Sumo Logic & Druva: Strengthening Data Security with Seamless SIEM Integration

Enhancing threat detection and incident response by integrating backup data with SIEM systems.

The challenge

As organizations face increasing cyber threats, traditional security monitoring systems often overlook backup data, making it vulnerable to attacks such as ransomware, unauthorized access, and data corruption. Backup environments are critical for business continuity, yet they remain disconnected from broader security operations. Without integrating backup data into Security Information and Event Management (SIEM) systems, organizations struggle to detect, investigate, and respond quickly to security incidents. Additionally, regulatory compliance requirements demand enhanced visibility into backup events for auditing and reporting.

Integrating backup telemetry with SIEM solutions enables real-time monitoring, improves threat detection, and streamlines incident response workflows. This integration provides security teams with holistic visibility, ensuring that backup data is protected from emerging threats and compliance gaps are minimized.

The solution

Integrating Druva's cloud-native backup data with Sumo Logic allows organizations to ingest critical backup-related events into their SIEM platform, enabling security teams to monitor and analyze these events in real time. This solution supports advanced threat detection, faster incident response, and enhanced regulatory compliance reporting. By consolidating backup data into a single security framework, organizations can quickly identify suspicious activity, reduce the attack surface, and ensure business continuity in case of a cyberattack.

Benefits of the integration

- **Unified Security Operations**: Ingest backup telemetry data into Sumo Logic, enriching your SIEM ecosystem for comprehensive threat monitoring.
- **Improved Threat Detection**: Correlates backup telemetry data with other security logs to identify anomalies and potential risks.
- **Real-Time Incident Response**: Automates the identification and escalation of backup-related threats for faster response times.
- **Compliance Readiness**: Supports regulatory compliance by providing visibility and reporting for backup events.
- **Enhanced Cyber Resilience**: Strengthens protection against data loss, ransomware, and other threats targeting backup systems.
- **Operational Efficiency**: Automates data ingestion and correlation, reducing manual efforts for security teams.

The integration

The Druva integration with Sumo Logic enables seamless data ingestion of backup-related events into Sumo Logic Enterprise. This integration empowers security teams with enhanced visibility into backup data, helping them detect anomalies, respond to incidents, and ensure compliance with data governance requirements.

Key features

- **Automated Event Ingestion**: Collects and ingests backup-related events from Druva's Data Security platform into Sumo Logic in real time.
- **Advanced Correlations**: Correlates backup data with other security logs (network, endpoint, cloud) for enhanced threat analysis.
- **Real-Time Event Collection**: Captures critical backup events such as access attempts, file changes, and backup status.
- **Incident Management**: Integrates with Sumo Logic's Incident Review functionality for streamlined threat remediation.
- **Compliance and Reporting**: Provides detailed event logs for compliance auditing and regulatory reporting needs.

This integration enhances Sumo Logic's capabilities by providing critical backup visibility, enabling faster threat detection and streamlined security workflows.

Sumo Logic and Druva

The integration of Druva's backup data with Sumo Logic provides security teams with a unified view of their environment, enabling the detection of anomalies and potential threats in real time. This seamless integration allows for faster incident response, automated alerting, and comprehensive reporting. By correlating backup-related events with other security data, organizations can detect backup-targeted ransomware, unauthorized access attempts, and other attacks more quickly, reducing the time to remediate.

With this integration, organizations improve their cyber resilience by ensuring that backup environments are part of their overall security monitoring strategy, thereby minimizing the risk of data loss or disruption caused by malicious activity.

Use Case: Backup Anomaly Detection

- **Challenge:** Backup systems are often vulnerable to cyberattacks, such as ransomware or unauthorized data access. Detecting suspicious backup activities (e.g. abnormal file changes or failed backups) is crucial to maintaining data integrity and business continuity.
- **Solution:** By integrating Druva's backup data with Sumo Logic, security teams gain real-time visibility into backup activities, enabling the detection of anomalous behavior such as unauthorized access or irregular backup failures. This helps detect threats earlier, improving response times and minimizing operational risks.

Use Case: Incident Correlation for Threat Remediation

- **Challenge:** Correlating backup events with other IT infrastructure data (network, endpoint, cloud) is essential for providing a comprehensive understanding of security incidents. The lack of integrated data sources can delay threat identification and incident response.
- **Solution:** Integrating Druva's backup data with Sumo Logic enhances the correlation of backup anomalies with broader security events across the enterprise. This enables faster detection and investigation of complex attacks, such as ransomware targeting backup systems, by providing security teams with a comprehensive security view that accelerates root-cause analysis and remediation efforts.

Use Case: Proactive Backup System Monitoring and Threat Prevention

- **Challenge:** Backup systems are critical to data recovery, but they are also frequent targets for cybercriminals, including those employing tactics like ransomware, insider threats, or misconfigurations. Monitoring backup operations in real time is essential to detect and prevent any irregular activities that could compromise backup integrity or hinder recovery efforts. Organizations need a comprehensive solution to track the health and security of their backup environments to minimize downtime and data loss.

- **Solution:** Integrating Druva's backup data with Sumo Logic allows security teams to proactively monitor backup systems across multiple dimensions, enabling the detection of early warning signs of potential security issues or system failures. This integration helps teams:
    - **Monitor anomalous activities**, such as abnormal changes in backup files, unauthorized access attempts, or unusual data movement, which could signal cyberattacks or operational issues.
    - **Monitor failed login events**, identifying potential security threats such as brute-force attacks or compromised credentials targeting backup systems.
    - **Monitor suspicious restore activities**, flagging any unauthorized or unexpected restores that may indicate data theft, tampering, or ransomware attacks trying to recover encrypted data.
    - **Monitor deployment health**, ensuring that backup solutions are correctly deployed and functioning properly across all systems, preventing disruptions due to misconfigurations or performance issues.
    - **Monitor backup failure trends**, helping detect patterns of repeated backup failures or degraded performance, which could point to emerging threats, system malfunctions, or resource limitations that could impact data protection and recovery.

Product Integrations Between Sumo Logic and Druva

- **Druva App for Sumo Logic**: A robust integration for collecting Druva backup data and enriching your SIEM environment with backup-related events for threat detection.

druva Sales: +1-800-375-0160 | sales@druva.com

Americas: +1-800-375-0160
Europe: +44 (0) 20-3750-9440
India: +91 (0) 20 6726-3300
Japan: japan-sales@druva.com
Singapore: asean-sales@druva.com
Australia: anz-sales@druva.com

Druva, the autonomous data security company, puts data security on autopilot with a 100% SaaS, fully managed platform to secure and recover data from all threats. The Druva Data Security Cloud ensures the availability, confidentiality, and fidelity of data, and provides customers with autonomous protection, rapid incident response, and guaranteed data recovery. The company is trusted by its more than 6,000 customers, including 65 of the Fortune 500, to defend business data in today's ever-connected world. Amidst a rapidly evolving security landscape, Druva offers a $10 million Data Resiliency Guarantee ensuring customer data is protected and secure against every cyber threat. Visit druva.com and follow us on LinkedIn, Twitter, and Facebook.