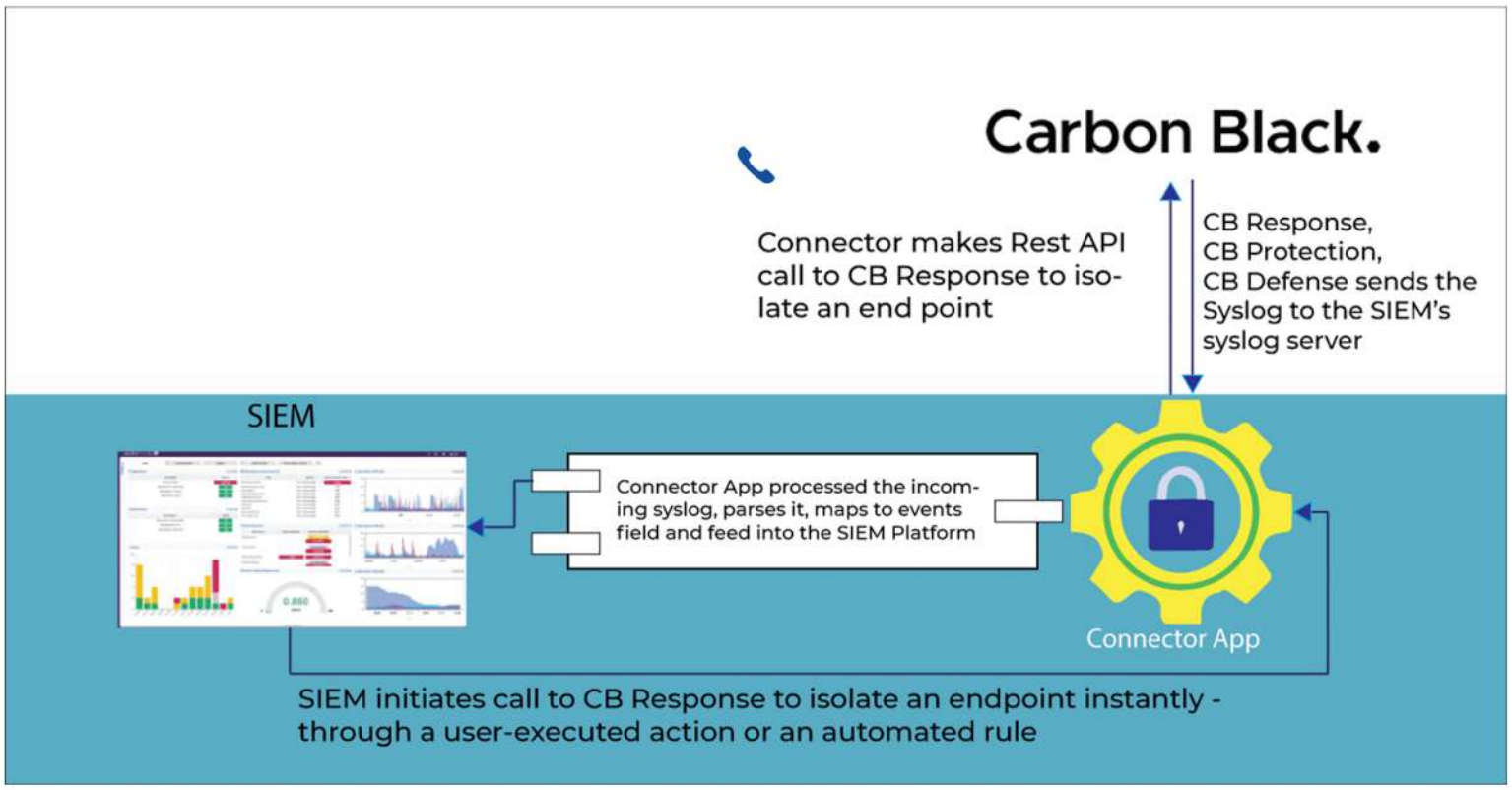
Carbon Black integration with SIEM Platform



Customer

Customer is a leading SIEM solution provider.
They provide a platform for companies to aggregate and act upon Threat Intelligence.

Requirement

Customer requested for the integration of their product with Carbon Black

Technology Solution

- Sacumen developed the Connector app that enhances the threat detection capabilities of SIEM platform by collecting and analysing log data from your Carbon Black applications and provides orchestration actions to streamline incident response activities.
- CB Response, CB Protection, CB Defense sends the Syslog to the SIEM's syslog server. Connector App processed the incoming syslog, parses it, maps to events fields and feed into the SIEM Platform
- SIEM initiates call to CB Response to isolate an endpoint instantly – through a user-executed action or an automated rule. Connector makes REST API call to CB Response to isolate an end point

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

+1 408 585 9982