Microsoft Sentinel SOC Activities

Daily SOC Tasks

- **Triage and investigate incidents:** Review the Microsoft Sentinel Incidents page to check for new incidents generated by the currently configured analytics rules and start investigating any new incidents. For more information, see Tutorial: Investigate incidents with Microsoft Sentinel
- **Explore workbooks:** Analyze visualized data in your Sentinel workbooks. Use this information for monitoring, preparing for further investigations, and hunting.
- **Explore hunting queries and bookmarks:** Explore results for all built-in queries and update existing hunting queries and bookmarks. Manually generate new incidents or update old incidents if applicable. For more information, see:
  - Automatically create incidents from Microsoft security alerts
  - Hunt for threats with Microsoft Sentinel
  - Keep track of data during hunting with Microsoft Sentinel
- **Playbook failures:** Verify playbook run statuses and troubleshoot any failures.

Weekly SOC Tasks

- **Analytic rules:** Review and enable new analytics rules as applicable, including both newly released or newly available rules from recently connected data connectors.
- **Data connectors:** Review the status, date, and time of the last log received from each data connector to ensure that data is flowing. Check for new connectors, and review ingestion to ensure set limits haven't been exceeded.
- **Log Analytics Agent:** Verify that servers and workstations are actively connected to the workspace and troubleshoot and remediate any failed connections.
- **Workbook updates:** Verify whether any workbooks have updates that need to be installed. For more information, see Commonly used Microsoft Sentinel workbooks
- **Microsoft Sentinel auditing:** Review Microsoft Sentinel activity to see who has updated or deleted resources, such as analytics rules, bookmarks, and so on. For more information, see Audit Microsoft Sentinel queries and activities

Monthly SOC Tasks

- **Review user access:** Review permissions for your users and check for inactive users. For more information, see Permissions in Microsoft Sentinel
- **Log Analytics workspace review:** Review that the Log Analytics workspace data retention policy still aligns with your organization's policy. For more information, see Data retention policy
- **What's new in Microsoft Sentinel:** This article lists recent features added for Microsoft Sentinel, and new features in related services that provide an enhanced user experience in Microsoft Sentinel.
- **Microsoft Sentinel GitHub repository review:** Review the Microsoft Sentinel GitHub repository to explore whether there are any new or updated resources of value for your environment, such as analytics rules, workbooks, hunting queries, or playbooks.

By:
Daniel Chronlund (https://danielchronlund.com)

Version:
2022-09-20

Inspired by:
https://learn.microsoft.com/en-us/azure/sentinel/best-practices