SOC Management Platform

Technical Overview

assuria

Automated SOC Configuration & Management. Virtual Multi-tenant SOC.
Integrated Protective Monitoring & Secure Configuration Services.

Innovative new SOC Management Platform

Assuria cyber defence solutions are used by hundreds of end user organisations around the world, as well as major Security Operations Centre (SOC) providers to deliver critical Managed Cyber Defence Services. Assuria technology is proven in the most demanding environments.

Now, we have developed a highly scalable, resilient, heavily automated and easy to manage SOC Management Platform to make the delivery of these world class, defence grade cyber security services to SME's a practical reality for the first time.

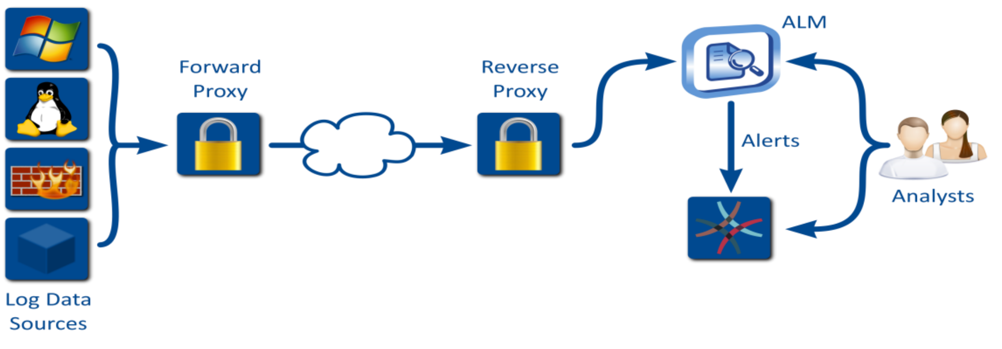
Most SME's would not normally employ these services or licence the solutions themselves because of cost and a lack of internal cyber security skills. The Assuria SOC Management Platform aims to change this. The focus of this innovative new platform has been on ease of use, speed of deployment, scalability, persistence and lowest possible operating costs.

The Assuria SOC platform is tightly integrated with Assuria's award winning cyber security defence software solutions, including *Protective Monitoring*, *Vulnerability Assessment*, *File Integrity Monitoring* and *Secure Configuration*, as used by hundreds of customers in more than 20 countries worldwide.

This platform allows smaller, but capable local companies, to run world class, low cost SOC operations built on a complete technology platform provided by Assuria. We believe that most SME's would much prefer to receive these essential Managed Security Services from trusted local providers.

This document describes the basic technical architecture and data flows for SOC partners.

Basic data flow diagram – single customer



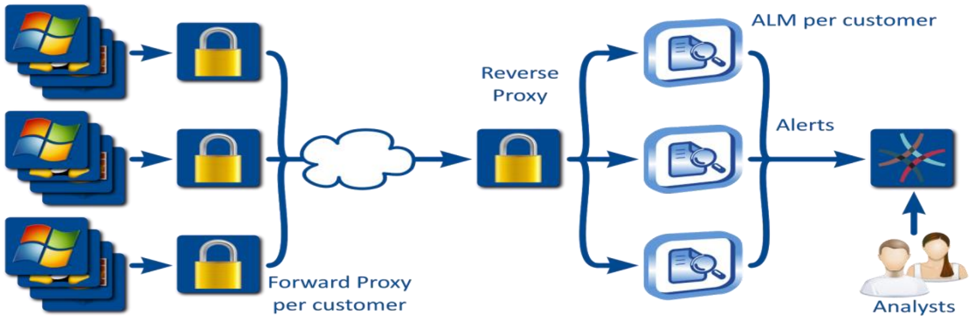
Sources of customer log data are shown on the left-hand side: [Note: with Assuria's ALM SIEM, log data can be collected from almost any system, device, application, database etc.]

- Logs flow through a proxy on the customer site across the Internet to a proxy in the SOC, then onto an ALM SIEM instance
- The ALM SIEM instance creates a forensic audit trail for future investigations and then undertakes automated analysis and generates alerts into a central ticketing system
- Analysts review alerts and instigate investigations, consulting ALM SIEM as appropriate.

*Note, ALM SIEM ensures that all log data transfer is secure end-to-end. The Forward Proxy is provided for networking convenience and optimisation.

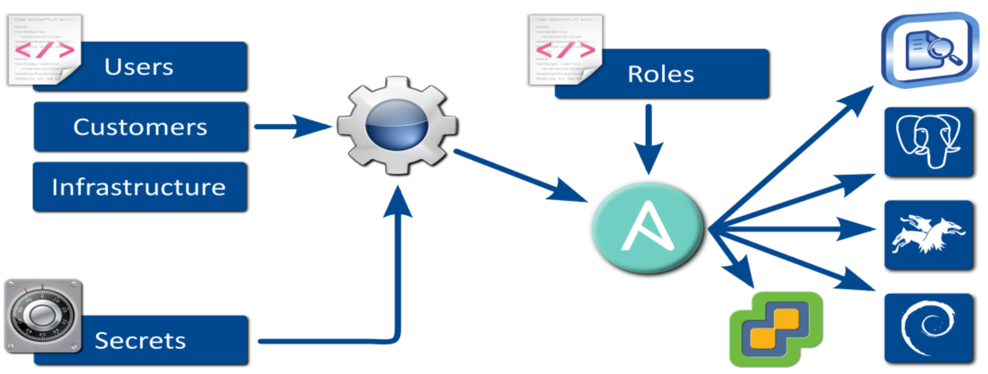
© Copyright 2017 Assuria Limited. All rights reserved

Basic data Flow - Multiple customers



Multiple customer (multi-tenancy) principles:
- Each customer has their own forward proxy
- The reverse proxy in the SOC selects the customer’s ALM SIEM server
- Each customer has their own ALM instance: no risk of mixing up customers’ data. Separation is normally via a dedicated VM per customer, but separate physical servers or separate disks can be provided if required
- The ticketing system (OTRS by default) is a single-pane-of-glass for analysts
- Analysts can drill-down to the relevant ALM SIEM instance(s)
- This is made possible (i.e. multiple ALM instances) because deployment is fully automated (see the automation process below)
- Excellent horizontal scalability is assured, because the SOC doesn’t have one enormous SIEM instance containing and trying to manage every customer’s data within it.

SOC Automation Process:



Process to deploy a customer virtual SOC instance (V-SOC):

Input configuration files list (top left group) contains:
- User details (i.e. SOC analysts)
- Customer details (for each customer)
- Customer infrastructure to be monitored (VMs, VM servers, VLANs, IP addresses etc.)

Secrets files (bottom left) contains:
- Sensitive information (e.g. cryptographic keys) held in a strongly-encrypted store.

Cog wheel: this is the deployment software, which takes the above inputs and processes them to create Ansible input.

Ansible (the stylised A circle) deploys the entire SOC, using the processed input and a set of role definitions. A “role” is a function performed by a VM (e.g. proxy, ALM server). Core SOC components include:
- VMware instances
- Base operating system (Debian) instances
- Kerberos (single sign-on)
- Database (PostgreSQL) instances (per customer)
- ALM SIEM instances (per customer)
- Pre-configured OTRS ticketing system + Other miscellaneous VMs (not shown on slide).

Assuria Ltd. Reading Enterprise Centre, The University of Reading, Reading, Berkshire RG6 6BU U.K.
W: www.assuria.com E: info@assuria.com Tel: +44 118 935 7395 Fax: +44 118 935 7330

© Copyright 2017 Assuria Limited. All rights reserved.