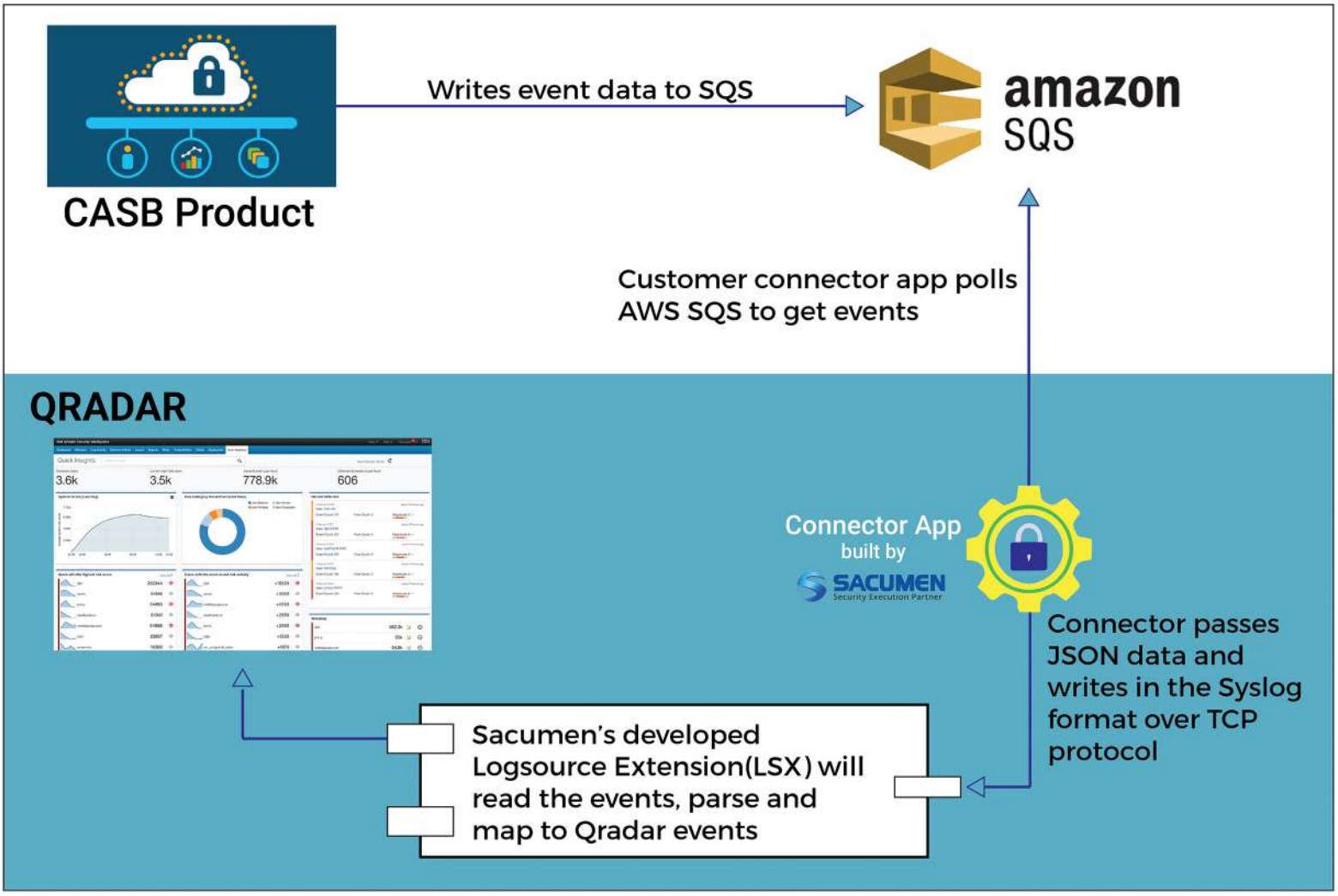
Secure Cloud Infrastructure Monitoring integration with QRadar



Customer

Customer is a leading CASB Monitoring solution provider.

They have a platform that provides the ease of use, visibility, continuous monitoring and investigation tools that security and compliance teams need to do their jobs at DevOps speed. The platform seamlessly integrates into multiple Cloud environments and provides a single pane of glass view into a compliance posture.

The Client requested for the integration of their CASB product with the On-premise/Cloud based QRadar so that they can monitor the Cloud through one SIEM console

Requirement

Technology Solution

- Sacumen developed the QRadar app that polls events data from the SQS service. Customer pushes the event data to SQS.
- Customer QRadar app write the event data in Syslog format over TCP.
- By configuring Customer log source to pick up the Syslog data and the custom event mapping feeds into QRadar, Customer event data is visible on QRadar console.
- QRadar app was developed for QRadar version 7.2.8 and above.
- Custom events regular expression configuration and other details packaged to make QRadar app deployment simpler

SACUMEN Security Execution Partner

Learn More : www.sacumen.com/services/connector-development

www.sacumen.com

Sacumen is an award winning pure play security product development services company. We are engaged with 50+ security product companies such as Symantec, Palo Alto Networks, Varonis, AlienVault, IBM, CA Technologies, ThreatConnect, SecurityScorecard, ForgeRock, Code42, BigID, Flashpoint etc in the areas of Connector Development, Connector Support and Product Engineering.

info@sacumen.com

+1 408 215 1253