Modernizing SIEM Solution for Secureview FCU

Evaluating and Procuring an Enterprise-Grade SIEM Solution

SECURE SENTINELS™
Always Secured

Sufian Adnan, Yash Devani, Saraj Mollah, Guled Warsame

Case Study

SFCU suffered a data compromise incident.

Incident report shows that current SIEM solution cannot suffice the SFCU’s IT and cybersecurity operations

In-depth information of SFCU’s IT Environment

300 Workstations

100 Onsite Servers

25 Offsite Servers Windows/Linux

200 Company Laptops

In Depth Information of SFCU’s Networking Devices

- 30 Cisco Routers & Switches
- 100 Wireless Access Points
- 2 Palo Alto Gateway Firewall, IDS and IPS

In Depth Information of SFCU’s Applications

- Online Banking – Cloud
- HR Application – SaaS: Workday
- CRM Application – Salesforce
- Finance Application – Onsite: PeopleSoft

In Depth Information of SFCU’s WFH Setting

Employees work from home 3/5 days in a work week

Selected employee groups can log in from anywhere within USA and Canada

20 Physical Branches across South Carolina

Three SIEM Solutions

01

Splunk Enterprise

- **Flexible Architecture**
- **Rich App Ecosystem**
- **User-Friendly Interface**
- **Adaptive Scaling**

Three SIEM Solutions

01

Splunk Enterprise

•Flexible Architecture
•Rich App Ecosystem
•User-Friendly Interface
•Adaptive Scaling

02

IBM Qradar

•Advanced Threat Intelligence
•QRadar Advisor
•Pre-Built Use Cases:
•Integrated Risk Management

Three SIEM Solutions

01

Splunk Enterprise

•Flexible Architecture
•Rich App Ecosystem
•User-Friendly Interface
•Adaptive Scaling

02

IBM Qradar

•Advanced Threat Intelligence
•QRadar Advisor
•Pre-Built Use Cases:
•Integrated Risk Management

03

LogRhythm

•SmartResponse™ Automation
•Compliance Automation Suites
•Built-In Case Management
•Security Analytics Platform

The Cons of Splunk

Complex Licensing: The licensing model of Splunk can be intricate and potentially lead to unexpected costs as the organization scales.

Resource-Heavy: Splunk's resource-intensive nature might require additional hardware investment to maintain optimal performance.

Customization Effort: Achieving customization might demand significant effort, impacting time-to-value and project timelines.

splunk>®

The Cons of IBM QRadar

Steep Learning Curve: QRadar's extensive features and capabilities could lead to a steeper learning curve, affecting initial usability.

Dependency on IBM Ecosystem: Integration with other non-IBM tools or applications might pose challenges and require workarounds.

High Expertise Requirement: Due to its complexity, QRadar implementation and management might require specialized expertise, raising operational costs.

The Cons of LogRhythm

Integration Complexity: While LogRhythm excels in diverse data collection, integrating with certain non-standard applications could be more challenging.
Resource Impact: Similar to the others, LogRhythm's resource utilization might influence system performance during high data periods.
Initial Investment vs. Use Case: The initial investment might be higher compared to the specific use cases the organization seeks to address.

SECURE SENTINELS™
Always Secured

Type a Message

SECURE SENTINELS™
Always Secured

Type a Message

SentinelGPT

Recommendation: IBM QRadar

1. **Advanced Capabilities**: QRadar excels in swift threat detection and response.
2. **Integrated Risk Management:** Ensures comprehensive security and compliance.
3. **Hybrid Environment:** seamless fit for SFCU's hybrid IT landscape, encompassing on-premises, Azure, and SaaS systems.
4. **Enhanced Threat Intelligence:** Equips with up-to-date threat data.
5. **Immediate Insights**: Quick setup, essential for addressing gaps.
6. **Efficient Automation:** Proactive anomaly identification.
7. **Investment in Expertise:** Specialized skills enhance effectiveness.

What SIEM should we invest in for our case?

References

- https://www.splunk.com/en_us/products/enterprise-security.html
- https://www.ibm.com/products/qradar-siem?utm_content=SRCWW&p1=Search&p4=43700074872917532&p5=e&gclid=Cj0KCQjwldKmBhCCARIsAP-0rfy6JCglfKhysmeZkFT0f4Yvk-KrwBIg16DJbyE8pIx1xmO96UmvvXoaAmvxEALw_wcB&gclsrc=aw.ds
- https://logrhythm.com/schedule-demo-ppc/
- https://www.gartner.com/reviews/market/security-information-event-management