DESIGNING A SIEM PRODUCT REVIEW FRAMEW

PURE SECURE SOLUTIONS

Prepared For:
Professor Hendra T. Hendrawan

Our Team

Aparna Pavitra Palem
Arshjeet Kaur
Deep Shikha
Kajal Sodhi
Mahtabul Bari
Rahulkumar Vaniya

Table of Contents

Selection Quadrant 01

Quadrant Descriptions 02

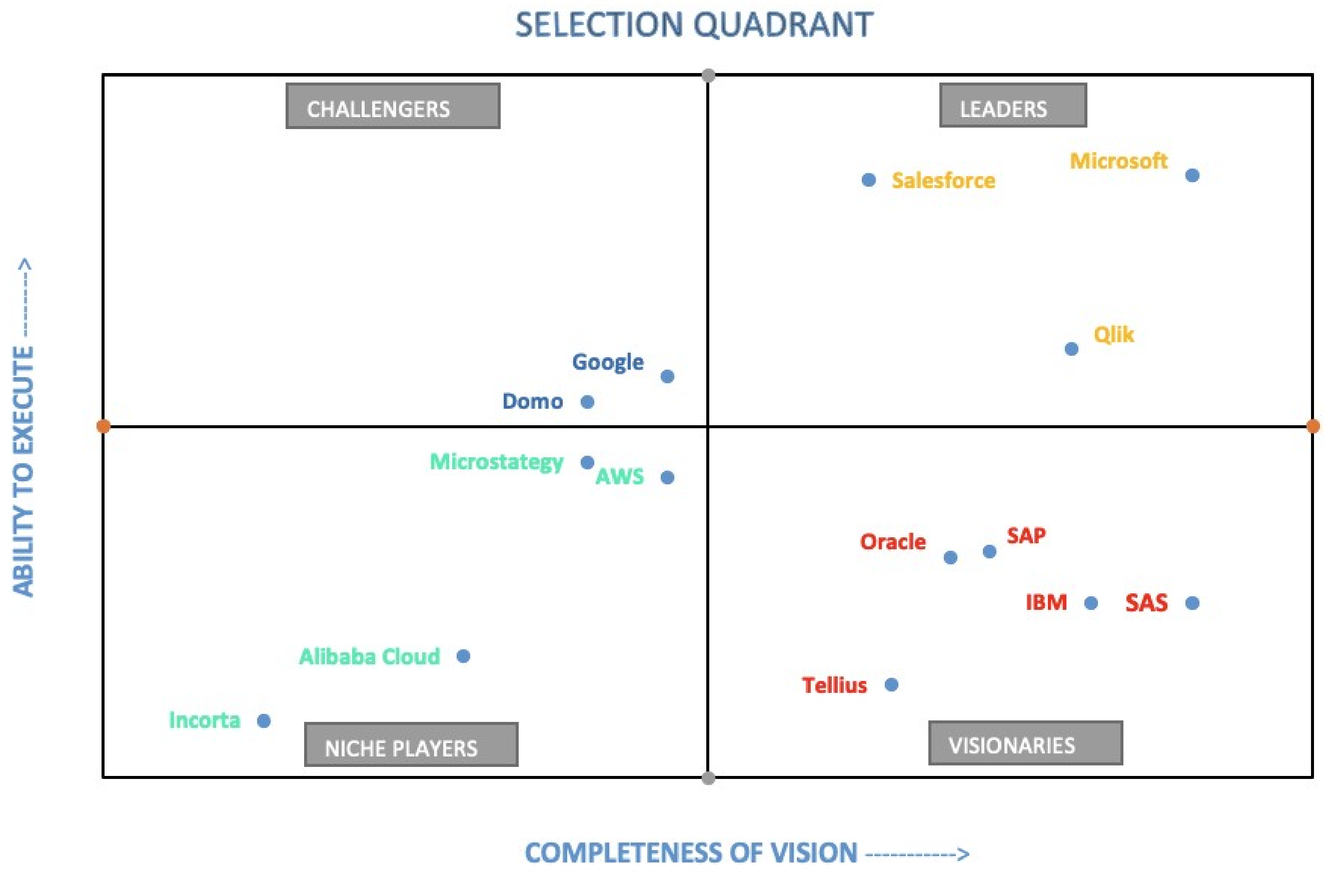
Evaluation Criteria 03

04 Key Features Of Effective SIEM Solutions

05 References

06 Our Team

Selection Quadrant



Quadrant Descriptions

- ***Leaders* -** Leaders show evidence of superior vision and execution for emerging and anticipated requirements.

- ***Challengers* -** Challengers typically have strong execution capabilities, as evidenced by financial resources and a significant sales and brand presence.

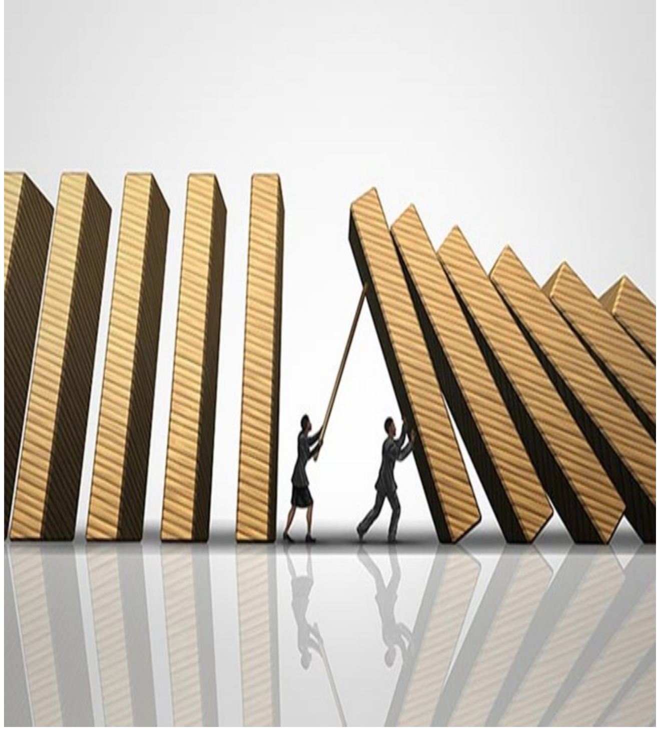
Quadrant Descriptions

- ***Visionaries* - **Visionaries provide products that are a strong functional match for the SIEM market's general requirements, but have less ability to execute than leaders.

- ***Niche Players* - **Niche Players focus on a particular segment of the client base or may provide a limited set of SIEM capabilities.

Evaluation Criteria

Ability to Execute	Completeness of Vision
• Product or Service • Overall Viability • Sales Execution/Pricing • Market Responsiveness/Record • Marketing Execution • Customer Experience • Operations	• Marketing Strategy • Sales Strategy • Offering (Product) Strategy • Vertical/Industry Strategy • Innovation • Geographic Strategy



Key Features Of Effective SIEM Solutions

Real-time log and data collection

Log correlation and threat intelligence

Real-time notification and alerting

Reporting and dashboards

Security Workflows and Incident response

Real-time Log And Data Collection

A SIEM can ingest logs from an array of IT devices and external sources, including servers, security devices, applications, operating systems, and more.

Why? When logs are collected, the security team obtains rich insights into the overall network activity and health.

Recommendation: Medium
Implementation: Medium complexity

Log Correlation And Threat Intelligence

The tool should be able to correlate security events and detect threats based on the correlation equations given.

Why? Security analysts need log correlation to understand precisely what is happening in the network. This solution ingests logs from various sources and correlates it to threat intelligence feeds.

Recommendation: high
Implementation: medium complexity

Real-time Notification And Alerting

A security analyst can set up triggered events based on specific data points found during the log collection and correlation phases

Why? Real-time notification and alerting by the SIEM enables analysts to respond to attacks much faster than before and potentially decrease your Mean-Time-to-Detect (MTTD) and Mean-Time-to-Respond (MTTR).

Recommendation: highly
Implementation: Low complexity

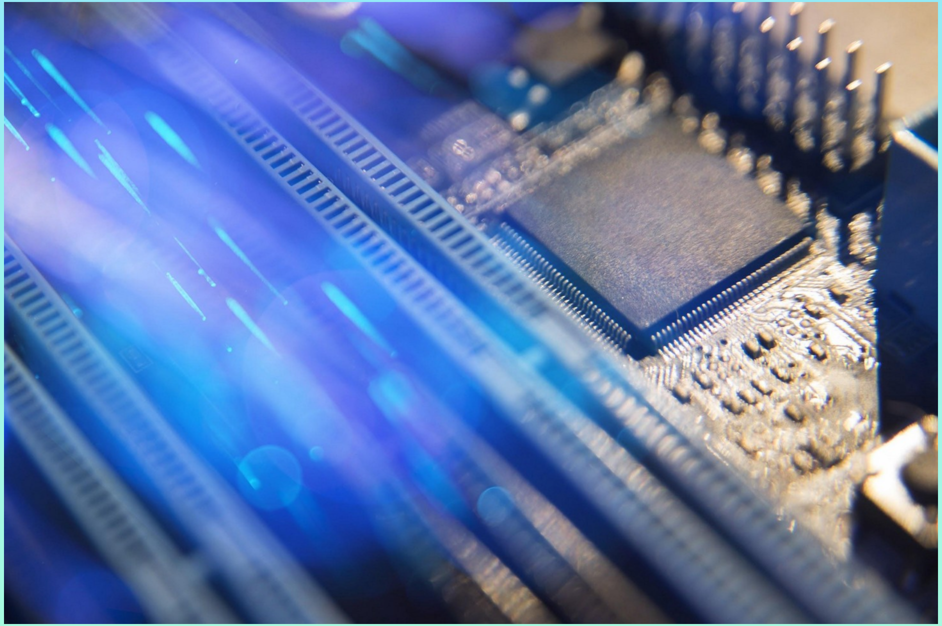
Compliance Reporting

It is based on a centralized infrastructure and provides valuable and concise information for company management.

Why? This information enables the security team to address critical, but also ordinary decisions related to the security management.

Recommendation: High
Implementation: High complexity

Security Workflows And Incident Response



A security workflow allows our security team to visualize the security monitoring stages, the incident response process, and the events that occur across each of these stages

Why? These are important in showing us where your security team spends its time and where improvements can be made

Recommendation: High
Implementation: Medium complexity

References

1. Keary, T. (2022, July 4). *13 best SIEM tools in 2022: Vendors & solutions ranked (Paid & free)*. Comparitech. https://www.comparitech.com/net-admin/siem-tools/
2. Bhatia, R. (2020, May 25). *Your 6-Point guide for evaluating Next-Gen SIEM tools*. Spiceworks. https://www.spiceworks.com/it-security/siem/deep-dive/guide-for-evaluating-siem-tools/
3. Kavanagh, K., Bussa, T., & Collins, J. (2021, June 29). *Magic Quadrant for Security Information and Event Management*. Gartner | Delivering Actionable, Objective Insight to Executives and Their Teams. https://www.gartner.com/doc/reprints?id=1-26OLSQ2N&ct=210630&st=sb
4. *The must-have SIEM features for advanced threats*. (2020, May 28). Cipher. https://cipher.com/blog/the-must-have-siem-features-for-advanced-threats/
5. *9 things to keep in mind while choosing a SIEM solution*. (2022, June 1). SISA. https://www.sisainfosec.com/blogs/9-things-to-keep-in-mind-while-choosing-a-siem-solution/
6. *ManageEngine Log360*. (n.d.). ManageEngine Log360. https://www.manageengine.com/log-management/siem/siem-functions.html

```
url_easy_setopt(conn, CURLOPT_URL, url);
 != CURLE_OK)
(stderr, "Failed to set URL [%s]\n",
 false;
 = curl_easy_setopt(conn, CURLOPT_FOLLOWLOCATION,
(code != CURLE_OK)
(stderr, "Failed to set redirect option [%s]\n",
return false;
code = curl_easy_setopt(conn, CURLOPT_WRITEFUNCTION,
if (code != CURLE_OK)
{
  (stderr, "Failed to set writer [%s]\n",
```

Thank You!!!