ICSFUSION

IBM

Technical Use Case Document

Industrial Cybersecurity Platform ICSFusion and SIEM QRadar Integration

This document outlines the technical integration use case for the seamless collaboration between our Industrial Cybersecurity Platform, ICSFusion, and IBM's Security Information and Event Management (SIEM) solution, QRadar. By ensuring continuous log integration, leveraging native integration capabilities, and providing robust monitoring features, this integration empowers Security Operations Center (SOC) teams with enhanced visibility and actionable insights into industrial network security.

Continuous Log Integration

The integration between ICSFusion and QRadar ensures the continuous flow of log data from industrial control systems (ICS) to the SIEM platform. This continuous log integration is vital for real-time threat detection and incident response. ICSFusion extracts, transforms, and forwards logs generated by ICS devices to QRadar, allowing SOC teams to gain insights into the operational technology (OT) environment alongside traditional IT data.

Native Integration

Our solution offers a native integration with QRadar, leveraging standardized protocols and formats for seamless data exchange. This native integration ensures compatibility and interoperability between ICSFusion and QRadar, reducing complexity and optimizing performance. By adhering to QRadar's data formats and communication standards, ICSFusion maximizes the effectiveness of the SIEM solution in handling and analyzing industrial cybersecurity events.

Continuous Monitoring of Integration Health

To guarantee the reliability and effectiveness of the integration, ICSFusion includes robust monitoring features that continuously assess the health of the connection between ICSFusion and QRadar. This monitoring functionality provides real-time alerts and notifications for any issues that may arise, enabling prompt resolution and minimizing the risk of disruptions to the security monitoring workflow.

Ready Use Cases for QRadar to Enable SOC Teams

The integration comes with a set of pre-configured use cases specifically tailored for QRadar, enabling SOC teams to quickly and effectively monitor and respond to industrial cybersecurity events. These ready use cases leverage the unique capabilities of QRadar to correlate and analyze data from ICSFusion, providing SOC analysts with actionable intelligence for identifying, investigating, and mitigating potential threats in the industrial environment.

Benefits of Integration

Conclusion

The integration between ICSFusion and QRadar establishes a robust and effective synergy between industrial cybersecurity and SIEM capabilities. By ensuring continuous log integration, leveraging native integration, monitoring integration health, and providing ready use cases for QRadar, this collaboration enhances the overall cybersecurity posture of industrial environments, empowering SOC teams to proactively defend against emerging threats. This use case document serves as a guide for organizations looking to integrate ICSFusion and QRadar for comprehensive and efficient industrial cybersecurity management.