

IoT-based Security Incident Handling Toolkit

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

IoT-based Security Incident Handling Tools	
Category	Tools
IoT Incident Management Tools	<ul style="list-style-type: none">▪ PagerDuty (https://www.pagerduty.com)▪ OnPage (https://www.onpage.com)▪ Asimily (https://asimily.com)▪ AggreGate (https://aggregate.digital)▪ Microsoft Defender for IoT (https://www.microsoft.com)
IoT Monitoring Tools	<ul style="list-style-type: none">▪ Domotz (https://www.domotz.com)▪ AWS IoT Device Management (https://aws.amazon.com)▪ Datadog IoT Monitoring (https://www.datadoghq.com)▪ Particle (https://www.particle.io)▪ ScienceLogic SL1 Platform (https://sciencelogic.com)
IoT Network Traffic Analysis Tools	<ul style="list-style-type: none">▪ Wireshark (https://www.wireshark.org)▪ IoT Inspector (https://github.com)▪ IoT Analytics (https://www.cellusys.com)▪ IoTShark (https://github.com)▪ Open Sniffer (https://www.sewio.net)▪ Foren6 (https://cetic.github.io)
Tools for Detecting IoT-based Security Incidents	<ul style="list-style-type: none">▪ Microsoft Sentinel (https://www.microsoft.com)
IoT-based Log Analysis Tools	<ul style="list-style-type: none">▪ Datadog (https://www.datadoghq.com)▪ Sematext Logs (https://sematext.com)▪ Mezmo (https://www.mezmo.com)▪ Coralogix (https://coralogix.com)
IoT Security Tools	<ul style="list-style-type: none">▪ SeaCat.io (https://www.teskalabs.com)▪ Check Point Quantum IoT Protect (https://www.checkpoint.com)▪ Paloalto IoT Security (https://www.paloaltonetworks.com)▪ DigiCert ONE (https://www.digicert.com)▪ Bosch IoT Insights (https://bosch-iot-suite.com)▪ Cisco Industrial Threat Defense (https://www.cisco.com)