SIEM AUGMENTATION

How Stellar Cyber Open XDR Enhances Microsoft Sentinel

Microsoft Sentinel is a cloud-native security information and event management (SIEM) solution with a variety of useful capabilities, especially for organizations with a large footprint of Microsoft products in use. By adding Stellar Cyber Open XDR to their security stack, organizations can improve the effectiveness, efficiency, and outcomes from Microsoft Sentinel.

Here are three ways Stellar Cyber enhances Microsoft Sentinel.

Data Ingestion and Retention

- **How Microsoft Sentinel Works:** Microsoft Sentinel charges based on the volume of data ingested, which can become costly, particularly for organizations with high-volume environments. The retention costs for storing data beyond a certain period can also add up.

- **How Stellar Cyber Helps:** Stellar Cyber Open XDR helps by pre-filtering and correlating the data before sending it to Sentinel, reducing the overall volume of data ingested into Sentinel. It performs advanced threat detection and analytics at the XDR level, sending only high-priority or correlated events to Sentinel, reducing unnecessary data and lowering the associated costs.

Alert Volume and Prioritization

- **How Microsoft Sentinel Works:** Like many SIEM systems, Microsoft Sentinel users often face alert fatigue due to a high volume of false positives, making it difficult for security teams to identify actual threats among the noise.

- **How Stellar Cyber Helps:** Stellar Cyber's Open XDR platform provides more intelligent alert prioritization and correlation by unifying signals from various sources into meaningful incidents. This action reduces the number of alerts and false positives sent to Sentinel by performing context-aware correlation before Sentinel processes the data. This process ensures that Sentinel's alerting focuses more on actual threats, improving incident response efficiency.

Managing Multi-Vendor, Multi-Tool Environments

- **How Microsoft Sentinel Works:** Many organizations use multiple security tools from various vendors, making integrating all these tools into Microsoft Sentinel complex. Sentinel's integration capabilities are sufficient, but managing data from different security products can be challenging and lead to siloed data.

- **How Stellar Cyber Helps:** Stellar Cyber Open XDR is a unifying layer that integrates data from various security tools into a single platform. It normalizes, correlates, and enriches data from multi-vendor sources before sending it to Sentinel. This approach simplifies the process for organizations using different tools and helps Sentinel ingest data more seamlessly, improving overall visibility and reducing the complexity of managing a multi-tool environment.

Summary of How Stellar Cyber Open XDR Helps Make Microsoft Sentinel More Effective

- **Improved Integration**: Stellar Cyber simplifies integration and data management across multi-vendor security environments, improving operational efficiency in Sentinel.

- **Data Filtering and Optimization**: Reduces data ingestion costs by filtering out irrelevant data and correlating meaningful events before sending them to Sentinel.

- **Enhanced Threat Detection**: Reduces alert fatigue by correlating multi-source data and reducing false positives, leading to a more effective use of Sentinel's alerting.

In summary, Stellar Cyber helps improve the efficiency and cost-effectiveness of using Microsoft Sentinel as the primary SecOps platform.

Stellar Cyber delivers comprehensive, unified security without complexity, empowering lean security teams of any skill to successfully secure their environments. With Stellar Cyber, organizations reduce risk with early and precise identification and remediation of threats while slashing costs, retaining investments in existing tools, and improving analyst productivity, delivering an 8X improvement in MTTD and a 20X improvement in MTTR. The company is based in Silicon Valley. For more information, visit **stellarcyber.ai**.