

GREENTEA TECHNOLOGY

TRUSTED TECHNOLOGY ADVISORS

SOC-in-a-Box Explained

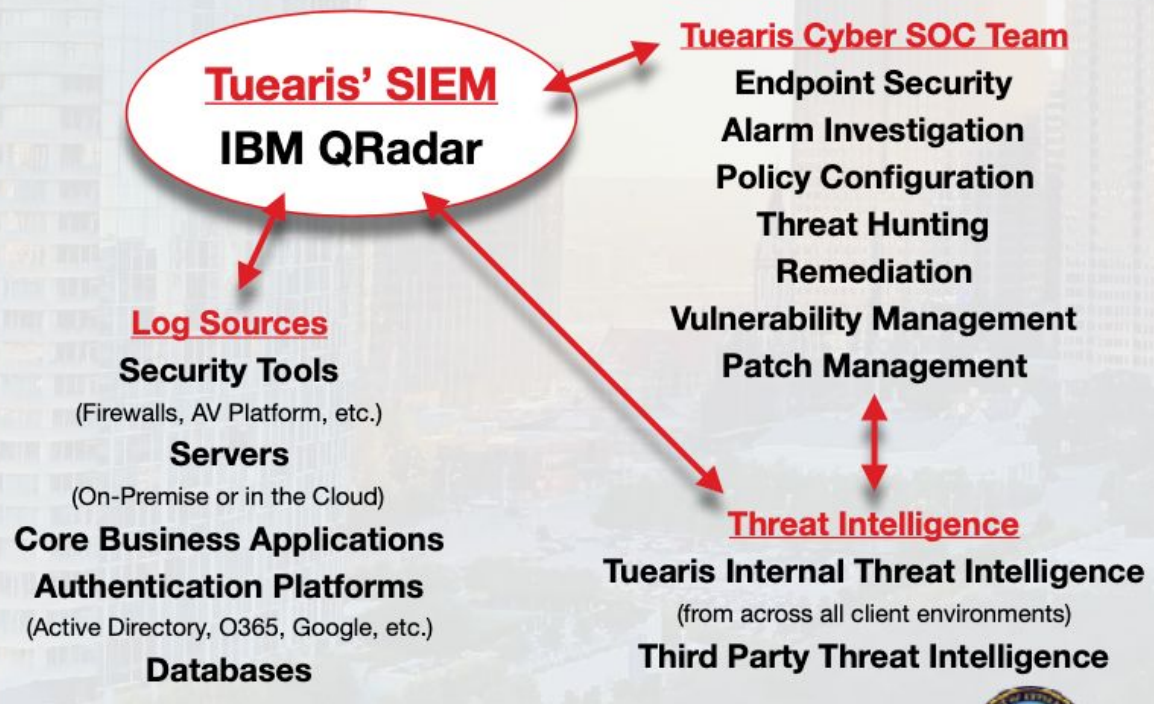
Observe. Protect. Respond.

What is a SIEM?

A Security Information and Event Management platform collects the logs produced by many sources in the environment, correlates that data and processes it through the Threat Intelligence and policies from the Security Operations Center (SOC). Leading SIEM technologies, such as IBM's QRadar, are even capable of identifying Zero-Day Threats since the platform hunts anomalous behaviors.

Policy configuration to reduce false positives and optimize the SIEM platform is an important part of the SOC's work as well as alarm investigation. The Tuearis SOC also performs endpoint protection by utilizing behavior based security platforms, Threat Hunting, manages a Threat and Vulnerability Management program in order to hunt unpatched vulnerabilities, a Patching Program to mitigate threats, remediation, and Incident Response.

Tuearis Cyber is more than a managed SIEM; we are your cybersecurity team for observation, protection, and response of your network!



Security. Managed.

