A person sitting at a desk with multiple screens

AI-generated content may be incorrect.

**Microsoft Sentinel SOC Optimization Report**

Table of Contents

[Introduction 3](#_Toc189988115)

[Microsoft Sentinel SOC Optimization Activities 3](#_Toc189988116)

[1. Analysis of Sentinel SOC Optimizations 3](#_Toc189988117)

[2. Microsoft Sentinel SOC Optimization Details 4](#_Toc189988118)

[Next Steps 4](#_Toc189988119)

# Introduction

Security Information and Event Management (SIEM) optimization is an ongoing process that requires continuous assessment and enhancement of detection capabilities. Microsoft Sentinel provides SOC Optimizations based on best practices, analytics, and threat intelligence to improve SIEM effectiveness. These recommendations address areas such as missing detection rules and log source ingestion.

This report presents an analysis of Microsoft Sentinel SOC Optimizations, categorizes their status, and outlines activities undertaken to enhance SIEM functionality. The focus is placed on addressing detection gaps, particularly those related to Threat Actor Tactics, Techniques, and Procedures (TTPs).

# Microsoft Sentinel SOC Optimization Activities

1. Analysis of Sentinel SOC Optimizations

Microsoft Sentinel generates SOC Optimizations based on identified security monitoring gaps. These recommendations are classified into three statuses:

* **Active** – Recommendations pending implementation.
* **In Progress** – Recommendations are in progress.
* **Completed** – Recommendations successfully applied.
* **Dismissed** – Recommendations reviewed but deemed unnecessary or irrelevant.

During the assessment period, the following categorization was recorded:

* **Total Optimizations:** {{TotalOptimizations}}
* **Active:** {{ActiveOptimizations}}
* **In Progress:** {{InProgressOptimizations}}
* **Completed:** {{CompletedOptimizations}}
* **Dismissed:** {{DismissedOptimizations}}

|  |
| --- |
| {{Chart}} |

2. Microsoft Sentinel SOC Optimization Details

{% for optimization in Optimizations %}

### {{optimization.Title}} - {{optimization.Status}}

Creation Date: {{optimization.CreationTime}}

{{optimization.Description}}

{% endfor %}

# Next Steps

* Continued monitoring of Sentinel recommendations to prioritize high-impact detections.
* Expansion of coverage for emerging threat actor techniques based on updated threat intelligence.
* Regular fine-tuning of detection rules based on new attack trends and SIEM analytics insights.

Ongoing refinement of SIEM configuration and detection strategies is essential for strengthening security posture and improving the ability to detect and respond to evolving threats effectively.