squad

Squad offer : Sentinel SIEM/SOAR assessment

Sentinel SIEM/SOAR - Assessment - Overview

- Sentinel is the SIEM/SOAR (Security Information and Event Management /Security Orchestration, Automation, and Response) tool natively provided by Microsoft.
- It is the key tool for your SOC to protect your company.
- Squad can help you unleash the full potential of this product.

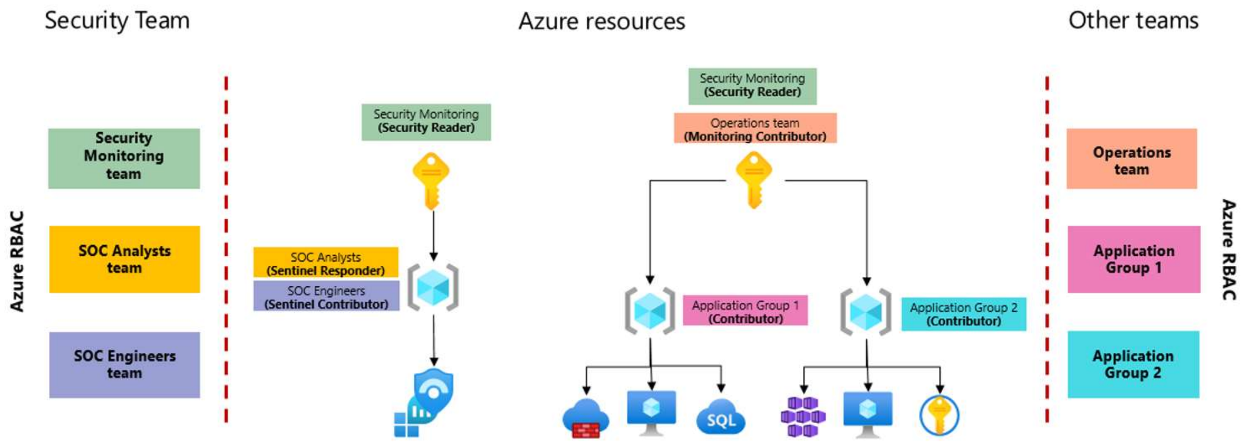
Sentinel SIEM/SOAR - Assessment - Summary

- **Includes the following**
  - Assessment and gap analysis of the Microsoft Secure Score
  - Assessment and gap analysis of the best practice
  - Executive summary and management recommandation
- **Service type :** Assessment
- **Duration and pricing :** 10 days and and 20 000 $*(depending on your infrastructure size, this duration and amount may vary. A formal proposal will be issued upfront)*
- **Country/Region :** France, Switzerland
- **Product :** Sentinel, Azure Logic Apps

- **Delivery Format**
  - Kickoff Conference Call
  - Security Discovery and Planning Workshop
  - Detailed Assessment (completed remotely)
  - Summary Presentation (physically or remotely)
- **Deliverables Included**
  - Security and configuration Assessment Report
  - Security and configuration Gap Analysis and Recommendations
  - Summary Presentation (includes deployment roadmap for recommended changes, if applicable)

Sentinel SIEM/SOAR - Assessment - Description

- Assess the relevance of your analysis rules and associated responses (playbook, logic app)
- Assess the proper usage of SOAR catalog provided by MS
- Management report will also adress :
  - FINOPS : Filter logs before ingestion (with azure monitor agent or logstash to enrich them), Prioritie for your data connectors, storage management…etc
  - Any forgotten log sources
  - RBAC table level to make sure yours is respecting least privilege



Security Team

Azure resources

Other teams

Azure RBAC

Security Monitoring team

SOC Analysts team

SOC Engineers team

Security Monitoring (Security Reader)

SOC Analysts (Sentinel Responder)

SOC Engineers (Sentinel Contributor)

Security Monitoring (Security Reader)

Operations team (Monitoring Contributor)

Application Group 1 (Contributor)

Application Group 2 (Contributor)

SQL

Operations team

Application Group 1

Application Group 2

Azure RBAC