Castellum Labs

WHITE PAPER 2022

Buying SIEM .
The Important "30"

Castellum Labs

WHITE PAPER 2021

SIEM and Security Monitoring is a strangely crowded market.

Loads of products and technologies and options to choose from. And, each one of them claiming to have one score up over their competition in terms of feature, adoption, scalability, coverage and costs. It can be confusing, real confusing!

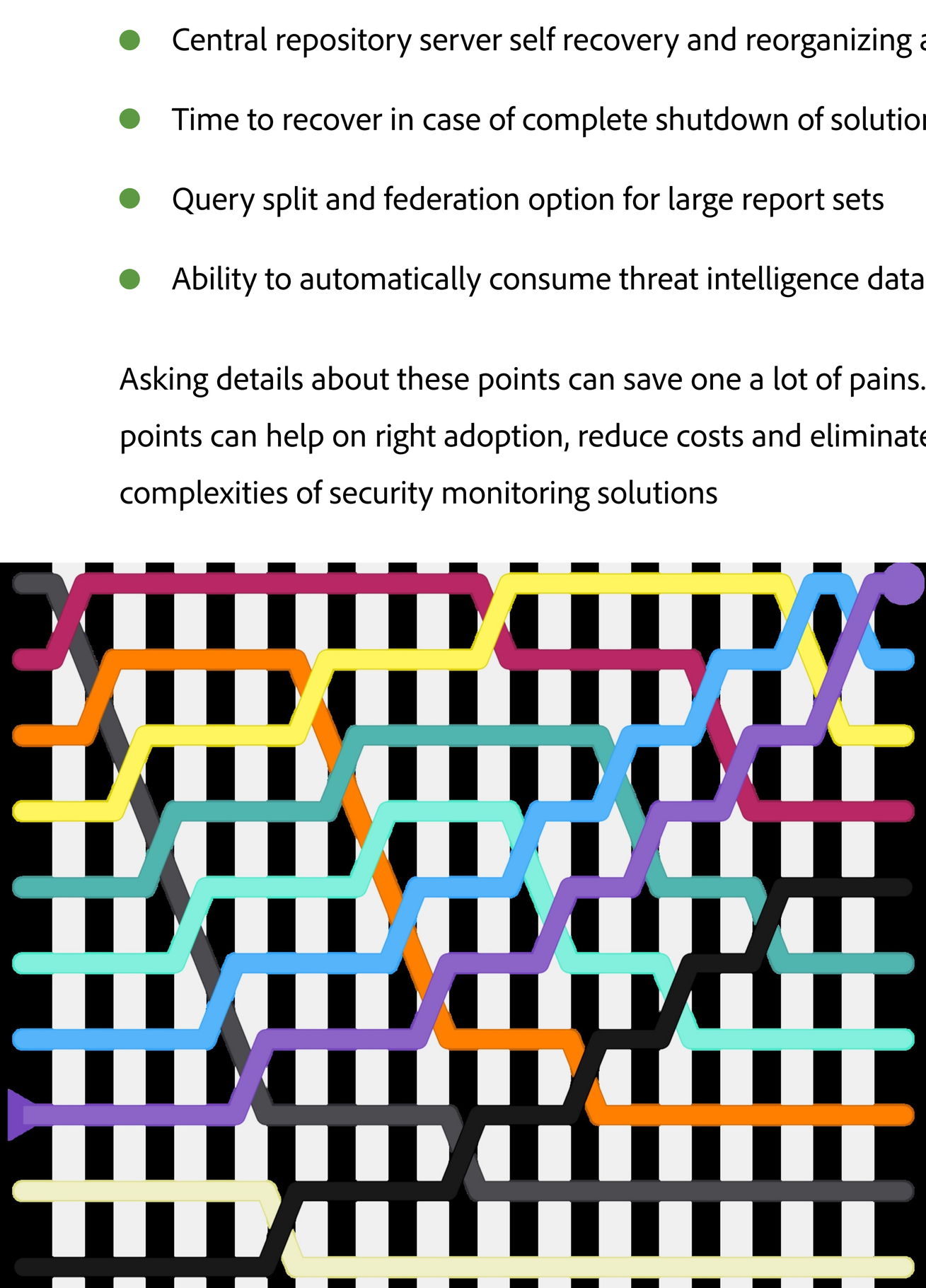
Here is a list of most important questions and/or points. All of 30!

> *"Ask These Questions to Your Security Vendor"*
>
> *Let them pass the "Walk on Fire" Test!*

- Auto-recovery and self healing capabilities of collection agents/mechanism
- Remote operations options for all collection agents/technologies
- Out of box support for log sources and types, including version variances
- Parsing tool and parsing widgets for customizations to events mapping
- Log/Event filtering options at the collection point/agent
- Compression ratios as data travels from log source to central repository
- Event enrichment with real time context at collection point
- Event enrichment with stored context during its journey to central store
- Event selection options for real time correlation dispatch
- Realtime correlation abilities and time-window of real-time correlation
- Event data volumes for variety of log source and event types
- Event throughput support for normal and peak volume generation
- Event caching at the collection source and in real time store location
- Built-in rule templates for correlation and alerting

- Out of the box alerts, specifically for operations related issues
- Virtual groups at central store for segregation of event types in static store
- Physical storage structure at central store, i.e., files and their types
- Built-in archival abilities and granularity of restore options
- Event/log data export options in the tool across the board
- Out of box device and source specific security reports
- Out of box alert library for security scenarios and attack vectors
- Operational console for incident monitoring and reporting
- Workflow support for incident handling, follow up and closure
- Advanced search abilities in the stored event/log data
- Ability to directly consume data from third party products/repositories
- Federated deployment options for central log stores
- Central repository server self recovery and reorganizing abilities
- Time to recover in case of complete shutdown of solution or failure
- Query split and federation option for large report sets
- Ability to automatically consume threat intelligence data

Asking details about these points can save one a lot of pains. Appropriate details on these points can help on right adoption, reduce costs and eliminate or reduce operational complexities of security monitoring solutions



Key Services Areas

Application Security

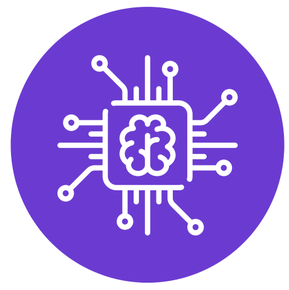
Managed AppSec Programs

Cloud Security

Cloud Security Design & Governance

SOC Monitoring

Managed Detection and Response



Threat Intelligence

Contextual Threat Intel & Hunting

Our Technology Platforms

appFORT

Continuous Application Security

watchOUT

Darkweb Monitoring

threatNIXD

Next Gen SOC Monitoring

Continuous Unified View of your Cyber Security

Get in touch with us to know more on our Cyber Security offerings

WHITE PAPER 2021

Castellum Labs

+91 97009 70397

info@castellumlabs.com

www.castellumlabs.com