Huntsman®
Defence-Grade Cyber Security

On-premise Huntsman Enterprise SIEM:

Flexibility advantages for LogRhythm and QRadar customers

Following the acquisitions of the IBM QRadar cloud business by Palo Alto (a cloud native endpoint/XDR vendor) and LogRhythm by Exabeam (also cloud native and endpoint focussed) there is understandable concern about the future of the existing SIEM solutions, specifically the on-premise/software-based versions of both the QRadar and LogRhythm SIEMs.

SIEM users who specifically bought those solutions (in many cases instead of cloud-hosted endpoint solutions) are naturally worried about their chosen technology going end-of-life, lacking in investment or being steered towards the new vendor's cloud platforms that are focussed on endpoint detection, rather than the wider infrastructure monitoring and compliance coverage of SIEM.

This briefing note focusses on the flexibility and functionality of on-premise SIEM that existing users will be familiar with.

" I worry about the flexibility and fit of cloud-based SIEM solutions "

1. **Users who specified an on-premise SIEM find a move to cloud-based SIEM/XDR/UEBA unwelcome**

   This could be due to worries around security, sovereignty, control, flexibility, cost or simply the network architecture and Internet accessibility. Huntsman's on-premise SIEM means faster processing, control over data storage and costs, no need to move data in/out of providers systems and full compliance with local security rules.

2. **Users want support for wider use cases than just endpoint detection**

   UEBA and EDR/XDR solutions focus on endpoint detection – logs, activity, running processes, local user settings and configuration. Endpoint solutions are not designed for wider collection of data for correlation and compliance purposes. These facilities are a bolt-on or afterthought.

   A SIEM, such as Huntsman, is better suited to wider infrastructure sources, network devices, firewalls, servers, devices, physical systems and applications.

3. Users struggle to meet compliance use cases/requirements

XDR solutions focus on threat detection rather than compliance so may not collect data from all sources or retain it for the duration compliance rules mandate. Not all data is captured, some might only be used locally only to identify issues with no centralised, remote storage.

Huntsman SIEM is fully capable of collecting/retaining/reporting on data for compliance purposes.

4. Users prefer a local SIEM even if they have, or are planning, to use an MSSP

SIEM users with MSSPs that want the flexibility to move provider will have to migrate data from their old provider to a new one. One solution is an in-house/on-premise platform the MSSP operates to deliver security monitoring services or as a local repository for use in incident handling.

Huntsman SIEM can be managed by an MSSP, transferred as a unit, or the data can be extracted and retained for archive purposes. This saves the effort, inconvenience or cost of moving data from one MSSP/cloud provider and to another each time contracts change.

5. Users want visibility of their internal controls status for alerting/threat enrichment

If an existing SIEM contains configuration and vulnerability information to support threat detection and incident management, this will need to be factored into the cloud-based XDR requirements. Users may not want this data available externally, if it is even possible.

Huntsman SIEM leverages inbuilt modules to monitor and report on security controls and leverage these within SIEM alerts to add context and risk-based enrichment to alerts.

6. Users don't want to move to the cloud (or realise later it's not right for them)

Moving between cloud services is often difficult as there is little incentive for outgoing providers to allow free/easy data migration. Support for existing on-premise solutions will decline over time, both Exabeam and Palo Alto are pure cloud-plays. So SIEM users will be forced to move to a cloud solution – even if it is not suitable – and will need to clarify how they can extract data from it.

Moving from an on premise SIEM where you have control over the information in its entirety to a cloud provider that you haven't chosen (and may not be suitable) is therefore a risk. Huntsman SIEM keeps all customer data on-premise under their control and can be managed by a third party/MSSP if desired.

Contact Huntsman Security for a free migration consultation

Huntsman Enterprise SIEM is a solution delivered on premise, on hardware or virtualised, or for deployment in a customer's own private cloud. It provides easy migration and a stable upgrade path for users of traditional SIEM platforms who are worried about the cost implications of data storage, movement or migration to/from cloud-bases SaaS platforms.

e ukinfo@huntsmansecurity.com t +44 845 222 2010 huntsmansecurity.com

Huntsman®