live.net</a>)</li></ul>
<b>OT-based Log Analysis Tools</b>	<ul style="list-style-type: none"><li>▪ Splunk Enterprise (<a href="https://www.splunk.com">https://www.splunk.com</a>)</li><li>▪ NXLog Enterprise Edition (<a href="https://nxlog.co">https://nxlog.co</a>)</li></ul>
<b>OT Security Tools</b>	<ul style="list-style-type: none"><li>▪ Tenable.ot (<a href="https://www.tenable.com">https://www.tenable.com</a>)</li><li>▪ Forescout eyeSight (<a href="https://www.forescout.com">https://www.forescout.com</a>)</li><li>▪ Singtel One (<a href="https://www.singtel.com">https://www.singtel.com</a>)</li><li>▪ Claroty (<a href="https://www.claroty.com">https://www.claroty.com</a>)</li><li>▪ PA-220R (<a href="https://www.paloaltonetworks.com">https://www.paloaltonetworks.com</a>)</li><li>▪ Radiflow's CIARA (<a href="https://www.radiflow.com">https://www.radiflow.com</a>)</li></ul>