SOC Optimization in Microsoft Sentinel  
  
We are thrilled to announce the new SOC Optimization feature in Microsoft Sentinel, now available in both the Microsoft Defender portal and the Azure portal. This preview feature is designed to help Security Operations Center (SOC) teams enhance their processes and outcomes efficiently.  
  
Key Benefits:  
  
Actionable Recommendations: High-fidelity insights to optimize security controls, ensuring maximum value from Microsoft security services.  
Cost Optimization: Identify opportunities to reduce data ingestion costs without compromising security needs or coverage.  
Tailored Solutions: Recommendations customized to your environment, based on your current coverage and threat landscape.  
  
How It Works:  
  
Optimize Security Controls: Gain more value from your Microsoft security services with tailored recommendations.  
Close Coverage Gaps: Address specific threats by tightening ingestion rates and adding necessary security controls.  
Automated Efficiency: Save time on manual analysis with automated recommendations to optimize your Microsoft Sentinel workspace.  
  
Prerequisites:  
  
Microsoft Sentinel Roles and Permissions: Ensure your team has the necessary roles and permissions.  
Integration with Microsoft Defender XDR: Connect Microsoft Sentinel to Microsoft Defender XDR for seamless optimization.  
  
Access and Manage Recommendations:  
  
 In the Azure Portal:  
🔹 Navigate to Microsoft Sentinel > Threat Management > SOC Optimization.  
🔹 View metrics and recommendations on the Overview tab.  
🔹 Filter and search for specific optimizations.  
🔹 View full details of each recommendation and take action directly from the portal.  
  
In the Defender Portal:  
🔹Access the unified SOC operations platform for a comprehensive view.  
🔹 Use the SOC Optimization page to review and manage recommendations.  
  
Utilize the API for advanced access to SOC optimizations.  
  
Key Metrics:  
  
🔹 Ingested Data: Monitor the total data ingested over the last three months.  
🔹 Optimization Status: Track active, completed, and dismissed recommendations.  
🔹 Threat Scenarios: View relevant threats, active and recommended detections, and coverage levels.  
  
Take Action:  
  
🔹 Analytics Rules: Add or update analytics rules to enhance protection.  
🔹 Cost Management: Adjust your data plan to maximize security value while managing costs.  
  
This preview feature is part of our continuous efforts to enhance security operations and provide our customers with the tools they need to stay ahead of evolving threats. We invite you to explore and leverage SOC Optimization to make your security operations more efficient and cost-effective.

