Quadrant Sagan Solution Implementation and Commencement of Service

Quadrant's all-inclusive Sagan Solution offers real-time, 24/7/365 identification, validation and ultimately notification on malicious activity at both the log and network levels. Quadrant deploys its Sagan technologies, along with the 24/7/365 monitoring, alerting, reporting and overall management. Ensuring the easiest procurement process, Quadrant offers all hardware, software, services and support for one monthly fee, with no upfront costs. Quadrant believes that the people + product approach of its solution delivers the most effective protection of customer data.

Implementation

Overview

Once the decision has been made to implement the Sagan solution, whether as a Proof-of-Concept (POC) or full implementation, there are a number of considerations and subsequent actions that will be required to commence with the Sagan service. Primary consideration will be the number and placement of sensors for both network packet analysis using a 'Packet Inspection Engine', or PIE, and log analysis via a 'Log Analysis Engine', or LAE.

In order to ensure a smooth implementation and to minimize client resources, Quadrant provides a Client Liaison/ Project Manager to coordinate the efforts of the client's team and the Quadrant Implementation Team. Much of the hardware setup and installation will be completed by the Quadrant Implementation team, though some actions, such as directing log traffic to the LAE, will need to be completed by the client's information systems/ network team.

Determining Number, Type and Placement of Sensors

Number of Sensors

The number of sensors required is determined, primarily, by the physical nature of the client's infrastructure. For example, if there are three physical locations that have Internet points of presence which are determined to need PIE sensors, then there will need to be three physical PIE sensors, one at each location. There will also be at least one log analysis and storage sensor/appliance. However, if the traffic volume allows, this appliance may function as one of the PIE sensors as well. Determining the number of sensors is usually done by Quadrant through review of a supplied scoping document and discussion with the client network team.

Type of Sensors

The type and specifications of the sensors are determined by volume of traffic each machine is expected to analyze and, in the case of log storage, the volume of log data expected for a fifty-three week period. The number of ports that are required for each sensor is a function of the number of PIE input ports that are required plus one port for use as a Quadrant management port. Finally, the type of connection (copper or fiber-optic cabling, etc.) and the expected bandwidth needs to be provided to Quadrant. It is important to note that the ownership and responsibility of maintenance of the sensors remains with Quadrant, freeing the client from dedicating additional resources to the sensor hardware.

Placement of Sensors

Through the discussions with the client network team, scoping document and additional network documentation, the best placement of the sensors will be determined. Typically, the PIE sensors will be placed physically close to core infrastructure. Where applicable, the PIE sensors are usually placed behind the firewall in order to cut down on alerts triggered by detections that would ultimately be stopped by the firewall.

Preparation of Sensors

When the sensor hardware has been received by Quadrant, the implementation team will have the sensor operating system(s) and all required software loaded. They will then have the machines configured for the specific client sites. Towards this purpose, the Quadrant team will request the IP addresses that each sensor will have, as they will be needed for remote access for maintenance, etc.. The client will not be required to load any software or configure the sensors.

Installation of Sensors

The installation of the sensors is typically done by the Quadrant implementation team. This includes physical transport, mounting into the server rack, physical connection and boot-up of the hardware. Once the sensor is in place, the implementation team will verify that the Quadrant Security Operations team is able to access the device, and that they are receiving alerts. This on-site portion of the implementation typically takes only a couple of hours per sensor. It should be noted that, in the advent of unforeseen issues, it is important that the client's network resources are present or can be made available during the installation process.

Directing Log Traffic to LAE for Analysis

Quadrant's log analysis and storage process requires that logs for all relevant assets are forwarded to the LAE log sensor. This typically includes servers, firewalls, switches as well as other network devices. The LAE appliance is designed to analyze and store logs in Syslog format.

Syslog

For almost all non-Windows devices, logs can be directed to the LAE device in Syslog format, without any additional software. The client network team will need to configure each of these devices to forward logs to the LAE device. Once complete, the Quadrant team will be able to provide confirmation that logs are, in fact, being received from each device.

Windows Agent

Windows devices do not have a native option for sending logs in syslog format. Fortunately, Quadrant provides a custom Syslog agent that is delivered in an install package (MSI) that does not require restart. Though most Windows devices are 64bit, it is important that the client inform Quadrant of the existence of any 32bit devices, as this will require a separate installer package. As with non-Windows devices, the Quadrant team will verify that logs are being received from each of the Windows devices.

Additional Network and Systems Considerations

Network Traffic Analysis

In order to ensure that Quadrant sensors will not disrupt network traffic, even in the event of failure, Quadrant sensors are not placed 'in-line', but rather, receive traffic mirrored via span. Network impacts are addressed during the implementation kick-off meeting, prior to span configuration.

Log Analysis and Storage

Windows Agent Install

As stated before, an agent must be installed on each Windows device in order for those devices to forward logs to the LAE log sensor. Quadrant continually tests to ensure that there are no server issues with the addition of the agents.

Log Traffic/Network Load

Finally, it should be noted that the transmission of logs to *any* central log repository will increase the network load by the volume of log data to be stored. However, this is not typically a significant burden over the existing traffic load.

Implementation Action Items at a Glance

The table below provides an at-a-glance view of the steps and responsible parties for a typical Sagan implementation.

Implementation Action	Responsible Parties	Week #
Scoping Document Completed and Delivered	Client	1
Meeting to Determine Sensor Placement and Configuration	Set up by Quadrant Client Liaison/PM	1
- **Schedule Meeting**		1
- **Meet**	Client and Quadrant Implementation Team	1
- **Provide IPs for Sensors**	Client	1
- **Provide Cabling and Rack Specs for each Sensor (Copper/Fiber?)**	Client	1
- **All 64bit Windows Servers (if Applicable)?**	Client	1
- **Determine Install Dates**	Client and Quadrant Implementation Team	1
Procure Hardware	Quadrant Implementation Team	1
Configure Sensors	Quadrant Implementation Team	2-3
Build and Deliver Windows Agent MSI (if Applicable)	Quadrant Implementation Team	2-3
Install Hardware	Client and Quadrant Implementation Team	2-3
Configure PIE Spans	Client	
Load Windows Agent on Windows Devices	Client	2-3
Direct Syslog to LAE Sensor for Non-Windows Devices	Client	2-3
Verify Visibility by SOC of Logs and Network Traffic	Client and Quadrant Implementation Team and SOC	2-3
Configure and Provide Sagan Console Access	Quadrant Implementation Team	2-3
Go Live	Client and Quadrant Implementation Team and SOC	2-3

Sagan Implementation

Full Deployment

Client: _____

Primary Contact: _____

Phone: _____

Email: _____

Scope

Dates of Contract

TBD _____ To TBD _____

Total Devices

Devices/Sensors	Physical Devices	Sensors
Log Analysis and Storage Engine and Repository (LAE)		
Packet Inspection Engine (PIE)		

Assets

Contracted Assets to be Monitored: _____

Locations

Location	LAE Count	PIE Count

Additional Services

Additional Services	Number	Frequency

POC (If Applicable)

Dates of POC

TBD To TBD

POC Devices

Devices/Sensors	Physical Devices	Sensors
Log Analysis and Storage Engine and Repository (LAE)		
Packet Inspection Engine (PIE)		

Assets

Assets to be Monitored During POC:

POC Locations

Location	LAE Count	PIE Count

Notes/Additional Information

Notes/Additional Information

Network and Website Information

Company Domains

Subnet Ranges Where Network Traffic Should be Seen by PIE Devices	
PIE	**Subnet Ranges** (Can be sent in an attached document if needed.)

Quadrant Device Specifications

Device 1	
Device Name	
Location	
Address	
LAE or PIE**	
Size**	
Management IP	
Subnet/Netmask	
Gateway	
Primary DNS	
Secondary DNS	
Tunnel Port**	
Tunnel Protocol**	
ILO Interface**	
ILO IP*	
ILO Netmask*	
ILO Gateway*	

*Optional **Provided by Quadrant

Device 2	
Device Name	
Location	
Address	
LAE or PIE**	
Size**	
Management IP	
Subnet/Netmask	
Gateway	
Primary DNS	
Secondary DNS	
Tunnel Port**	
Tunnel Protocol**	
ILO Interface**	
ILO IP*	
ILO Netmask*	
ILO Gateway*	

*Optional **Provided by Quadrant

Device 3	
Device Name	
Location	
Address	
LAE or PIE**	
Size**	
Management IP	
Subnet/Netmask	
Gateway	
Primary DNS	
Secondary DNS	
Tunnel Port**	
Tunnel Protocol**	
ILO Interface**	
ILO IP*	
ILO Netmask*	
ILO Gateway*	

*Optional **Provided by Quadrant

Device 4	
Device Name	
Location	
Address	
LAE or PIE**	
Size**	
Management IP	
Subnet/Netmask	
Gateway	
Primary DNS	
Secondary DNS	
Tunnel Port**	
Tunnel Protocol**	
ILO Interface**	
ILO IP*	
ILO Netmask*	
ILO Gateway*	

*Optional **Provided by Quadrant

Device 5	
Device Name	
Location	
Address	
LAE or PIE**	
Size**	
Management IP	
Subnet/Netmask	
Gateway	
Primary DNS	
Secondary DNS	
Tunnel Port**	
Tunnel Protocol**	
ILO Interface**	
ILO IP*	
ILO Netmask*	
ILO Gateway*	

*Optional **Provided by Quadrant

Quadrant Device Specifications – Additional Devices

Device	
Device Name	
Location	
Address	
LAE or PIE**	
Size**	
Management IP	
Subnet/Netmask	
Gateway	
Primary DNS	
Secondary DNS	
Tunnel Port**	
Tunnel Protocol**	
ILO Interface**	
ILO IP*	
ILO Netmask*	
ILO Gateway*	

*Optional **Provided by Quadrant