SOLUTION BRIEF

1Password

1Password and Stellar Cyber

Streamline Security Data Management and Accelerates Threat Detection and Response

Stellar Cyber Open XDR is a security operations platform that empowers lean security teams to take control of their operations. By combining NG-SIEM, NDR, UEBA, TIP, FIM, IDS, and intelligent automation, Stellar Cyber streamlines investigation workflows, reduces attacker dwell time, and boosts security analyst productivity. With the 1Password integration, organizations can leverage these advanced features to ingest, normalize, and enrich all security data, including endpoints, network, cloud, and log data, into a single, unified repository.

The 1Password integration supports audit events, item usage events, and sign-in attempts, allowing for comprehensive monitoring and threat detection. Stellar Cyber's proprietary threat detection engine, powered by Multi-layer AI™, automatically detects and correlates alerts, accelerating threat investigations and hunting. The integration offers real-time automated and manual response actions, ensuring that security teams can respond swiftly to incidents, further reducing risk and enhancing overall security effectiveness.

How it Works

The integration between 1Password and Stellar Cyber works as follows:

Data Ingestion: The 1Password integration pulls critical security data from 1Password Business accounts using the 1Password Events API. This data includes audit events (e.g., account updates, vault permissions), item usage events (e.g., when and who accessed specific items), and sign-in attempts (e.g., details about login attempts, including location and device).

Normalization and Enrichment: Once ingested into Stellar Cyber, 1Password data is automatically normalized and enriched. Normalization ensures that the data is formatted and categorized consistently with other security data within the Stellar Cyber ecosystem. Enrichment involves adding context and metadata to the raw data, making it more useful for analysis and threat detection.

Threat Detection and Correlation: Stellar Cyber analyzes the normalized and enriched data from 1Password. It automatically detects potential security threats and correlates these events with other data sources like endpoints, networks, and cloud services. This correlation helps identify complex attack patterns that might go unnoticed if security analysts analyzed each data source in isolation.

Incident Investigation and Response: Security teams can use Stellar Cyber's platform to investigate incidents involving 1Password data. The platform provides detailed contextual information, such as who accessed sensitive items or when suspicious sign-in attempts occurred. Analysts can then use this information to perform threat hunting or initiate automated or manual responses. The integration enables real-time response actions, such as alerting security teams, blocking suspicious IPs, or triggering additional authentication measures.

User Interface and Management: Users can manage the integration through a user-friendly interface within the Stellar Cyber platform. Administrators can configure the 1Password integration, setting parameters like API tokens, data retrieval intervals, and SSL verification. The platform also provides tools to search and filter 1Password data by specific properties, making it easy to drill down into particular events or trends.

Overall, this integration enables organizations to enhance their security operations by providing a comprehensive view of their security landscape, combining the critical data from 1Password with the advanced detection and response capabilities of Stellar Cyber.

Stellar Cyber Open XDR platform 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.**