

# Cloud Security Incident Handling Toolkit

Listed below are some of the tools that can be used by the incident handler to handle cloud security incidents.

Cloud Security Incident Handling Tools	
Category	Tools
Cloud-based Log Analysis Tools	<ul style="list-style-type: none"><li>Datadog (<a href="https://www.datadoghq.com">https://www.datadoghq.com</a>)</li><li>Loggly (<a href="https://www.loggly.com">https://www.loggly.com</a>)</li><li>Sumo Logic (<a href="https://www.sumologic.com">https://www.sumologic.com</a>)</li><li>Splunk Cloud (<a href="https://www.splunk.com">https://www.splunk.com</a>)</li><li>Papertrail (<a href="https://papertrailapp.com">https://papertrailapp.com</a>)</li><li>Logz.io (<a href="https://logz.io">https://logz.io</a>)</li></ul>
Tools for Detecting Cloud Security Incidents	<ul style="list-style-type: none"><li>Falco (<a href="https://falco.org">https://falco.org</a>)</li><li>ExtraHop Reveal(x) 360 (<a href="https://www.extrahop.com">https://www.extrahop.com</a>)</li><li>MetaFlows (<a href="https://www.metaflows.com">https://www.metaflows.com</a>)</li><li>Radware (<a href="https://www.radware.com">https://www.radware.com</a>)</li><li>Confluera (<a href="https://www.confluera.com">https://www.confluera.com</a>)</li><li>Qualys Cloud Platform (<a href="https://www.qualys.com">https://www.qualys.com</a>)</li><li>Sumo logic (<a href="https://www.sumologic.com">https://www.sumologic.com</a>)</li></ul>
Tools for Containment of Cloud Security Incidents	<ul style="list-style-type: none"><li>Teleport (<a href="https://goteleport.com">https://goteleport.com</a>)</li><li>Cisco Identity Services Engine (ISE) (<a href="https://www.cisco.com">https://www.cisco.com</a>)</li><li>Trend Micro One (<a href="https://www.trendmicro.com">https://www.trendmicro.com</a>)</li><li>Tigera (<a href="https://www.tigera.io">https://www.tigera.io</a>)</li><li>Deepfence (<a href="https://deepfence.io">https://deepfence.io</a>)</li><li>Qualys Cloud Platform (<a href="https://www.qualys.com">https://www.qualys.com</a>)</li></ul>
Tools for Detecting and Responding to Azure Security Threats	<ul style="list-style-type: none"><li>Microsoft Azure Sentinel (<a href="https://www.microsoft.com">https://www.microsoft.com</a>)</li></ul>
Tools for Managing and Responding to Azure Security Alerts	<ul style="list-style-type: none"><li>Microsoft Defender for Cloud (<a href="https://www.microsoft.com">https://www.microsoft.com</a>)</li></ul>
Azure Incident Response Tools	<ul style="list-style-type: none"><li>VIACode Incident Management System (<a href="https://viacode.com">https://viacode.com</a>)</li><li>Sparrow.ps1 (<a href="https://github.com">https://github.com</a>)</li><li>Sonrai Dig (<a href="https://sonraisecurity.com">https://sonraisecurity.com</a>)</li><li>Stormspotter (<a href="https://github.com">https://github.com</a>)</li></ul>

	<ul style="list-style-type: none"> <li>▪ InsightIDR (<a href="https://www.rapid7.com">https://www.rapid7.com</a>)</li> <li>▪ Sysdig (<a href="https://sysdig.com">https://sysdig.com</a>)</li> </ul>
<b>Azure Security Tools</b>	<ul style="list-style-type: none"> <li>▪ Orca (<a href="https://orca.security">https://orca.security</a>)</li> <li>▪ Barracuda (<a href="https://www.barracuda.com">https://www.barracuda.com</a>)</li> <li>▪ Zscaler Private Access for Azure (<a href="https://www.zscaler.com">https://www.zscaler.com</a>)</li> <li>▪ CyberArk (<a href="https://www.cyberark.com">https://www.cyberark.com</a>)</li> <li>▪ Trend Micro Cloud One (<a href="https://www.trendmicro.com">https://www.trendmicro.com</a>)</li> <li>▪ Rubrik (<a href="https://www.rubrik.com">https://www.rubrik.com</a>)</li> </ul>
<b>Tools for Detection and Analysis of AWS Security Incidents</b>	<ul style="list-style-type: none"> <li>▪ GuardDuty (<a href="https://aws.amazon.com">https://aws.amazon.com</a>)</li> </ul>
<b>Tools for Recovery after AWS Security Incidents</b>	<ul style="list-style-type: none"> <li>▪ CloudEndure Disaster Recovery (<a href="https://aws.amazon.com">https://aws.amazon.com</a>)</li> </ul>
<b>AWS Security Tools</b>	<ul style="list-style-type: none"> <li>▪ Qualys (<a href="https://www.qualys.com">https://www.qualys.com</a>)</li> <li>▪ Aqua (<a href="https://www.aquasec.com">https://www.aquasec.com</a>)</li> <li>▪ Check Point CloudGuard (<a href="https://www.checkpoint.com">https://www.checkpoint.com</a>)</li> <li>▪ SIOS (<a href="https://us.sios.com">https://us.sios.com</a>)</li> <li>▪ Recon.Cloud (<a href="https://recon.cloud">https://recon.cloud</a>)</li> <li>▪ Laminar (<a href="https://laminarsecurity.com">https://laminarsecurity.com</a>)</li> </ul>
<b>Tools for Analyzing Google Cloud Log Data</b>	<ul style="list-style-type: none"> <li>▪ Google Cloud Log Analytics (<a href="https://cloud.google.com">https://cloud.google.com</a>)</li> </ul>
<b>Google Cloud Security Tools</b>	<ul style="list-style-type: none"> <li>▪ Dynatrace (<a href="https://www.dynatrace.com">https://www.dynatrace.com</a>)</li> <li>▪ Chronicle (<a href="https://chronicle.security">https://chronicle.security</a>)</li> <li>▪ CrowdStrike Falcon (<a href="https://www.crowdstrike.com">https://www.crowdstrike.com</a>)</li> <li>▪ GCP Monitor (<a href="https://www.site24x7.com">https://www.site24x7.com</a>)</li> <li>▪ Datadog (<a href="https://www.datadoghq.com">https://www.datadoghq.com</a>)</li> <li>▪ ManageEngine Applications Manager (<a href="https://www.manageengine.com">https://www.manageengine.com</a>)</li> </ul>
<b>Cloud Security Tools</b>	<ul style="list-style-type: none"> <li>▪ Fidelis CloudPassage Halo (<a href="https://fidelissecurity.com">https://fidelissecurity.com</a>)</li> <li>▪ CrowdStrike (<a href="https://www.crowdstrike.com">https://www.crowdstrike.com</a>)</li> <li>▪ Darktrace (<a href="https://darktrace.com">https://darktrace.com</a>)</li> <li>▪ Trend Micro (<a href="https://www.trendmicro.com">https://www.trendmicro.com</a>)</li> <li>▪ Sophos Cloud Native Security (<a href="https://www.sophos.com">https://www.sophos.com</a>)</li> <li>▪ Cato SASE Cloud with SSE 360 (<a href="https://www.catonetworks.com">https://www.catonetworks.com</a>)</li> </ul>