SYNERGY ADVISORS

Micro-Vigilant SecOps Agent

Improve Visibility and Operational Efficiency Across Microsoft Defender XDR Security Operations

Security Operations Centers (SOCs) are expected to **manage increasing volumes of alerts, incidents, and investigations** while maintaining efficient response processes and consistent operational performance. Although Microsoft Defender XDR provides extensive visibility into security activity, many organizations still struggle to understand how effectively their security operations are functioning on a day-to-day basis.

As incident queues grow, security teams often face unresolved investigations, aging incidents, uneven workload distribution, and limited visibility into operational bottlenecks.

From Security Telemetry to Operational Intelligence

The **Micro-Vigilant SecOps Agen**t is an AI-powered operational intelligence solution that transforms Microsoft Defender XDR operational data into actionable insights for SOC teams. By continuously analyzing security operations activity, the solution helps organizations gain visibility into performance, identify operational inefficiencies, and support more informed decision-making.

Operational Visibility:
Understand the current state of security operations.

Performance Intelligence:
Measure analyst workload and response performance.

Actionable Recommendations:
Improve efficiency through AI-driven insights.

How the Micro-Vigilant SecOps Agent Works

The solution leverages **Microsoft Defender XDR** telemetry through the **Micro-Vigilant** platform to continuously analyze incident lifecycle data, analyst activity, investigation status, and security signal trends. These insights are processed by the SecOps Intelligence Agent and presented through operational dashboards, analytics, and AI-generated recommendations.

Operational Intelligence Capabilities

The **Micro-Vigilant SecOps Agent** continuously evaluates operational security data to provide visibility into incident management, analyst performance, detection effectiveness, and overall SOC operations. By correlating operational activity with security workflows, the solution helps organizations identify inefficiencies, prioritize actions, and support ongoing operational improvement initiatives.

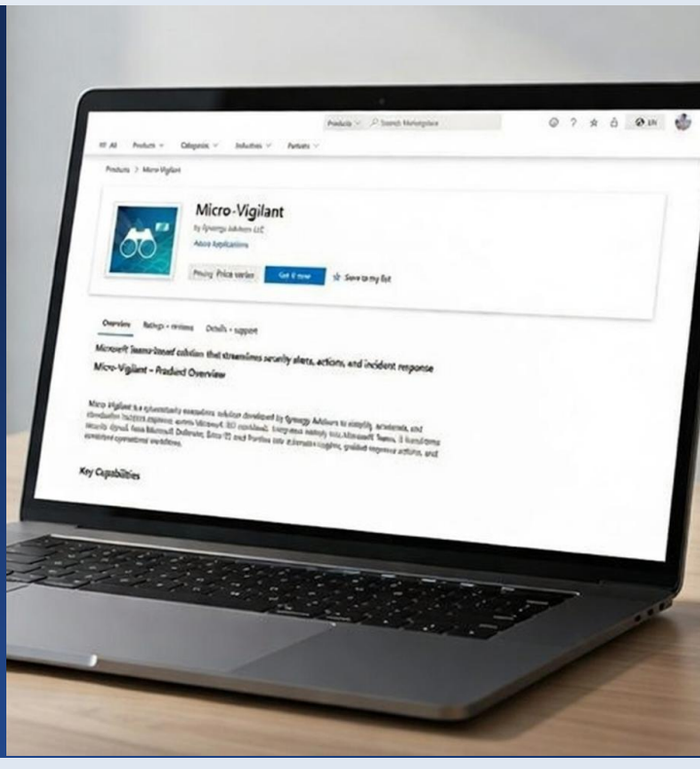
Operational Area	Insights
SOC Operational Health	Visibility into open, unresolved, aging, and stale incidents, including ownership gaps and workflow bottlenecks that may impact response effectiveness.
Analyst Performance & Workload	Analysis of incident ownership, workload distribution, response activity, and Mean Time to Resolution (MTTR) to support workload visibility across teams.
Critical Incident Prioritization	Identification of unresolved investigations requiring attention based on age, investigation status, and operational relevance.
Detection Quality Analysis	Visibility into recurring false positives, noisy detections, repetitive alert patterns, and potential opportunities to improve alert effectiveness.
Operational Recommendations	AI-generated recommendations designed to support workload optimization, prioritization improvements, and operational efficiency.
Trend & Signal Visibility	Analysis of recurring alert categories, operational patterns, and Defender XDR activity trends that may influence SOC performance.

Gain a Deeper Understanding of Your Security Operations

The **Micro-Vigilant SecOps Agent** helps organizations move beyond incident visibility by providing a clearer understanding of how security operations perform over time.

Through continuous analysis of operational activity within **Microsoft Defender XDR**, the solution delivers actionable insights into incident management, analyst workload, detection effectiveness, and overall, SOC performance.

By transforming operational security data into meaningful intelligence, organizations can improve operational awareness, identify opportunities for optimization, and support more effective security operations.



For more information, please feel free to contact us at micro-vigilant@synergyadvisors.biz

Learn more