Select and Implement a SIEM Solution

Optimize IT security management and simplify compliance with SIEM tools.

Info-Tech Research Group, Inc. is a global leader in providing IT research and advice. Info-Tech's products and services combine actionable insight and relevant advice with ready-to-use tools and templates that cover the full spectrum of IT concerns.
© 1997-2015 Info-Tech Research Group Inc.

INFO~TECH
RESEARCH GROUP

Use this blueprint and accompanying Vendor Landscape to support your SIEM selection and implementation

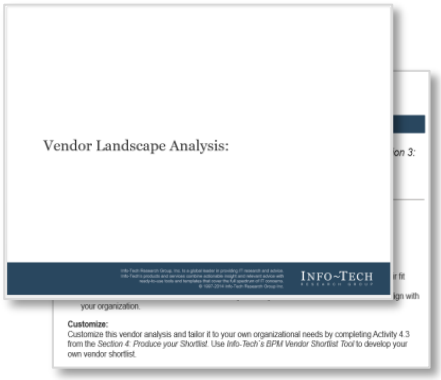
Phase 1 **Launch your SIEM selection project and collect requirements**

Phase 2 **Select your SIEM solution**

Phase 3 **Plan your SIEM implementation**

Use the project steps and activity instructions outlined in this blueprint to streamline your selection process and implementation planning.

Save *time and money, and improve the impact of your SIEM procurement* by leveraging Info-Tech's research and project steps.



Use Info-Tech's SIEM V*endor Landscape Analysis* contained in Phase 2 of this project *to* support your vendor reviews and selection. Refer to the use-case performance results to identify the vendors that align with the requirements and solution needs identified by your earlier project findings.

Info-Tech Insight

Not everyone's process needs are the same. These differences drive out different categories and niches within the Security Information and Event Management (SIEM) market space. Understand your own business's processes and the unique technical and functional requirements that accompany them. Use your own set of requirements to determine the SIEM solution that best fits your organization.

Our Understanding of the Problem

This Research Is Designed For:

- ✓ IT or Security managers who wish to implement a Security Information and Event Management (SIEM) solution at their organization.
- ✓ Organizations that want additional security and visibility into their network activity.
- ✓ Organizations under stringent compliance obligations.

This Research Will Help You:

- ✓ Select an appropriate SIEM solution based on vendor research.
- ✓ Create an implementation roadmap.
- ✓ Define your SIEM architecture.
- ✓ Measure the continued value of your SIEM.

Outcomes of this Research:

- ✓ A formalized selection process to identify which SIEM solution is best for your organization to gain full visibility and analyze activity across your network.
- ✓ An evaluation of the current SIEM products and vendors that can be customized to your organization through the Vendor Shortlist tool.
- ✓ A completed selection process through the use of a Request for Proposal (RFP) template and a Vendor Demo Script to ensure that you are obtaining the correct information.
- ✓ An implementation plan that includes the overall defining architecture of your final SIEM solution.

Executive Summary

Situation

- Security threats continue to be more sophisticated and advanced with each day, with the majority often going completely undetected.
- Organizations are usually scrambling to keep up and implement new security controls to protect themselves, which adds a new layer of complexity.

Complication

- With the rise of Advanced Persistent Threats (APTs) and insider attacks, it becomes extremely difficult for security staff to detect all the risks.
- Many IT and IT Security staff are already stretched thin by keeping track of many different security technologies that already exist.

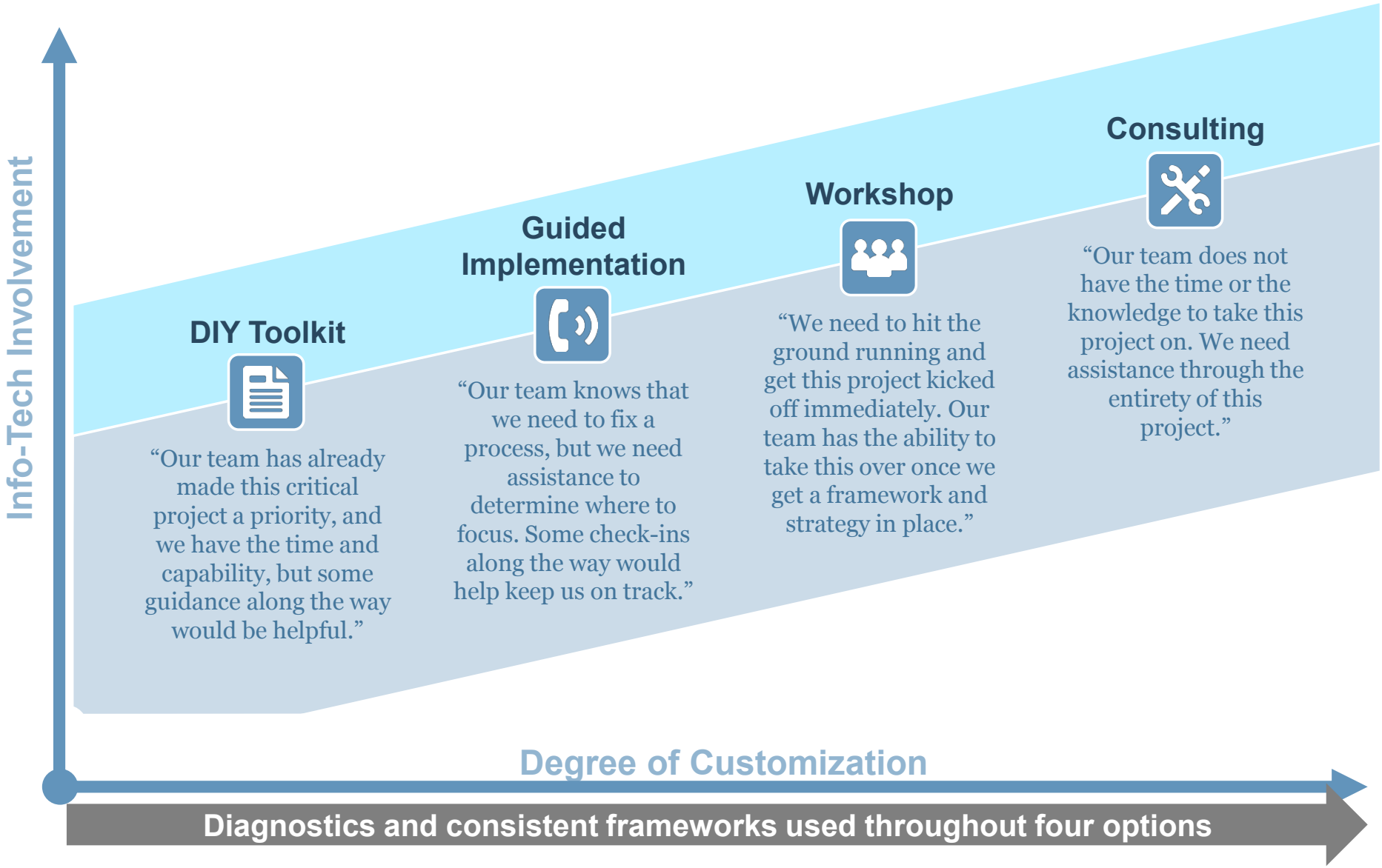
Info-Tech Insight

1. **A SIEM isn't for everyone.** Review your appropriateness and create a formalized SIEM selection process to determine your needs.
2. **A SIEM is not your only answer.** Proper implementation and ongoing use is needed in order to maximize the benefits of a SIEM solution

Resolution

- SIEM can provide a great deal of visibility into an organization's networks and identify extremely sophisticated threats that may have otherwise been hidden.
- By integrating with other security technologies, the SIEM solution can act as a single window into the threats and possible breaches that your organization is facing.
- SIEM technology is also becoming more advanced with the capability to use advanced correlation engines as well as big data analytics to provide insightful analysis and forensics into the overall data.
- Use Info-Tech's research to gain more insight into which vendors and products are appropriate for your business, and follow our implementation to ensure that you are set up for success.

Info-Tech offers various levels of project support to best suit your needs



Select and Implement a SIEM Solution – Project Overview

	1. Launch the SIEM selection project and collect requirements	2. Select a SIEM solution	3. Plan the SIEM implementation
Best-Practice Toolkit	**1. Assess value and identify fit.** *SIEM Appropriateness Tool* **2. Build the procurement team and project plan.** *SIEM Procurement Project Charter Template* **3. Identify the requirements for the SIEM.** *SIEM Use-Case Fit Assessment Tool*	**4. Produce the vendor shortlist.** *SIEM Vendor Landscape Analysis* *SIEM Vendor Shortlist and Detailed Analysis Tool* **5. Select a SIEM solution.** *SIEM RFP Template* *SIEM Evaluation and RFP Scoring Tool* *SIEM Vendor Demo Script*	**6. Create an implementation plan.** **7. Measure the value of the SIEM solution.**
Guided Implementations	Start with an analyst kick-off call to identify your fit for a SIEM. Identify staffing needs and build a project plan. Gather your business, security, and IT requirements.	Create a shortlist based on your needs. Review findings with analyst and create your RFP. Conduct a contract review and select your SIEM solution.	Create an implementation plan. Set up your SIEM capabilities. Hand over your SIEM solution to your security operations.
Onsite Workshop	**Module 1:** Launch the SIEM selection project and analyze SIEM requirements	**Module 2:** Shortlist SIEM vendors and plan the procurement process	**Module 3:** Plan your SIEM implementation
	Phase 1 Outcome: • Launch your SIEM selection project. • Gather and align requirements between IT and business.	**Phase 2 Outcome:** • Shortlist your vendors based on your requirements. • Select a vendor after writing a successful RFP and reviewing the contract.	**Phase 3 Outcome:** • Plan the implementation of the SIEM solution and determine its evaluation.

GI and general value

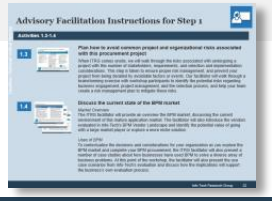
Phase	Measured Value
Phase 1: Launch the SIEM selection project and collect requirements	Cost to assess value and identify fit: • Consultant at $100 an hour for 4 hours = **$400** Cost to build your procurement team and project plan: • Consultant at $100 an hour for 40 hours = **$4,000** Cost to identify the requirements for your SIEM • Consultant at $100 an hour for 80 hours = **$8,000**
Phase 2: Select a SIEM solution	Cost to produce a vendor shortlist: • Consultant at $100 an hour for 40 hours = **$4,000** Cost to select your SIEM solution: • Consultant at $100 an hour for 40 hours = **$4,000**
Phase 3: Plan the SIEM implementation	Cost to create an implementation plan • Consultant at $100 an hour for 16 hours = **$1,600** Cost to measure the value of your SIEM solution • Consultant at $100 an hour for 8 hours = **$800**
Potential financial savings from utilizing Info-Tech resources:	Phase 1 ($12,400) + Phase 2 ($8,000) + Phase 3 ($2,400) = **$22,800**

Workshop overview

Contact your account representative or email Workshops@InfoTech.com for more information.

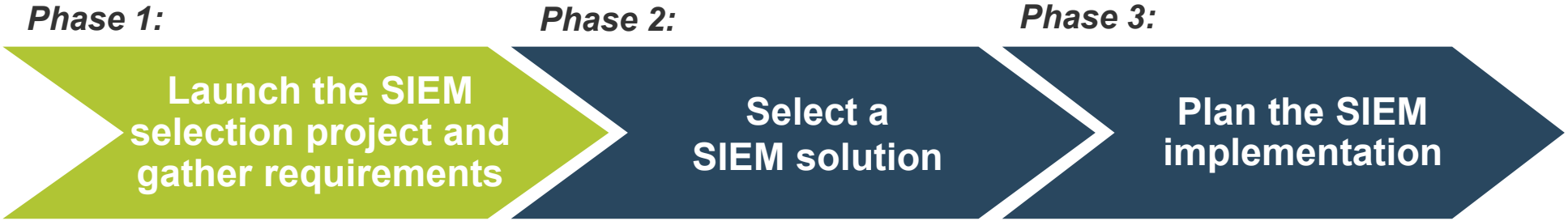
This workshop can be deployed as either a four or five day engagement depending on the level of preparation completed by the client prior to the facilitator arriving onsite.

Day 1	*Day 2*	*Day 3*	*Day 4*	*Day 5*
Preparation	**Workshop Day**	**Workshop Day**	**Workshop Day**	**Working Session**
Workshop Preparation • Review your current log management process. • Conduct interviews.	**Morning Itinerary** • Identify the drivers behind the SIEM procurement. • Complete the *SIEM Appropriateness Assessment Tool*. **Afternoon Itinerary** • Identify the scope and purpose of the project. • Select the staff resourcing. • Identify stakeholders.	**Morning Itinerary** • Create a project plan for SIEM selection. • Determine metrics to evaluate selection process. • Select the pilot. **Afternoon Itinerary** • Determine your use-case scenario by completing the *SIEM Use-Case Fit Assessment Tool.* • Analyze relevant Vendor Landscape use-case results. • Customize vendor analysis.	**Morning Itinerary** • Complete *SIEM Vendor Shortlist and Detailed Analysis Tool.* • Create and prioritize solution requirements. • Create an RFP to submit to vendors. • Evaluate RFPs received. **Afternoon Itinerary** • Create a demo script. • Discuss the SIEM implementation plan.	**Workshop Debrief** • Review documents. **Next Steps** • Analyst calls to provide guidance during the selection and implementation processes.



The light blue slides at the end of each section highlight the key activities and exercises that will be completed during the engagement with our analyst team.

Phase 1: Plan the SIEM implementation



Phase 1 outline

Call 1-888-670-8889 or email GuidedImplementations@InfoTech.com for more information.

Complete these steps on your own, or call us to complete a guided implementation. A guided implementation is a series of 2-3 advisory calls that help you execute each phase of a project. They are included in most advisory memberships.

Guided Implementation 1: Launch the SIEM Selection Project and Gather Requirements

Proposed Time to Completion: 2-4 weeks

Step 1: Assess the value and identify fit

Start with an analyst kick-off call:

- Identify your fit for SIEM – understand the value of investment.
- Assess the appropriateness.

Then complete these activities…

- Identify the drivers behind your organization's decision to invest in SIEM.
- Assess your organization's fit for an investment in SIEM.

With these tools & templates:

SIEM Appropriateness Tool

Step 2: Build your procurement team and project plan

Identifying staffing needs and build a project plan

- Determine the resourcing for your selection team.
- Create an overview of your plan.

Then complete these activities…

- Complete your procurement charter to have a thorough plan for completion.

With these tools & templates:

SIEM Procurement Project Charter Template

Step 3: Identify the requirements for your SIEM

Finalize phase deliverable:

- Review the findings of your requirements gathering.
- Identify security, business, and technical requirements.

Then complete these activities…

- Review the use cases for SIEM and perform a use-case assessment.
- Document your requirements as you continue to collect them

With these tools & templates:

SIEM Use-Case Fit Assessment Tool

Phase 1 Results & Insights:

- Identification of the value and appropriateness of SIEM to your organization.
- Creation of a project plan, with collection of requirements for the final solution.

Step 1: Assess the value and fit for SIEM

Assess value and identify fit

Build the procurement team and project plan

Identify the requirements for a SIEM

Produce a vendor shortlist

Select a SIEM solution

Create an implementation plan

Measure the value of the SIEM solution

This step will walk you through the following activities:

- 1.1: Understand the value of a SIEM solution
- 1.2: Assess your organization's fit for procuring SIEM
- 1.3: Avoid the pitfalls for your procurement project
- 1.4: Review the market overview for SIEM

Info-Tech suggests involving the following participants in this step of the project:

- Project Sponsor
- Project Manager
- Additional security analysts
- CISO

Outcomes of this step:

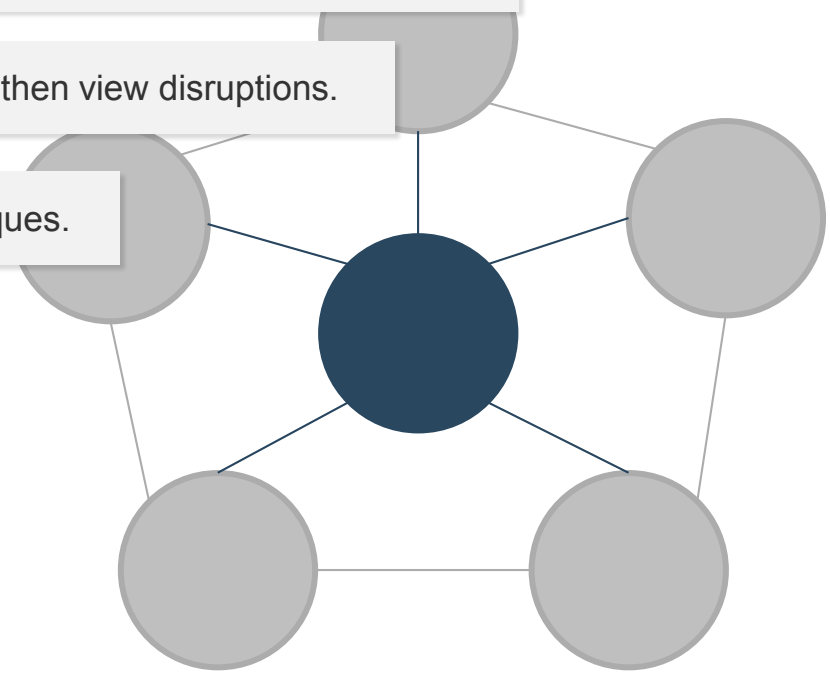
- Identification of the opportunities associated with SIEM
- Confirmation of the organization's suitability for a SIEM investment
- An appraisal of Info-Tech's Vendor Landscape market overview for SIEM
- Determination if now is the right time to proceed with this project

Leverage a SIEM solution to protect your organization

Security information and event management (SIEM) is a technology that allows a comprehensive view into an organization's information security.

A SIEM is a security technology that provides a security advantage for an organization or business. By looking across different data sources and locations, it provides one central point in which to analyze and correlate information. It defends against increasingly sophisticated and advanced threats by analyzing data and comparing it to previous trend analysis. Further, many SIEM products provide reporting templates for compliance issues and to provide overviews of the security state of your organization. SIEM works a single piece of security technology to provide all these security benefits in one package.

- Performs forensic analysis to dive into the security events, while integrating with other technologies.
- Defines a baseline based on the normal activity of an organization to then view disruptions.
- Uses basic correlation, aggregation, and normalization (CAN) techniques.
- Enables basic data management security and retention.
- Uses standard correlation tactics to view these threats.
- Presents information through dashboards and reports.



SIEM began as a combination of two separate technologies – a SEM and a SIM

1.1

Security Event Management (SEM)

SEM was a security technology that was meant to collect security events and attempt to provide real-time analysis on these events.

Security Information Management (SIM)

SIM analyzed previously collected security events and would attempt to find threats by correlation and analyzing this historical data.

Security Incident and Event Management (SIEM)

- SIEM grew from both of these products by offering correlation, analysis, and normalization of both real-time and historical security event information.
- By combining both these functionalities, it becomes possible to have a more comprehensive view of the security issues facing your organization.
- SIEM solutions are now seen as commonplace as more organizations are looking to adopt this into their infrastructure.

Review the business drivers behind SIEM adoption

SIEM was first designed to evaluate and asses your compliance and help track your requirements.

SIEM evolved to be used for complex networks and detection.

It is now able to provide holistic visibility as a means of overall risk reduction through a combination of threat and vulnerability mitigation.

43%

43% of companies had a data breach in 2014, with 60% having had more than one in the past two years, according to the Ponemon Institute.

94%

Kaspersky Labs has indicated that 94% of companies encountered cyber security issues in 2014.

By implementing SIEM solutions, organizations find that compliance and security become a top priority.

Business Drivers

Regulatory compliance

Risk management

Lack of strong security controls

Sources: Ponemon Institute, *2014 Cost of a Data Breach Study*.
Kaspersky Lab, *IT Security Risks Survey 2014: A Business Approach to Managing Data Security Threats*.

Look for these main capabilities from your SIEM solutions

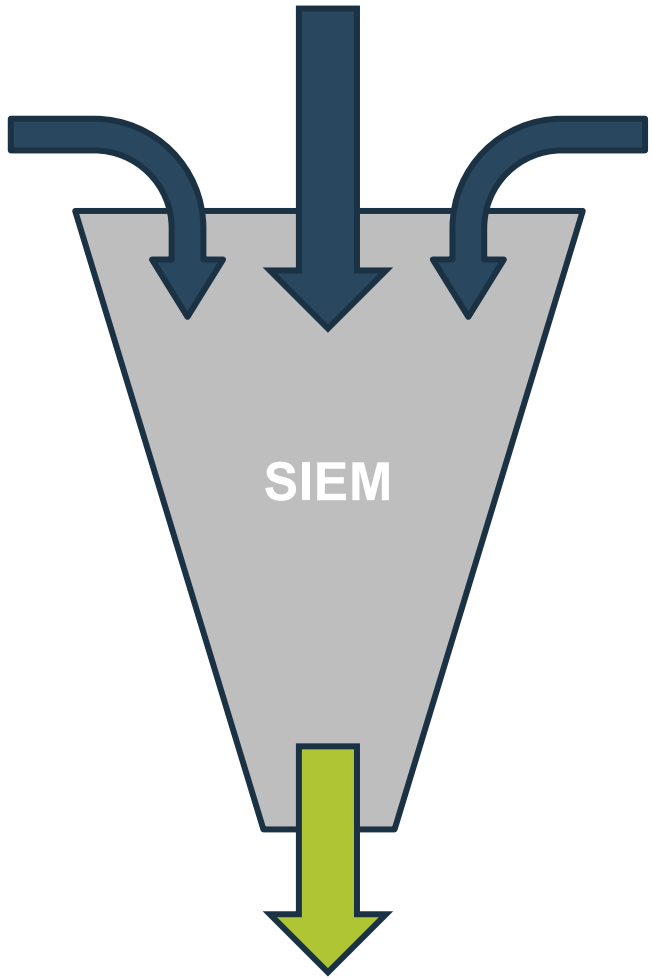
Organizations are typically looking for their SIEM solution to do the following:

Ability to aggregate
SIEM products are able to collect security information and events from different sources and feeds into a common platform, which can later allow for easier correlation and analysis. This allows different events to be found easily on one platform.

Ability to report
As security threats occur, there is the need to report on these threats and determine where these threats originate with other details.

Ability to detect
SIEM products should be able to analyze the data in your system in real-time. More often than not, it is not possible to review your data at a later stage.

Usability of the solution
As security events become more complex and technologies more advanced, with budgets remaining stagnant, SIEM products need to be able to provide quicker value to less trained individuals.



Case Study: Use a SIEM to monitor the internal activities of your system

Firstmark Credit Union
San Antonio, Texas

Company description: Regulated financial services company
Number of branches: 14
Customers served: Over 93,000

Source: LogRhythm, *Case Study: Firstmark Credit Union Uses LogRhythm to Monitor Internal Activities*
Note: This case study is for illustrative purposes of describing the implementation of a SIEM, and is not an endorsement of LogRhythm's product.

Situation

- Since opening in 1932, Firstmark has grown to become one of the largest financial institutions in Texas.
- Along with notable growth, Firstmark has been targeted for attack by hackers looking to gain members' personal and financial information.
- There was strong security around the perimeter, but if an attacker was already in the system, it was difficult to find these events.

Action

- Security managers and administrators collected logs from many difference advices.
- Firstmark determined that a SIEM would be the best tool to monitor their user activities.
- They enabled their solution to monitor and alert for a wide range of user activities such as creating new accounts, installation of new software, and even users exceeding a number of logins.

Future

- Since the implementation of the SIEM, Firstmark has found that it has improved correlation of events with significant events being displayed on the dashboard.
- Reporting has also improved considerably, especially in the time to create one.
- Further, the dashboard has allowed security managers to drill down and find the causes of various security incidents.

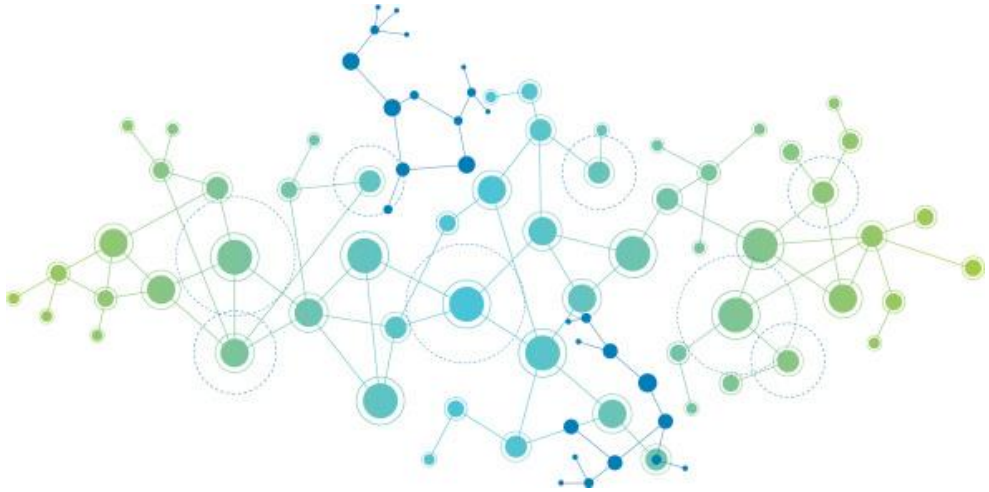
Use Info-Tech's research and methodology to ensure that your SIEM selection and implementation will be smooth

Start your project by examining drivers behind a SIEM solution and review the appropriateness.

Anyone looking to purchase a SIEM product must understand what they want and need from this technology. Many are quick to get any SIEM product and assume that it will satisfy their requirements, while it may not be the correct choice for them. Others may find greater value in the capabilities of another security technology rather than a SIEM. This can also go beyond what your peers at similar organizations are doing. As each company has its own unique processes and internal controls, their requirements become very specific and can differ widely from that of others in the same industry.

Various questions need to be asked:

- What compliance obligations need to be met? Do reports need to be generated behind these?
- What risks are you looking to identify?
- How will your security team deploy and implement a SIEM product in the organization?
- How many full time employees will be dedicated to the process?
- What is the implementation timeline for the product?



Collecting all these requirements can be extremely time consuming and difficult to do. Use Info-Tech's research and methodology to make this process easier.

Identify the drivers behind your SIEM procurement agenda

1.1 1 hour

Understand the drivers that are motivating your own organization's SIEM procurement to ensure that the implemented technology provides returns in the critical areas identified.

Instructions

1. Book a meeting with the project's key stakeholders to outline the purpose of the future SIEM and the drivers behind this business decision.
2. Document plans to ensure that these drivers are taken into consideration and realized following implementation.

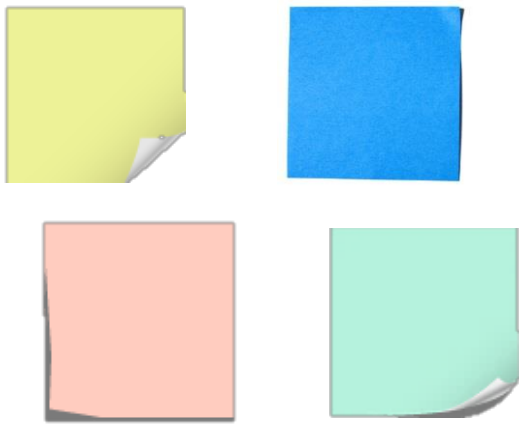
Materials

- Whiteboard and markers or sticky notes

Time Commitment

- One-hour brainstorming session

Improve



Reduce/Eliminate

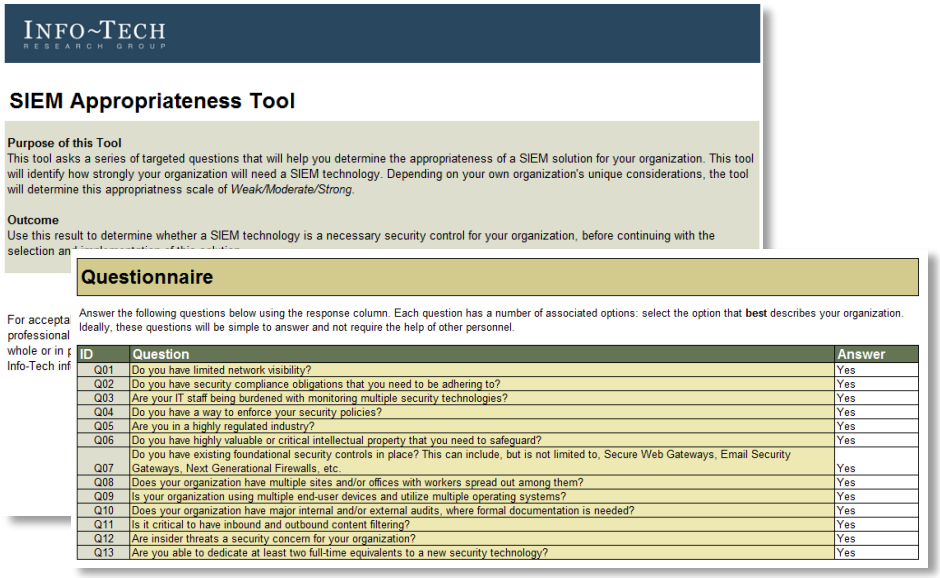
Determine the appropriateness of a SIEM solution for your organization

1.2 30 minutes

SIEM solutions can be costly and complex to implement in any organization and may also not be the best security technology for everyone. Use the *SIEM Appropriateness Tool* in order to determine if this security control is appropriate for your organization.

Steps

1. Use Tab 2 to answer simple questions about your company and its security.
2. Review your fit in Tab 3, which provides the overall appropriateness of a SIEM solution to your organization and provides relevant notes as well.



INFO-TECH RESEARCH GROUP

SIEM Appropriateness Tool

Purpose of this Tool
This tool asks a series of targeted questions that will help you determine the appropriateness of a SIEM solution for your organization. This tool will identify how strongly your organization will need a SIEM technology. Depending on your own organization's unique considerations, the tool will determine this appropriatness scale of *Weak/Moderate/Strong*.

Outcome
Use this result to determine whether a SIEM technology is a necessary security control for your organization, before continuing with the selection an

Questionnaire

Answer the following questions below using the response column. Each question has a number of associated options: select the option that **best** describes your organization. Ideally, these questions will be simple to answer and not require the help of other personnel.

ID	Question	Answer
Q01	Do you have limited network visibility?	Yes
Q02	Do you have security compliance obligations that you need to be adhering to?	Yes
Q03	Are your IT staff being burdened with monitoring multiple security technologies?	Yes
Q04	Do you have a way to enforce your security policies?	Yes
Q05	Are you in a highly regulated industry?	Yes
Q06	Do you have highly valuable or critical intellectual property that you need to safeguard?	Yes
Q07	Do you have existing foundational security controls in place? This can include, but is not limited to, Secure Web Gateways, Email Security Gateways, Next Generational Firewalls, etc.	Yes
Q08	Does your organization have multiple sites and/or offices with workers spread out among them?	Yes
Q09	Is your organization using multiple end-user devices and utilize multiple operating systems?	Yes
Q10	Does your organization have major internal and/or external audits, where formal documentation is needed?	Yes
Q11	Is it critical to have inbound and outbound content filtering?	Yes
Q12	Are insider threats a security concern for your organization?	Yes
Q13	Are you able to dedicate at least two full-time equivalents to a new security technology?	Yes

Call an analyst to review your results and dive into the appropriateness of a SIEM.

Look for this icon at the bottom right of slides where recording data into the tool is required.

Use Info-Tech's *SIEM Appropriateness Tool* to assess whether a SIEM solution is appropriate for your organization.

Avoid these pitfalls to ensure the success of your SIEM procurement

Identify risks and mitigation strategies early to improve your ability to perform a successful procurement and implementation of SIEM.

Common Pitfalls

Business Engagement

- Lack of stakeholder buy-in.
- Unrealistic expectations of how the tool will perform.
- Not engaging business stakeholders and identifying their business needs for the tool.
- Lack of consensus on the expectations and needs for a SIEM.
- Selecting a tool that is not user or business friendly.

Procurement Process

- Not following a clear and planned procurement process.
- Creating too many mandatory requirements.
- *Getting caught up with the bells and whistles*. Fancy features are nice, but look for the tool that meets your organization's specific needs.
- Not conducting a custom review of vendors based on the specific business requirements and organizational considerations.
- Selecting a demo or pilot that is not valuable to the business.

Optimize IT Procurement

Project Management

- Not identifying proper management and ownership of the procurement process.
- Not identifying the constraints and business requirements for the selection.
- Failing to properly transition from implementation to maintenance.
- Improper change management that makes the tool's integration into the live environment disruptive and riddled with incidents.

Create Project Management Success

Info-Tech Insight

Even if the organization's business landscape would benefit from SIEM, and the IT department has the maturity to manage a SIEM solution, a successful procurement and implementation is not guaranteed. Avoid the pitfalls related to business engagement, project management, software procurement, and implementation that could disrupt your SIEM selection and implementation project.

SIEM Market Overview

1.4

How it got here

- SIEM used to be two separate products: Security Event Management (SEM) and Security Information Management (SIM).
- SIEM was created initially as a compliance management tool. It had the ability to centralize, review, and report on log activity.
- Soon after, the ability to correlate logs was leveraged to provide threat detection and advanced intelligence tools in order to examine IT systems more closely.
- SIEM solutions were initially directed towards large enterprises with high volumes of data and resources. This changed as more and more SIEM vendors began offering products to the small and mid-sized market.
- SIEM products expanded use with integration into other security technologies in order to provide a holistic view into the security of an organization with the ability to push out commands and data to other systems.

Where it's going

- Advanced analytics will change the landscape of SIEM entirely and allow for the detection of complex and sophisticated security events.
- Organizations are looking to take advantage of big data and SIEM vendors are no different. More SIEM solutions will focus on leveraging and analyzing big data to provide superior results.
- Managed SIEM providers will continue to increase in demand for small and large organizations. Smaller organizations won't have internal resources or expertise to staff a SIEM. Larger organizations may not want to dedicate resources, or decide a provider has the necessary expertise they require.
- As organizations continue to grow larger and more diverse, the ability to scale in heterogeneous environments becomes more important as SIEM products will need to keep up with the advancing technology systems in organizations.

As the market evolves, capabilities that were once cutting edge become default and new functionality becomes differentiating. Basic forensic analysis capabilities have become a Table Stakes capability and should no longer be used to differentiate solutions. Instead focus on advanced detection methods and usability to get the best fit for your requirements.

SIEM vendor selection / knock-out criteria: market share, mind share, and platform coverage

1.4

- SIEM solutions continue to aggregate machine data in real-time for risk management through analysis and correlation to provide network event monitoring, user activity monitoring, compliance reporting, as well as store and report data for incident response, forensics, and regulatory compliance.
- For this Vendor Landscape, Info-Tech focused on those vendors that offer broad capabilities across multiple platforms and that have a strong market presence and/or reputational presence among mid- and large-sized enterprises.

Included in this Vendor Landscape:

- **AlienVault.** Provides a robust security management product with an impressive threat intelligence feed.
- **EventTracker.** While a smaller vendor, EventTracker provides a SIEM product for the resource-constrained.
- **HP.** One of the largest technology vendors in the market; provides a highly feature-rich SIEM solution in this VL.
- **IBM.** Provides strong event and log management and threat detection across networks and applications.
- **LogRhythm.** As a dedicated vendor, LogRhythm offers the most feature-rich product with the ability to adapt to trends.
- **Intel Security.** As a diverse and competitive vendor, Intel Security offers a strong and reliable SIEM product.
- **NetIQ.** Has a strong foundational SIEM offering with a competitive price point.
- **RSA.** Offers a highly advanced SIEM product garnered to large-scale, high-demand security organizations.
- **SolarWinds.** Offers a robust SIEM for resource-constrained organizations, with potential compliance needs.
- **Splunk.** As a big data software company, Splunk offers a very strong SIEM for high capacity and unique environments.

Use Info-Tech's vendor research and use-case scenarios to support your own organization's vendor analysis

 1.4

- This view of vendor and product performance provides multiple opportunities for vendors to place depending on their product and market performance. Selected use cases are based on market research and client demand.

Use Case	
Threat Management	Threat management is meant for highly security-conscious organizations that need to protect their data or intellectual property from advanced threats, whether internal or external.
Compliance Management	SIEM products can help organizations looking to pass their regulatory and industry framework audits and manage their multiple compliance obligations.
Management of Security Events	High-capacity and heterogeneous organizations that need to gain full organization visibility across high-rate information systems dispersed across geographic locations.
SIEM Small Deployment	Smaller and resource-constrained organizations will likely be looking for a simplified SIEM offering, with less advanced or additional features but still providing strong security insight.
Risk Management	Organizations are often looking to reduce their overall level of risk by implementing security controls that can help to protect their data and manage their obligations while providing risk visibility.

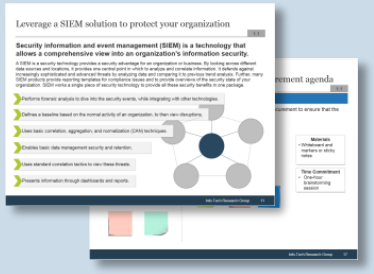
Workshop Scope for Step 1

Book a workshop with our Info-Tech analysts:

- To accelerate this project, call us to book a workshop with an Info-Tech Analyst.
- **Call 1-888-670-8889** or email Workshops@InfoTech.com for more information.

Workshop Activities

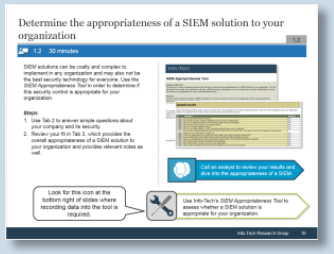
1.1



Identify the business drivers for investing in SIEM technology

An Info-Tech facilitator will work with the project sponsor, project manager, and additional business analysts (likely the core portion of your project team) to identify the business drivers that are motivating this SIEM investment. The facilitator will use a structured walkthrough to identify the specific drivers and how they relate to different lines of the business. The findings from this activity will be used as a reference throughout to ensure alignment between the business and the outcomes of the application implementation.

1.2



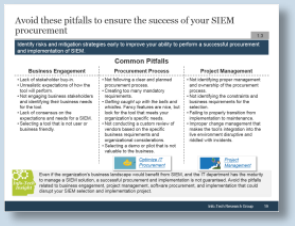
Review your organization's readiness for SIEM investment

An Info-Tech facilitator will review the *SIEM Appropriateness Tool* results, created by your organization, with your project team. This is done to confirm your organization's readiness for investing and successfully leveraging a SIEM suite. The facilitator will identify your current readiness and provide recommendations for initiatives that will help to best prepare your organization for security information and event management.

Workshop Scope for Step 1

Workshop Activities

1.3



Plan how to avoid common project and organizational risks associated with this procurement project

When Info-Tech comes onsite, we will walk through the risks associated with undergoing a project with this number of stakeholders, requirements, and selection and implementation considerations. This step is taken to ensure proper risk management, and prevent your project from being derailed by avoidable factors or events. Our facilitator will walk through a brainstorming activity with workshop participants to identify the potential risks regarding business engagement, project management, and the selection process, and help your team create a risk management plan to mitigate these risks.

1.4

Discuss the current state of the SIEM market

Market Overview

The Info-Tech facilitator will provide an overview of the SIEM market by discussing the current environment of this mature application market. The facilitator will also introduce the vendors evaluated in Info-Tech's SIEM Vendor Landscape and identify the potential value of going with a large market player or exploring a more niche solution.

Uses of SIEM

To contextualize the decisions and considerations for your organization as you explore the SIEM market and complete your SIEM procurement, the Info-Tech facilitator will also present a number of case studies about how businesses have used SIEM to solve a diverse array of business problems. At this point of the workshop, the facilitator will also present the use-case scenarios from Info-Tech's evaluation and discuss how the implications will support the business's own evaluation process.

Step 2: Build the procurement team and project plan

1. Assess value and identify fit
2. **Build the procurement team and project plan**
3. Identify the requirements for a SIEM
4. Produce a vendor shortlist
5. Select a SIEM solution
6. Create an implementation plan
7. Measure the value of the SIEM solution

This step will walk you through the following activities:

2.1: Identify the scope and purpose
2.2: Determine staff resourcing
2.3: Identify stakeholders and create a steering committee
2.4: Create a project plan
2.5: Determine metrics for your SIEM selection
2.6: Select a pilot for your project
2.7: Gain approval

Info-Tech suggests involving the following participants in this step of the project:

- Project manager
- Project sponsor
- Project steering committee (members) or key business stakeholders
- Security Analyst

Outcomes of this step:

- A completed and approved project charter for your SIEM selection project
- The creation of a granular project plan that outlines the steps and resourcing relating to each stage of the project
- An appraisal of the oversight and stakeholder engagement requirements for the project, including the creation of a steering committee or a plan for working with the organization's PMO or IT steering committee
- Launch of your SIEM selection project

Use Info-Tech's *SIEM Procurement Project Charter Template* to outline your own project plans

2.1 *SIEM Procurement Project Charter Template*

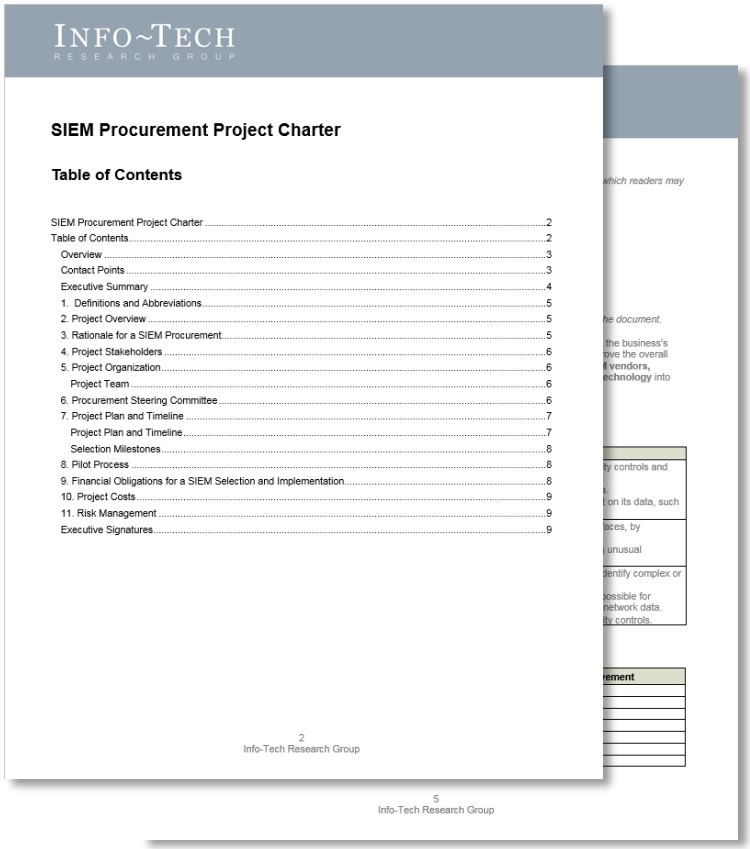
Use your charter as a project management tool. Use this master document to centralize the critical information regarding the objectives, staffing, timeline, budget, and expected outcome of the project.

Prior to project launch, prevent confusion by creating a clear plan that outlines the essential information and project steps.

Consider the common pitfalls, which were mentioned earlier, that can cause IT projects to fail. **Plan and take clear steps to avoid or mitigate these concerns.**

Build project management in at the beginning:

- Document the project manager and sponsor of the project
- Identify resourcing, including constraints
- Identify the project's timeline and document timeline
- If possible, document the budget for the project and the approved investment budget
- Outline the steps and outcomes of each stage of the project
- Plan how critical business stakeholders will be engaged and identify how their buy-in and support will be maintained


INFO-TECH RESEARCH GROUP

SIEM Procurement Project Charter

Table of Contents

2
Info-Tech Research Group

5
Info-Tech Research Group

Populate the relevant sections of *SIEM Procurement Project Charter* as you complete activities 2.1–2.7.

Identify the scope and purpose of your SIEM selection process

2.1 2 hours

As you begin your project, be upfront by outlining the purpose of the project and the rationale for a SIEM investment.

Instructions

Scoping Meeting

1. Hold a meeting with the project manager, project sponsor, and any other key personnel from IT or the business who understand the context and drive behind the SIEM procurement project.
2. Brainstorm and discuss, as a group, the purpose of the project and the organizational drivers supporting the business's decision to invest in SIEM.
    - Be specific, identifying the motivations regarding individual stakeholders and business units as they relate to specific business drivers.
3. Create a general statement that provides an overview of the purpose and scope of the project.

Follow-up Work

1. The Project Manager documents the meeting's findings in the charter's *Section 2. Project Overview*, and *Section 3. Rationale for SIEM Procurement.*

Materials

- *SIEM Procurement Charter Template*
- Whiteboard and markers

Time Commitment

1. One-hour meeting
2. One hour of additional documentation work (Project Manager)

Total Time: Two hours

Call an analyst to discuss and formalize the scope of your SIEM solution.

Determine the resourcing for your SIEM selection team

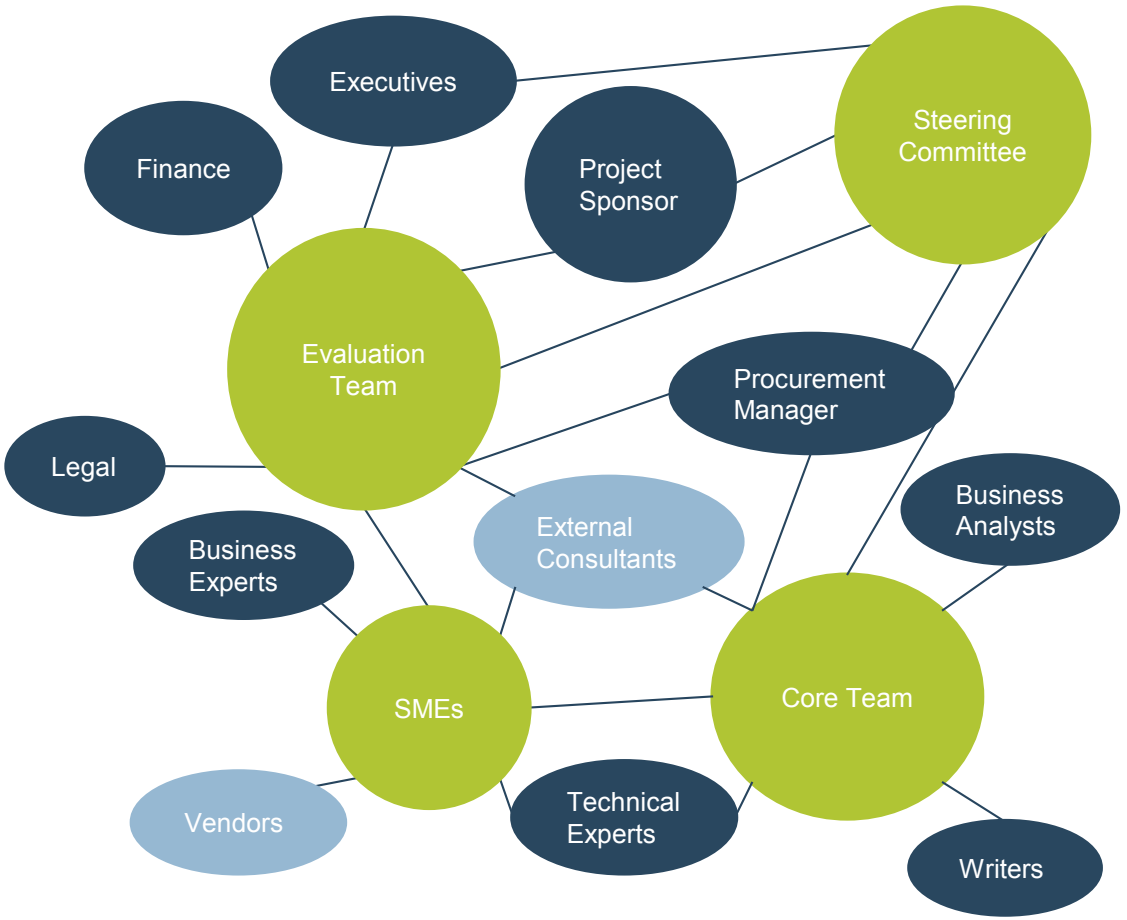
Info-Tech Insight

Don't create a project team that is isolated from the business and business users.
Create a cross-functional team that balances technical expertise, project management, vendor relations, and business perspective.

- Create project authority and accountability by clearly identifying the project sponsor and project manager.
- Identify the core project team and part-time staff who will be engaged at specific stages of the process.
- Identify the individual's role in the process and what stage of the project they are engaged in.

Keep Your Project in Perspective

Be realistic as you identify your staff resources. If an individual is already working full time on a number of projects, they may be only available for a part-time advisory role. Consider if this project warrants adjusting the department's current availability and resourcing plans.



Select the staff resourcing for your SIEM selection team

2.2 2 hours

Identify the staff who will be on the core team and evaluation team for the project.

Instructions

Resource Identification and Planning

1. Hold a meeting with the project manager, project sponsor, and SMEs who will likely be engaged in the project.
   - Have attendees arrive with an understanding of their upcoming schedules and any additional projects or considerations that might impede their involvement.
2. Identify the skills and roles that will be needed in order to fulfill the project.
3. Identify staffing allocations; ensure that the necessary skills and expertise are engaged with the project at the appropriate time.
4. Document staffing for the project in the project charter. *Consider creating a RACI chart around specific stages and tasks to ensure that responsibilities and expectations are clearly documented.*

Follow-Up Work

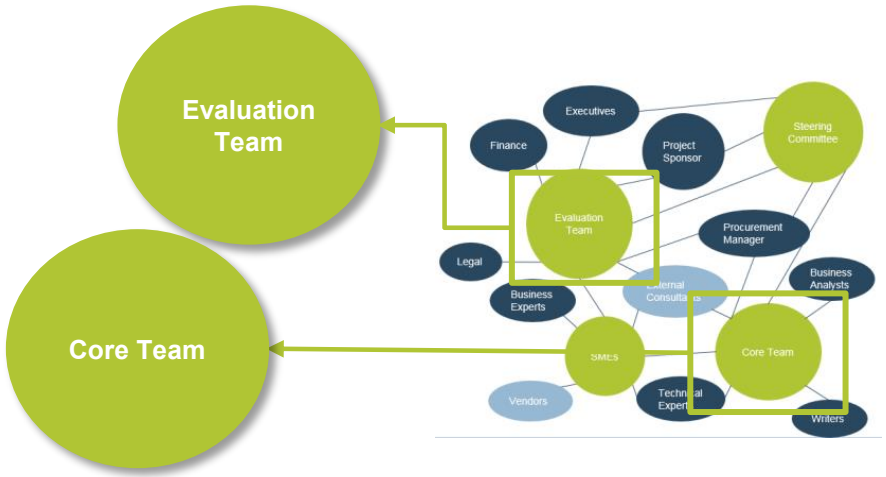
- If you have a large IT shop, distribute the staffing across IT and business management to ensure that the identified staffing does not conflict with any other projects or business functions.

Materials

- *SIEM Procurement Charter Template*
- Whiteboard and markers
- Staff schedules

Time Commitment

1.1 One-hour meeting
2.1 One hour of additional documentation work (**PM**)
Total Time: Two hours (plus confirmation time and effort)



Outline roles and expectations related to each project team to ensure project follow-through occurs

Staffing Plan
Build a RACI chart to outline the expectations regarding each project member at different stages of the project.

- **R** (Responsible), **A** (Accountable), **C** (Consulted), **I** (Informed)

Individual	Gather Requirements	Create Requirements List	Research Vendors	Shortlist Vendors	RFP	Analyze RFPs	Evaluate Vendors	Select Vendor	Plan Implementation	Demo Process
Project Manager										
Project Manager										
Steering Committee										
Business Rep										
SME										
Security Engineer										

Note: This template is just a sample of steps and activities to include when planning staff responsibilities.

Consider breaking the RACI charts down by stage of the process to create a more granular project plan.

Consult the recommended project steps in *Section 5. Project Plan and Timeline* to support your write-up.

Create a steering committee and identify the stakeholders whose support will be critical for securing investment approval

2.3 1 hour

Instructions

1. Hold a meeting to identify the stakeholders that should be included in the project's steering committee.
2. Finalize selection of steering committee members.
3. Contact members to ensure their willingness to participate.
4. Document the steering committee members and the milestone/ presentation expectations for reporting project progress and results.

Charter Sections

- *Section 6: Procurement Steering Committee*

Consider the following:

- Stakeholders whose approval and authority are necessary for budget approval and final selection
- Expertise of individuals
- Striking a balance between technical knowledge and business perspective

Info-Tech recommendation – who to include:

- Project sponsor
- Project manager
- Business rep(s)
- SMEs
- Executives or executive representation

If your organization has an established Project Management Office, rely on its standard procedures and steps to manage the oversight and planning required for your solution selection. Work with your PMO to establish your reporting and milestone requirements.

Your coordination with the PMO will be especially critical if you are engaging a third party at either the selection or implementation stage.

Create a project plan that outlines the evaluation, selection, and implementation for your SIEM tool

Info-Tech Insight

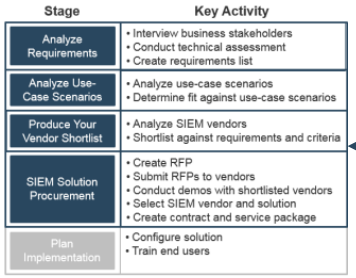
At this point in the project, **slow down** and ensure you have done the appropriate project planning and are following your business's procurement procedures before proceeding with your review and selection.

Identify key steps for each stage of the selection and procurement project.

Stage	Key Activity
Analyze Requirements	• Interview business stakeholders • Conduct technical assessment • Create requirements list
Analyze Use-Case Scenarios	• Analyze use-case scenarios • Determine fit against use-case scenarios
Produce Your Vendor Shortlist	• Analyze SIEM vendors • Shortlist against requirements and criteria
SIEM Solution Procurement	• Create RFP • Submit RFPs to vendors • Conduct demos with shortlisted vendors • Select SIEM vendor and solution • Create contract and service package
Plan Implementation	• Configure solution • Train end users

The project's implementation planning stage should be separated out as its own project. Use Section 6: Plan your SIEM Implementation to outline your project and complete this stage of your selection and implementation of SIEM.

Select your procurement vehicle



Procurement Vehicle

Now is the time to select the procurement vehicle to follow as you analyze and select your SIEM tool from the options in the market.

Info-Tech Recommendation

Info-Tech recommends the use of an RFP process, rather than a direct award or RFI process, due to the number of considerations and cost related to a SIEM procurement.

Please note that the remainder of this blueprint follows this structure. If this is not the vehicle your organization will use, simply adapt the procurement steps in section 5 to fit your own project plan.

Definitions

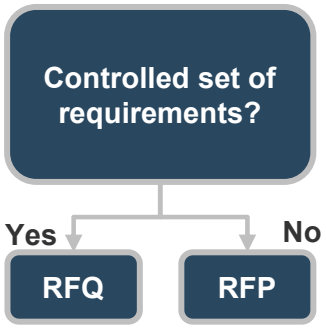
Request for Quotation: A simple description of the product and a small number of requirements.

Request for Information: A document requesting marketing-level information on the vendor's solution, it is meant to improve the client's understanding of the products in the marketplace and the specific product of the vendor.

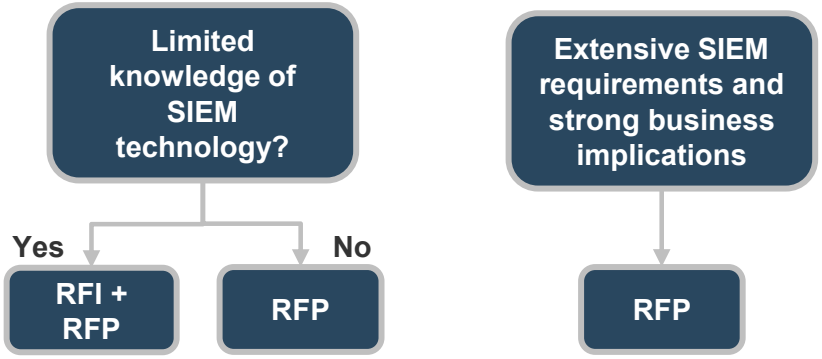
Request for Proposal: A lengthy document outlining the requirements, scope, systems, and processes related to the desired solution.

Selection Support

Small Enterprise



Medium-Large Organizations



Additional Research

Consult this blueprint for more information on procurement vehicle options.

Optimize IT Procurement

Create a plan for your SIEM selection project

2.4 1 hour

Instructions

1. Create a meeting for the project's management and leadership to scope the steps and stages of the project.
2. Identify the procurement vehicle for your procurement process.
3. Document the steps in the project's charter.
4. Identify the milestones associated with each step and determine the expected completion date/due date or additional consideration related to the milestone.

Time
- One-hour planning meeting
- Additional documentation hours for PM

Charter Sections
- *Section 7: Project Plan and Timeline*

Optional structure for designing your project plan.

Stage	Key Activity	Participants	Output
SIEM Solution Procurement Sample	• Create RFPs for shortlisted vendors • Submit RFPs to vendors • Evaluate proposals • Conduct demos for shortlisted vendors • Select SIEM suite • Create and approve contract and service package	• Core team • Project manager • Writers • Evaluation team • Vendors	• RFP proposals • Selected SIEM solution • Vendor contract and service package

Optional structure for outlining your project milestones.

Milestone	Start Date	End Date	Dependencies	Due Date	Product/Event

Determine the metrics you will use to assess the performance of your SIEM selection project

2.5

Your project cannot be deemed a success if a metric or measure cannot be applied to gauge its performance. Identify the metrics that will be used to assess the performance of your SIEM selection and implementation.

Project Performance

Timeline Adherence

- Was the project completed during its initially defined timeline?
- Did the SIEM selection occur in its defined period?
- Did the implementation and initial process rollout occur during the outlined window?
- What percentage of project milestones were met?

Discount Pricing Negotiated

- Percentage of discount negotiated

Project Costs

- Allocated project budget vs. actual project expenses

Budget Adherence

- Actual cost vs. budgeted cost for the solution

Determine the metrics you will use to assess the performance of your SIEM selection project

2.5 1 hour

What considerations will be used to evaluate the performance and success of your completed project?

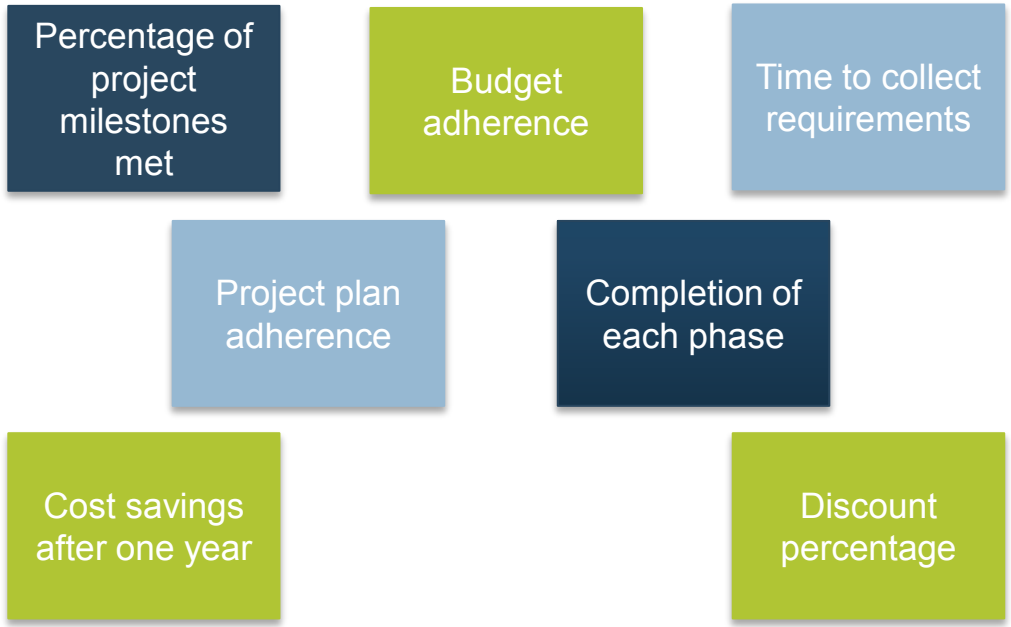
Instructions

1. As a group, brainstorm the metrics that will be used to evaluate the completed project.
2. Adapt the charter to include the metrics relevant to your project.

Charter Sections
- *Section 9: Financial Obligations for a SIEM Selection*
- *Section 10: Project Costs*

Materials
- Whiteboard and markers
- Sticky notes and markers

What project considerations and organizational drivers will drive your metric selection?



Select the pilot for your project in order to manage your SIEM deployment

2.6 1–2 hours

Instructions

1. As a group, discuss a process or line of the business that will best serve as a pilot for SIEM.
    - Include a diverse group of sites, user devices, and operating systems to create a realistic model of your SIEM solution.
2. Create a review process that allows you to examine the pilot and implement changes to the overall SIEM architecture that will optimize the solution. Focus on implementing a monitoring functionality only in the beginning.
3. Once the pilot has been sufficiently optimized, consider a slow rollout to other user groups or sites as opposed to a full implementation in the organization.

Considerations for Selecting Your Pilot

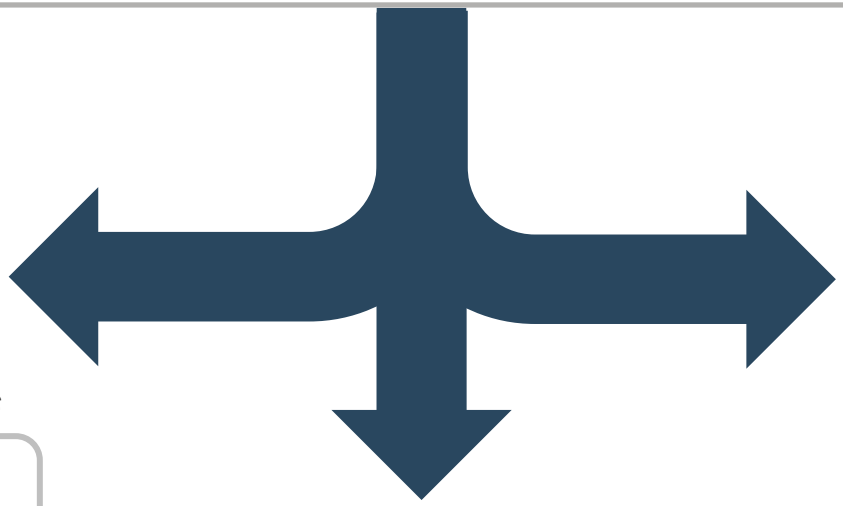
- Attempt to work across multiple sites.
- Attempt to include multiple user devices.
- Try to include multiple operating systems.
- Be wary of the many false positives that may result.
- Avoid selecting servers or users where deployment may disrupt their day-to-day activities.

Charter Sections
- *Section 8: Pilot*

Info-Tech Insight

Getting consensus will be the most difficult part of this activity, but make sure your stakeholders are on the same page before proceeding.

Gain approval for proceeding with your vendor evaluation and SIEM procurement project



Your CISO has the authority to approve your project.

Informal Process

1. Present any project plan changes to the CISO for review
2. CISO approves the project and budget

Project is launched

Business sign-off and budgetary approval must be given.

Formal Process

1. The project plan is presented to management and relevant business stakeholders
2. Project is reviewed and approved; budget is reviewed and approved

Project is launched

The steering committee is required to review and approve your project plan and budget.

Formal Process

1. The project plan is presented to the steering committee
2. Project is reviewed and approved; budget is reviewed and approved

Project is launched

In each case the budget may have to pass through the business's procurement committee or PMO in order to comply with organizational standards.

Record your approval at the end of the *SIEM Procurement Project Charter Template*.

Workshop Scope for Step 2

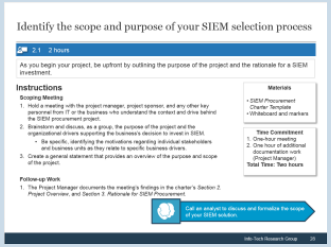
Call 1-888-670-8889 or email Workshops@InfoTech.com for more information

Preparatory Activity

- **2.2:** Create a project team for your SIEM selection and implementation projects. As scheduling allows, include these team members as participants in the onsite workshop.
- **2.6:** Meet with stakeholders and identify the business process that will serve as the best pilot for implementing process automation into the business environment. During a call prior to your workshop, use the guidance provided by your Info-Tech analyst to support your selection process.

An Info-Tech Analyst would facilitate the following activities during an onsite engagement:

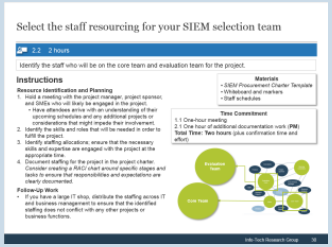
2.1



Determine the scope of your project

Work with the Info-Tech analyst to finalize the scope of your SIEM selection project. In this step, the facilitator will meet with the project team to review the causes for the project and business drivers. If necessary, interviews with the business, including the project sponsor, will be conducted to narrow and finalize project objectives and scope.

2.2



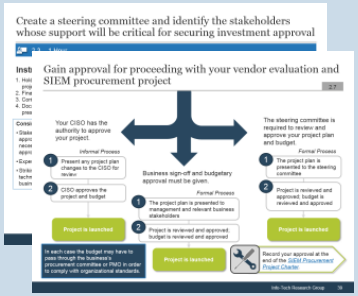
Identify and review the staffing requirements for your project

When Info-Tech comes onsite, we kick off this step with your team by reviewing the preliminary staff identified for your project. The facilitator will discuss the implications of resourcing and availability, as well as how the skills and knowledge captured on the team align with the selection requirements. Accompanying this review, the facilitator will discuss whether an outside consultant or integrator is potentially needed.

Workshop Scope for Step 2

Additional Activities

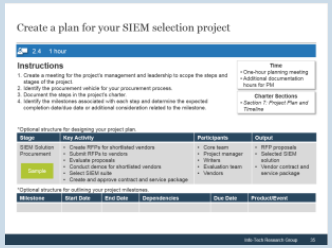
2.3 + 2.7



Discuss the oversight and organizational requirements associated with completing your project

The Info-Tech facilitator will discuss the stakeholder management considerations associated with this project and talk through your own organization's oversight requirements with your project team. This activity will identify the reporting and approval steps required for a steering committee or your organization's PMO.

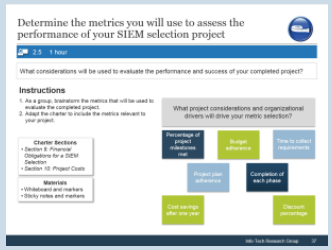
2.4



Create a project plan for your SIEM selection project

The Info-Tech analyst will facilitate the construction of your SIEM selection project plan. Led by the facilitator, this activity will document each step in the project, the key activities within them, and the outcomes associated. To support the execution of the project, resourcing responsibilities, milestones, and timelines will also be identified at this stage.

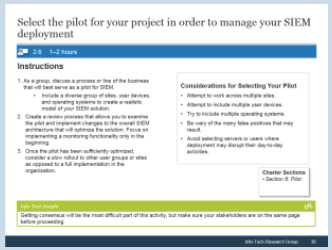
2.5



Determine the metrics for gauging your project success and the value of your SIEM investment

An Info-Tech facilitator will support your team in creating governance for your project through the setting of formal metrics. This activity will set the metrics that will gauge the success of your SIEM selection, and also identify the metrics that will be used to gauge the overall success of the implemented SIEM.

2.6



Review your selected pilot

Our Info-Tech expert will review the pilot selected by your team as the organization's introduction to SIEM. The facilitator will review the pilot and the factors behind its selection, helping to support your project team in identifying if this selected pilot will be the best fit for your project.

Step 3: Identify the requirements for a SIEM

1. Assess value and identify fit
2. Build the procurement team and project plan
3. **Identify the requirements for a SIEM**
4. Produce a vendor shortlist
5. Select a SIEM solution
6. Create an implementation plan
7. Measure the value of the SIEM solution

This step will walk you through the following activities:

3.1: Review which requirements need to be collected
3.2: Gather your business requirements
3.3: Gather your technical requirements from IT
3.4: Extract requirements from your previous assessments
3.5: Review use cases and their fit with your organization

Info-Tech suggests involving the following participants in this step of the project:

- Project manager
- Security engineers
- Security analysts
- Network manager

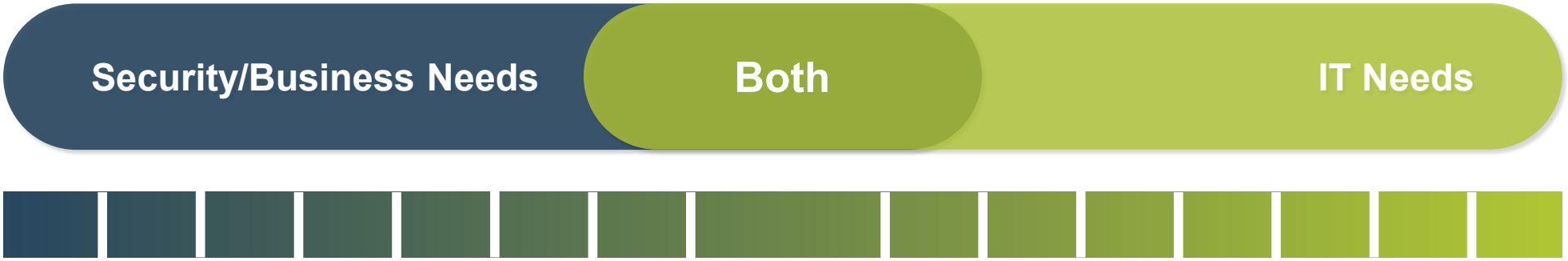
Outcomes of this step:

- Successful gathering of requirements from the business related to SIEM
- Completed interviews with IT and extraction of technical requirements regarding architecture, integration, and implementation for the future SIEM suite
- Documentation of high-level functional and solution requirements for SIEM; these findings will be used as a reference as the business begins analyzing and shortlisting vendors and will also serve as the critical foundation for the future RFP and evaluation process
- An appraisal of Info-Tech's SIEM use-case scenarios and identification of the use-case scenarios that apply to the business's desired use of SIEM

Get the capabilities you need by gathering the necessary security and IT requirements

3.1

Proper requirements gathering is critical for delivering value from security projects, but it can be a difficult and elusive process for any IT project. For a security project specifically, it involves incorporating the needs of security with the business and the technical requirements behind IT. This must be done by identifying and gathering the requirements from your multiple stakeholders.



- Understand how the organization can lower its overall risk with the solution.
- Identify the compliance and regulatory frameworks that can be followed by using a SIEM solution.
- Identify and remediate against external threats that can be facing your organization.
- Identify how the SIEM solution can be deployed across the organization.
- Determine what type of architecture is necessary in order for the SIEM to work best.

Info-Tech Insight

Requirements gathering for security technologies differs from that for typical IT projects, as they do not affect end-user processes as much. When it comes to business stakeholders, focus on their expectations of security in regards to the organization in general.

Engage security, IT, and the business while assessing SIEM requirements and identifying selection criteria

Conduct both a ***security/business assessment and an IT assessment*** to build your solution requirements.

	Security/Business Assessment	IT Assessment
Activity	• Interview business stakeholders	• Interview key IT & IT security personnel • Review the IT architecture
Findings	• Determine the business expectations of security within the organization	• Deployment options for the organization • Support requirements • Compatibility and integration requirements • Design process and programming capabilities
Outcomes	• Security requirements of the technology	• IT and technical requirements

Info-Tech Insight

Don’t focus on what the tool will look like at the beginning. Instead focus on what the business needs SIEM to do and the processes it must be able to support. Don’t use these opportunities to create a long list of features; instead use them to understand the motivations and functional uses that will be integral to a successful adoption and ROI of the technology.

Focus on these five categories for your requirements gathering

Below are SIEM-specific requirements that need to be considered before selecting your SIEM solution.

- Collection, storage, and deployment & management are three major architecture aspects that need to be evaluated based on your organization's needs.
- Analysis and reporting & alerting are viewed here as features, and will be reviewed more closely in Phase 2 of this blueprint.

> *Start with basics, such as understanding your requirements. Then find out what you need to do and then what it is you want to do.*
>
> - Christopher Warner, President/Chief Security Consultant, Cyberdine

Collection	Analysis	Reporting & Alerting	Storage
• Agent • Agentless			• Native • Relational • Extended

Deployment & Management	
• In-house • Managed Security Service Provider (MSSP)	• Hardware appliance • Virtual appliance • Software-based

Review the types of collectors that will be compiling your log information

3.1

Collectors are needed in order for log information to be collected. These logs are what provide the necessary security information and assist in later forensic analysis. The two types of collectors used are agent and agentless. The table below goes into more detail:

Agent

- Agents are installed on devices and typically run in the background to collect log information. These agents will then send logs either to collector points or to the SIEM.
- The benefits are as follows:
  - Logs can be filtered based on previously established criteria.
  - Agents tend to work well with firewalls and the overall network, although it may require full access.
  - Agents can perform some data normalization or compression to limit network bandwidth.
- The cons are as follows:
  - The installation of the agents can take a significant amount of time.
  - There is the possibility of the agent slowing down the device's performance.

Agentless

- Agentless collectors usually work through remote access of the device to collect log information.
- The benefits are as follows:
  - No specific installation is needed across devices.
  - Further, maintenance is not needed for agentless collectors.
  - Limited footprint on the endpoint device itself.
- The cons are as follows:
  - Log information is not always reliably transferred.
  - Often, logs must be normalized before being collected by the SIEM which can cause the loss of some event details.

Leverage the storage options available to find a right-sized solution

Storage is another important aspect of a SIEM solution. With the collection of hundreds, if not thousands, of logs, there is the need for extensive storage capability. This is especially useful as log information will need to be stored so that it can be later accessed for forensic analysis and provide more information.

Native

The solution itself provides its own storage options for the SIEM solution. It does not rely on the separated servers or databases to store information as the vendor itself will help to provide this.

Relational

This model is able to store information as it connects to other logs, and allows for an increase in the overall efficiency of the storage. It also becomes easier to change the data while still decreasing inconsistency.

Extended

These SIEM solutions will provide storage so that it can be part of the native solution, but also be extended to secondary storage as seen fit. This can extend to an organization's servers and networks, or through extended storage offerings of the vendor itself.

Consider the available on-premise SIEM deployment options

Each SIEM appliance model has its own merits and faults.

Platform	Pros	Cons
Hardware Appliance	Simplified management maximizes focus on SIEM operations Simplified support – no vendor concerns about underlying hardware	Dedicated on-premise storage is unavailable for other uses Scalability limited by appliance capabilities
	Tiered vs. shared	
Virtual Appliance	Leverages existing server virtualization and shared storage (SAN) investments Scalability and resiliency limited only by those environments	High-performance requirements consume virtual server resources Requires additional virtual server management
Software-Only Solutions	Allows wider choice of hardware Software-based updating and maintenance	Requires dedicated server hardware and ongoing server management. Elevates risk of hardware vs. software finger-pointing during support calls.

Regardless of the choice – or mix – of platforms, don't forget to plan for log data *backup* to meet regulatory and internal policy requirements.

Determine how you will staff the SIEM solution to ensure proper monitoring and alerting

Staffing a SIEM solution properly can be one of the biggest factors in deriving the full value of your SIEM solution.

A SIEM solution will help to provide alerts about any security incidents in your network. However, you need to have dedicated staff to ensure that real-time remediation accompanies your real-time monitoring:

- If your organization lacks a dedicated Security Operations Center (SOC), then adding real-time monitoring to your SIEM product can necessitate **five** full-time equivalents (assuming 24x7 monitoring capabilities).
- An alternative option is to add this on to the duties of your other security or network engineers, as even a small increasing in monitoring can yield better incident response.

Consider an Alternate Solution: Managed Security Service Providers (MSSP)

A Managed Security Service Provider (MSSP) can be a new approach to staffing and managing your SIEM solution:

- MSSPs provide 24/7 monitoring and alerting at prices that are often lower than the full TCO of implementing an in-house solution.
- Many MSSPs also provide other security services, such as remediation or incident response, that can integrate well with SIEM and reduce the pressure on your employees.
- However, there are some concerns: SIEM data is stored off-site, can be accessible to third parties, and/or follow different regulations from that of your organization.
    - If you choose to use an MSSP, ensure that all this information is addressed when creating your MSSP contract.

Engage the business stakeholders and determine security requirements

3.2 1-hour meeting

This activity could take the form of a meeting with multiple business stakeholders or through one-on-one meetings (e.g. with SMEs).

Instructions

Option 1: Open forum meeting

1. As a group, discuss the business and security considerations that must be taken into account as your organization selects its SIEM solution.
2. Brainstorm and discuss the architectural, staffing, and implementation (both integration and configuration) factors and decision points.
3. Document the technical requirements that were identified in this discussion.

Option 2: Conduct one-on-one interviews or interview by role

1. Ask the interview candidates what architectural and technical considerations they believe will be needed for the future SIEM tool.
2. Document interview findings.
3. Have your Project Management team (Project Manager, Project Sponsor) review the findings and create a final set of technical requirements.

Information Sources
- Business stakeholders

Time
- 1-2 hour meeting or 30-minute interviews
- Additional PM documentation time

Result
- Business expectations of security
- Security and business requirements

Call an analyst to assist in the collection and review of your business requirements.

Engage the IT staff and determine technical requirements

3.3 1-hour meeting

Similar to the business stakeholders, this can be completed through an open forum meeting or through one-one-one interviews.

Instructions

Option 1: Open forum meeting

1. As a group, discuss the technical considerations that must be taken into account as your organization selects its SIEM solution.
2. Brainstorm and discuss the architectural, staffing, and implementation (both integration and configuration) factors and decision points.
3. Document the technical requirements that were identified from this discussion.

Option 2: Conduct one-on-one interviews, or interview by role

1. Ask the interview candidates what architectural and technical considerations they believe will be needed for the future BPM tool.
2. Document interview findings.
3. Have you Project Management team (Project Manager, Project Sponsor), and, if possible, a SME review the findings and create a final set of technical requirements.

Information Sources
- Application architecture
- Business interview findings

Time
- 1-2 hour meeting or 30 minute interviews
- Additional PM documentation time

Result
- Technical requirements
- Implementation requirements

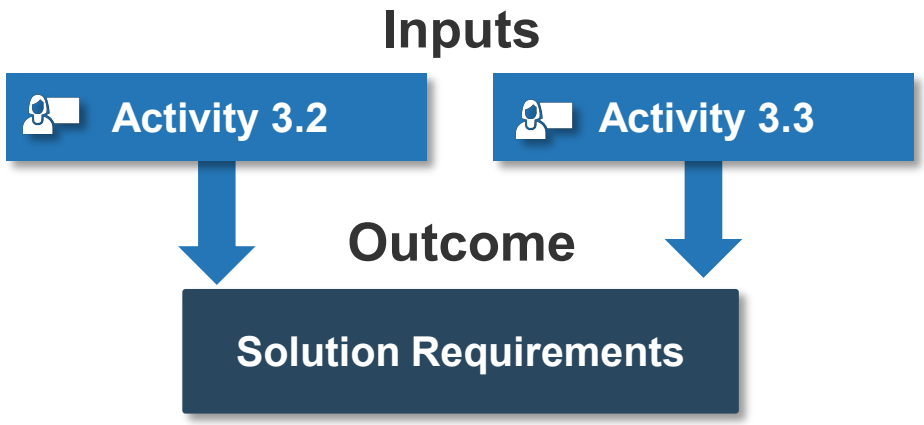
Call an analyst to assist in the collection and review of your IT requirements.

Extract functional and technical requirements from your business and IT assessments

3.4 Consolidate the findings of your requirements-gathering activities

Instructions

1. Use your business interviews and mapped processes to identify functional and capability requirements.
2. Use your project meetings and interviews with IT staff to identify technical requirements and considerations that will guide the selection of a SIEM.



Outcome

Create a preliminary document of solution requirements based on this requirements-gathering process.

Add as You Proceed

As you identify the use cases for your SIEM solution, add to these gathered requirements.

As you evaluate vendors in the market and identify the full capabilities of different SIEM solutions, add and adjust the requirements documented at this point of the project.

Identify the use-case scenario that applies to your business

3.5

- This view of vendor and product performance provides multiple opportunities for vendors to place depending on their product and market performance. Use cases selected are based on market research and client demand.

Use Case	
Threat Management	Threat management is meant for highly security-conscious organizations that need to protect their data or intellectual property from advanced threats, whether internal or external.
Compliance Management	SIEM products can help organizations looking to pass their regulatory and industry framework audits and manage their multiple compliance obligations.
Management of Security Events	High-capacity and heterogeneous organizations that need to gain full organization visibility across high-rate information systems dispersed across geographic locations.
SIEM Small Deployment	Smaller and resource-constrained organizations will likely be looking for a simplified SIEM offering, with less advanced or additional features but still providing strong security insight.
Risk Management	Organizations are often looking to reduce their overall level of risk by implementing security controls that can help to protect their data and manage their obligations while providing risk visibility.

SIEM Use Case: Threat Management

3.5

New threats are coming from all directions and the need to detect, analyze, and respond to all of them continues to be a growing concern.

Threat management is meant for high-security-demand organizations that need to mitigate against threats. With the complexity and sophistication of threats continuing to increase, it becomes more important that the organization be better prepared.

Key features to look out for:

- For proper threat management, there is a need for advanced correlation of all different security and non-security events and incidents, coupled with a threat intelligence feed to ensure that the SIEM stays up to date.
- Secondary features include the ability to manage and remediate incidents, having full visibility into the security incidents or attacks across systems and people, and the ability to use big data analytics for more insights into the threat detection and analysis.

Threat Management

Compliance Management

Management of Security Events

SIEM Small Deployment

Risk Management

Ideal for:

- Organizations looking to detect against threats that are otherwise difficult to detect, whether internal or external
- High security demand organizations: financial institutions, health care providers, retailers, intellectual property dependent organizations

SIEM Use Case: Compliance Management

3.5

With an increasing amount of compliance obligations and regulatory frameworks, SIEM was built to be leveraged to manage these.

As most solutions offer compliance reporting, SIEM products are often sought after by audit and compliance requirements that are looking for reporting capabilities into the organizations. Many of them offer templates and allow people to keep up with their audit concerns.

Key features to look out for:

- The ability to provide advanced reporting and alerting, especially around compliance requirements and adherence, is a key capability offered in this use case. The SIEM needs to be able to report on compliance to the organization and any third parties.
- Data management and security becomes an important concern for compliance use cases. Many compliance requirements have data retention periods and data protection requirements.

Threat Management

Compliance Management

Management of Security Events

SIEM Small Deployment

Risk Management

Ideal for:

- Organizations that are looking towards managing their compliance reporting and managing their reporting obligations
- Regulated industries: financial institutions, health care providers, credit card processing organizations, etc.

SIEM Use Case: Management of Security Events

3.5

As companies grow, network activity and security events rise and a SIEM solution becomes crucial in tracking and managing this activity.

The desire to monitor an expansive network's activity and threats in real-time is one of the highly sought after features of a SIEM. High capacity tools can allow security events to be monitored constantly in real time. Pair this with advanced correlation and analytics and it becomes possible to identify significant security events.

Key features to look out for:

- A key feature is a product focus/capability for scalability and network performance, as it is important to have a product that can continue to work well within high capacity environments through horizontal and vertical scalability.
- Advanced data enrichment becomes a key factor in this use case, as it ensures the different types of information and log data into the SIEM system is usable and actionable.

Threat Management

Compliance Management

Management of Security Events

SIEM Small Deployment

Risk Management

Ideal for:

- Organizations that are looking for more insights into security threats as they occur, as opposed to reviewing historical data and finding out about threats after the fact
- Largely heterogeneous and geographically dispersed organizations with high numbers of users and devices

SIEM Use Case: SIEM Small Deployment

3.5

Smaller organizations will be looking for cheaper and more basic products to fulfill their desired SIEM capabilities.

SIEM Small Deployment is the concept of providing a scaled-down solution that is also simple to deploy. Some SIEM vendors and offerings provide a large variety of features for consumers, but these can be more than expected. As a result, these organizations will be looking for a simpler version of SIEM that is highly usable, low cost, and does not necessarily have advanced features.

Key features to look out for:

- The main focus on SIEM Small Deployment here is, of course, the affordability of the product as many are looking for a cost-effective product.
- Beyond the price, most organizations are looking at the usability of the product and the ability to alert based on events, provide more forensics into the information, and provide ease of incident management.

Ideal for:

- Organizations that are looking to increase their security technology, but do not need many of the advanced or additional features found in some solutions
- Low user base, low device number, knowledge based employees, usually one location, e.g. professional services firms

SIEM Use Case: Risk Management

3.5

SIEM solutions can be used to mitigate against risk and decrease the overall risk profile of an organization.

Risk management is the ability to mitigate the organization's risk, which encompasses multiple risks including compliance and threat risk. This use case is roughly the average of the compliance management requirements and the threat management requirements. This use case highlights management of the entire organization's risk, not just that of information security.

Key features to look out for:

- In the area of risk management, all the product features are of concern. A heavier focus on features includes advanced data enrichment, correlation, forensic analysis support, and incident management.
- A full, comprehensive SIEM needs to be deployed that can serve many features in order to be very effective in this case.

Ideal for:

- Organizations that are looking to reduce their overall risk through the implementation of stronger security controls, which in this case would be a SIEM solution
- Organizations with a low risk tolerance looking to increase their overall cyber security

Determine your business's fit against Info-Tech's use-case scenarios

3.5 SIEM Use-Case Fit Assessment Tool

Activity 3.5: 2 Hours

Use the *SIEM Use-Case Fit Assessment Tool* to identify your organization's alignment with the functional use cases identified by Info-Tech.

Instructions

1. Download your own version of the tool and complete the Business Process Questionnaire on *Tab 2. Assessment*.
    - Use the information gathered from your business interviews and initial project scoping to respond to the prompts to identify the business and IT requirements for the tool.
    - Answer the prompts for each statement from a range of *Strong Disagree* to *Strong Agree*.
2. Review the outcomes on *Tab 3. Results*.
    - This tab provides a qualitative measure assessing the strength of your fit against the industry use-case scenarios.
3. If not completed as a team, debrief the results and implications to your core project team.

Questionnaire

Answer the following questions below using the response column. Each question has a number of associated options: select the option that **best** describes your organization. In some circumstances, you may need to involve departmental experts in order to answer each question.

	ID	Question	Answer
Business & Security Requirements	Q01	Do you have compliance obligations that require you to report on security control?	Yes
	Q02	Is your organization regularly audited by internal and/or external parties?	Yes
	Q03	Does your organization have the ability to dedicate full time employees to the deployment and maintenance of a SIEM product?	Yes
	Q04	Is there a limited security and/or IT budget for a new security technology?	Yes
	Q05	Do you have a history with insider threats?	Yes
	Q06	Do you have in-house security expertise?	Yes
IT Requirements	Q07	Currently, is your organization able to take advantage of big data security analytics? i.e. integration with Hadoop	Yes
	Q08	Are you looking to leverage an incident management platform with integrated workflow?	Yes
	Q09	Are you looking for a SIEM solution that is able to scale up as your organization continues to grow?	Yes
	Q10	Do you have a history with targeted attacks against your organization such as spear phishing, APTs, malware, etc.?	Yes
	Q11	Are you looking for remediation capabilities in your SIEM solution?	Yes
	Q12	Do you have security technologies such as a NGFW or an IDPS in place?	Yes
	Q13	How many event sources would your organization be monitoring?	Yes
	Q14	What is your required sustained events per second (EPS) rate?	Yes
	Q15	What is your back end use storage?	Yes
	Q16	Will you be requiring multiple reports per week?	Yes

Tab 2. Questionnaire

Time

- One hour to complete tool
- One-hour meeting to debrief results and implications

Interpret the results: Identify your fit against the use-case scenarios

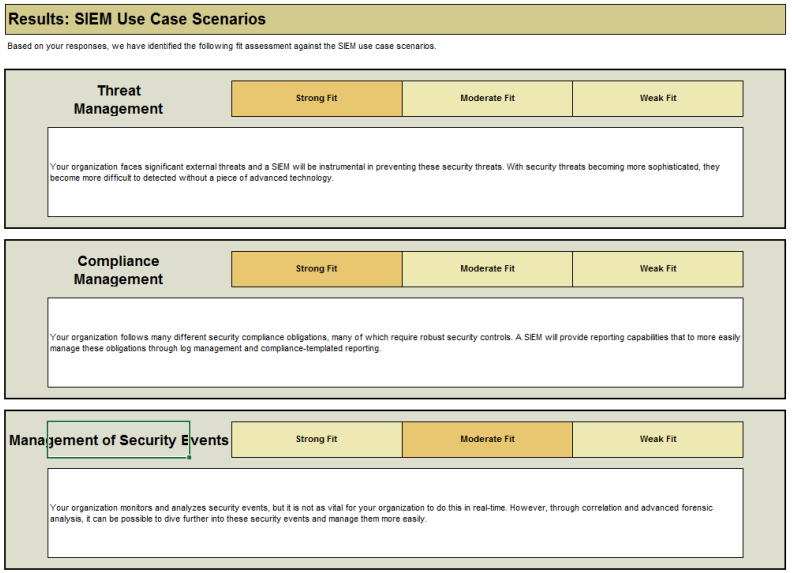
3.5 *SIEM Use-Case Fit Assessment Tool:* Tab 3. Results

Activity 3.4: Interpreting the Results

This tool will assess your answers and determine your relative fit against the ***Use-Case Scenario 1***, ***Use-Case Scenario 2***, etc.

Fit will be assessed as "*Weak,*" "*Moderate,*" or "*Strong.*"

Note: These use-case scenarios are not mutually exclusive; your organization can align with one or more scenarios based on your answers. If your organization shows close alignment to multiple scenarios, consider focusing on finding a more robust solution and concentrate your review on vendors that performed strongly in all three scenarios or meet the critical requirements for each.



Tab 3. Results

Use the strength of your fit to prioritize your requirements and narrow your focus as you evaluate and select a vendor.

Strong Fit | Moderate Fit | Weak Fit

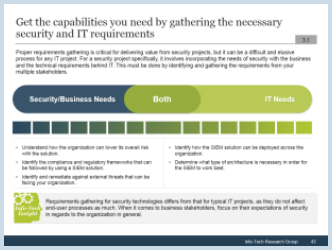
Implication: As you proceed with building your solution requirements and conducting a procurement, focus on evaluating vendors to meet use cases that were a moderate or strong fit for your organization. **Adjust the requirements gathered through your preliminary evaluations to consider your use-case findings.**

Workshop Scope for Step 3

Call 1-888-670-8889 or email Workshops@InfoTech.com for more information

An Info-Tech Analyst would facilitate the following activities during an onsite workshop:

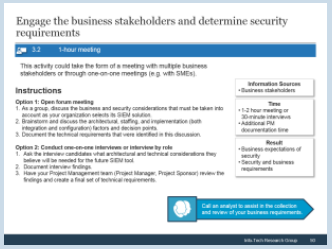
3.1



Review the unique requirements needed for your SIEM

The Info-Tech facilitator will review the requirements that need to be collected from your business stakeholders, security staff, and IT team. This extends beyond the requirements gathering of any IT project, as security can affect the entire business while still running in the background. The facilitator will focus on the requirements needed for a SIEM solution specifically including storage, types of collectors, and deployment options.

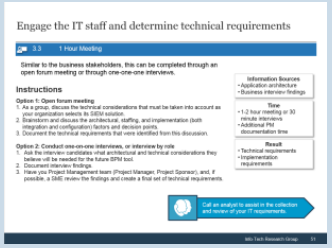
3.2



Identify the business requirements for the future SIEM suite

The Info-Tech facilitator will help to identify the key business stakeholders that will be able to provide leadership for the security of the organization. A plan can be created to approach the business stakeholders and collect their requirements.

3.3



Identify technical requirements for the future SIEM suite

The Info-Tech facilitator will use your own business and IT landscape to help guide your project team in identifying the architectural and integration requirements for your SIEM suite. The facilitator will either perform an open forum meeting with the IT staff of your project team or conduct one-on-one interviews with specific members of the team and general staff based on the scoping performed prior to the workshop. This step will identify the technical requirements for the tool and also identify considerations and requirements associated with the suite's implementation.

Workshop Scope for Step 3

An Info-Tech Analyst would facilitate the following steps during an onsite workshop:

3.4

Consolidate your interview and analysis findings into high-level solution requirements

The onsite facilitator will walk through the findings from the business interviews, process mapping, IT interviews, and technical requirements identification with the project team. Using these findings, the facilitator will guide the project team in prioritizing and streamlining requirements into a high-level solutions package.

3.5

Identify your use-case scenario results

The Info-Tech analyst will guide your organization in evaluating your organization's envisioned purpose and requirements for the future SIEM suite to identify the use cases that are applicable to your organization. Using both IT and business considerations, the facilitator will identify the strength of your business's fit against the use-case scenarios and discuss how the implications of the results may alter your selection process and guide you toward a specific vendor(s).

Phase 2: Select a SIEM solution

Phase 2 outline

Call 1-888-670-8889 or email GuidedImplementations@InfoTech.com for more information.

Complete these steps on your own, or call us to complete a guided implementation. A guided implementation is a series of 2-3 advisory calls that help you execute each phase of a project. They are included in most advisory memberships.

Guided Implementation 2: Select a SIEM solution

Proposed Time to Completion: 1-3 months

Step 4: Produce a Shortlist

Start with an analyst kick-off call:

- Discuss the Vendor Landscape and the different use cases.

Then complete these activities…

- Review SIEM Vendor Landscape overview.
- Review vendor profiles and analysis with use-case performance.

With these tools & templates:

- *SIEM Vendor Landscape Analysis*
- *SIEM Vendor Shortlist and Detailed Analysis Tool*

Step 5: Select a SIEM Solution

Review findings with analyst:

- Create and refine your RFPs.
- Evaluate collected RFPs.

Then complete these activities…

- Create solution requirements.
- Create RFP.
- Evaluate RFPs.
- Create demo script.
- Conduct vendor demonstrations.

With these tools & templates:

- *SIEM RFP Template*
- *SIEM Evaluation and RFP Scoring Tool*
- *SIEM Vendor Shortlist and Detailed Analysis Tool*

Step 5: Select a SIEM Solution

Conduct a Contract Review

- After you have selected a vendor and negotiated a contract, review your contract with an Info-Tech analyst.

Then complete these activities…

- Select vendor.
- Negotiate contract.

Phase 2 Results & Insights:

- Selection of a SIEM solution, after careful review of the vendors with according RFPs and contract reviews.

Step 4: Produce the vendor shortlist

1. Assess value and identify fit
2. Build the procurement team and project plan
3. Identify the requirements for a SIEM
4. **Produce the vendor shortlist**
5. Select a SIEM solution
6. Create an implementation plan
7. Measure the value of the SIEM solution

This step will walk you through the following activities:

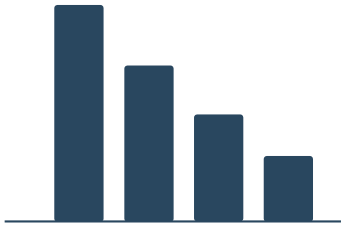
- 4.1: Review Info-Tech's SIEM vendor evaluation
- 4.2: Review vendor performance for use-case scenarios
- 4.3: Identify top vendors from relevant scenarios
- 4.4: Create custom vendor shortlist

Info-Tech suggests involving the following participants in this step of the project:

- Project manager
- Business analysts
- Subject matter experts

Outcomes of this step:

- Identification of the opportunities associated with SIEM
- Confirmation of the organization's suitability for a SIEM investment
- An appraisal of Info-Tech's Vendor Landscape market overview for SIEM
- Determination if now is the right time to proceed with this project



4.1 Info-Tech's Vendor Landscape Methodology

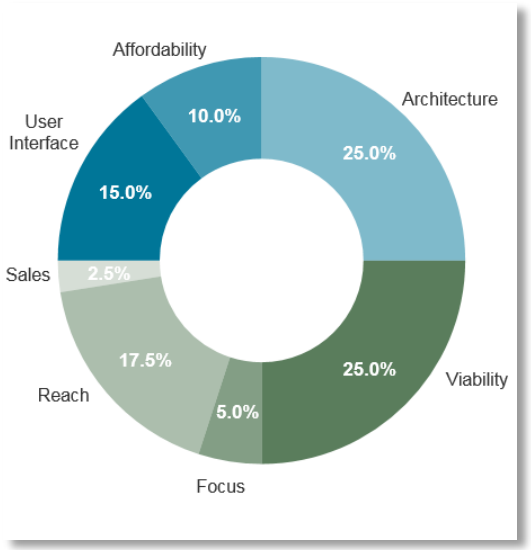
Vendor Landscape use-case scenarios are evaluated based on weightings of features and vendor/product considerations

4.1 Scoring Overview

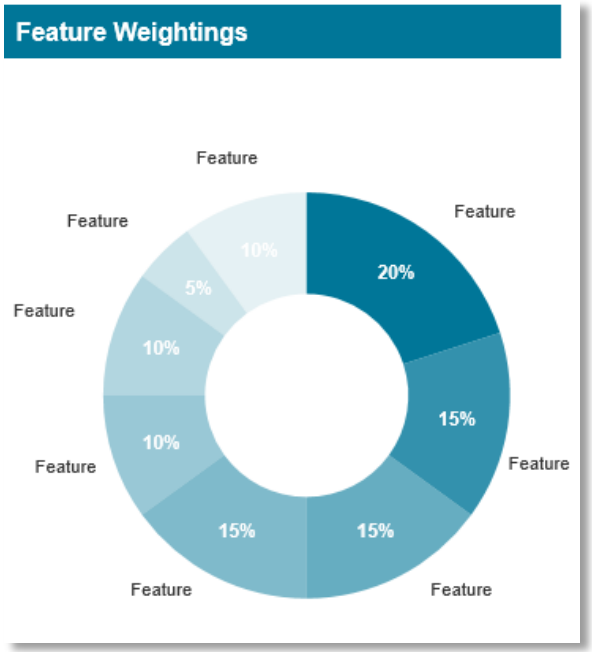
Use cases were scored around the features identified in the general scoring as being relevant to the functional considerations and drivers for each scenario.

Calculation Overview
Advanced Features Score X Vendor Multiplier = Vendor Performance for Each Scenario

Please note that both advanced feature scores and vendor multipliers are based on the specific weightings calibrated for each scenario.



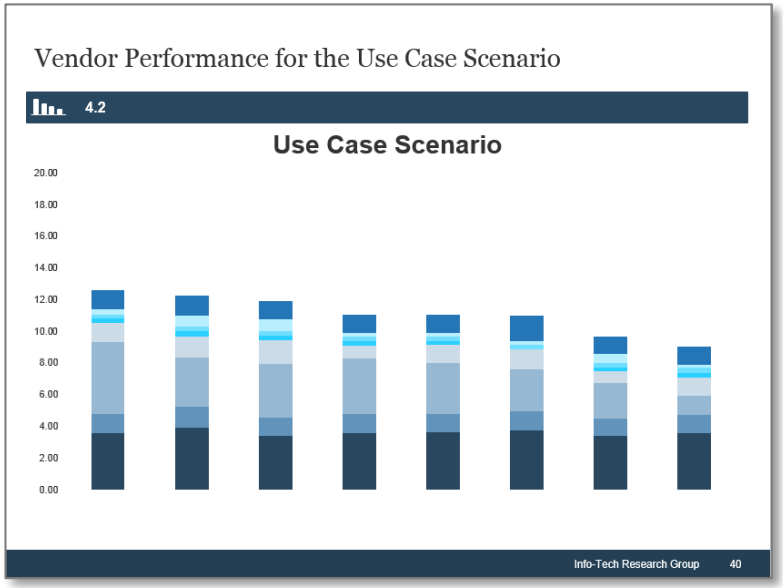
Product and Vendor Weightings



Advanced Features Weightings

Vendor performance for each use-case scenario is documented in a weighted bar graph

4.1 Scoring Overview



Vendor Performance

Vendors qualify and rank in each use-case scenario based on their relative placement and scoring for the scenario.

Vendor Ranking

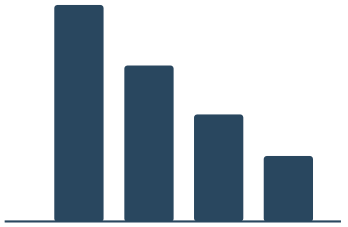
Champion: The top vendor scored in the scenario

Leaders: The vendors who placed second and third in the scenario

Players: Additional vendors who qualified for the scenarios based on their scoring

Value Score™

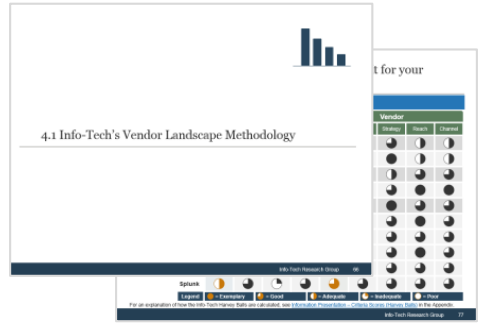
Each use-case scenario also includes a Value Index that identifies the Value Score for a vendor relative to their price point. This additional framework is meant to help price-conscious enterprises identify vendors who provide the best "bang for the buck."



4.2 Review the SIEM Vendor Evaluation

Review Info-Tech's Vendor Landscape of the SIEM market to identify vendors that meet your requirements

The following section includes an overview of vendor performance and the analysis of each use-case scenario. **Review the accompanying deliverable in order to understand the strengths, weaknesses, and capabilities of each vendor.**



Vendors Evaluated

ALIEN VAULT
EventTracker www.eventtracker.com
hp
IBM
RSA The Security Division of EMC
NetIQ
solarwinds
splunk>
LogRhythm
intel Security

Each vendor in this landscape was evaluated based on their **features, product considerations,** and **vendor considerations.** Each vendor was profiled using these evaluations and, based on their performance, qualified and placed in specific use-case scenarios.

SIEM Market Overview

4.2

How it got here

- SIEM used to be two separate products: Security Event Management (SEM) and Security Information Management (SIM).
- SIEM was created initially as a compliance management tool. It had the ability to centralize, review, and report on log activity.
- Soon after, the ability to correlate logs was leveraged to provide threat detection and advanced intelligence tools in order to examine IT systems more closely.
- SIEM solutions were initially directed towards large enterprises with high volumes of data and resources. This changed as more and more SIEM vendors began offering products to the small and mid-sized market.
- SIEM products expanded use with integration into other security technologies in order to provide a holistic view into the security of an organization with the ability to push out commands and data to other systems.

Where it's going

- Advanced analytics will change the landscape of SIEM entirely and allow for the detection of complex and sophisticated security events.
- Organizations are looking to take advantage of big data and SIEM vendors are no different. More SIEM solutions will focus on leveraging and analyzing big data to provide superior results.
- Managed SIEM providers will continue to increase in demand for small and large organizations. Smaller organizations won't have internal resources or expertise to staff a SIEM. Larger organizations may not want to dedicate resources or decide a provider has the necessary expertise they require.
- As organizations continue to grow larger and more diverse, the ability to scale in heterogeneous environments becomes more important as SIEM products will need to keep up with the advancing technology systems in organizations.

Info-Tech Insight

As the market evolves, capabilities that were once cutting edge become default and new functionality becomes differentiating. Basic forensic analysis capabilities have become a Table Stakes capability and should no longer be used to differentiate solutions. Instead focus on advanced detection methods and usability to get the best fit for your requirements.

SIEM vendor selection / knock-out criteria: market share, mind share, and platform coverage

4.2

- SIEM solutions continue to aggregate machine data in real time for risk management through analysis and correlation to provide network event monitoring, user activity monitoring, compliance reporting, as well as store and report data for incident response, forensics, and regulatory compliance.
- For this Vendor Landscape, Info-Tech focused on those vendors that offer broad capabilities across multiple platforms and that have a strong market presence and/or reputational presence among mid- and large-sized enterprises.

Included in this Vendor Landscape:

- **AlienVault.** Provides a robust security management product with an impressive threat intelligence feed.
- **EventTracker.** While a smaller vendor, EventTracker provides a SIEM product for the resource-constrained.
- **HP.** One of the largest technology vendors in the market; provides a highly feature-rich SIEM solution in this VL.
- **IBM.** Provides strong event and log management and threat detection across networks and applications.
- **LogRhythm.** As a dedicated vendor, LogRhythm offers the most feature-rich product with the ability to adapt to trends.
- **Intel Security.** As a diverse and competitive vendor, Intel Security offers a strong and reliable SIEM product.
- **NetIQ.** Has a strong foundational SIEM offering with a competitive price point.
- **RSA.** Offers a highly advanced SIEM product garnered to large-scale, high-demand security organizations.
- **SolarWinds.** Offers a robust SIEM for resource-constrained organizations, with potential compliance needs.
- **Splunk.** As a big data software company, Splunk offers a very strong SIEM for high capacity and unique environments.

Table Stakes represent the minimum standard; without these, a product doesn't even get reviewed

The Table Stakes

Feature:	What it is:
Basic CAN	Collection from firewall and network logs, IDS logs, Windows server logs, web server logs, and various *syslog* sources
Basic Reporting	Availability of a variety of out-of-the-box reports that can be customized by the client and run on a scheduled and ad hoc basis
Basic Alerting	Logging for all correlated events and alerting via dashboard alert/email/SMS/etc. for those that exceed a given threshold or meet specific alert criteria
Basic Correlation	Out-of-the-box correlation policies for basic CAN data and baselining, acting in near real time
Basic Forensic Analysis	Ability to generate custom data queries through flexible drill down and pivot capabilities
Basic Data Management Security and Retention	Securitization of SIEM data and notable storage capabilities

What does this mean?

The products assessed in this Vendor Landscape™ meet, at the very least, the requirements outlined as Table Stakes.

Many of the vendors go above and beyond the outlined Table Stakes, some even do so in multiple categories. This section aims to highlight the products' capabilities **in excess** of the criteria listed here.

Info-Tech Insight

If Table Stakes are all you need from your SIEM solution, the only true differentiator for the organization is price. Otherwise, dig deeper to find the best price to value for your needs.

Advanced Features are the capabilities that allow for granular differentiation of market players and use case performance

4.2 Vendor Landscape Overview

Scoring Methodology

Info-Tech scored each vendor's features on a cumulative four-point scale. Zero points are awarded to features that are deemed absent or unsatisfactory, one point is assigned to features that are partially present, two points are assigned to features that require an extra purchase in the vendor's product portfolio or through a third-party, three points are assigned to features that are fully present and native to the solution, and four points are assigned to the best-of-breed native feature.

Feature	What we looked for:
Advanced Data Enrichment	Advanced CAN from various log and non-log data sources (identity, database, application, configuration, netflow, cloud, file integrity, etc.) with full packet capture ability
Advanced Correlation	Advanced pre-built policies, user-defined policies, behavioral policies, machine learning style policies, and host criticality information inclusion
Big Data Analytics	Use of big-data-style analytics through integration into purpose-built big data tools or native capabilities, all based on advanced security style analytic methods
Advanced Reporting and Alerting	Pre-built reporting and alerting libraries, customizable dashboards, compliance use-case support, various alerting options, and integration into external reporting and third-party workflow tools
Forensic Analysis Support	Advanced query capabilities against all collected data with pre-built and custom drill down, pivot, and parsing with export functions and event session reconstruction
Data Management Security and Retention	Granular access controls to system data, protection of SIEM data, system access monitoring, external storage integration and efficient data compression

For an explanation of how Advanced Features are determined, see Information Presentation – Feature Ranks (Stoplights) in the Appendix.

Advanced Features are the capabilities that allow for granular differentiation of market players and use case performance

4.2 Vendor Landscape Overview

Scoring Methodology

Info-Tech scored each vendor's features on a cumulative four-point scale. Zero points are awarded to features that are deemed absent or unsatisfactory, one point is assigned to features that are partially present, two points are assigned to features that require an extra purchase in the vendor's product portfolio or through a third-party, three points are assigned to features that are fully present and native to the solution, and four points are assigned to the best-of-breed native feature.

Feature	What we looked for:
Threat Intelligence Feed	Security threat intelligence feed integration with ability to update multiple uses and control updating behaviors
Incident Management and Remediation	Advanced detection and incident management with pre-built and customizable remediation capabilities, integration into workflow systems, and optional automatic remediation through integration
Full Security Threat Visibility	Integration with security technologies for monitoring, incident analysis and data enrichment to support ability to track and analyze series of related events
Scalability and Network Performance	The product's ability to scale horizontally and vertically, while employing various methods to reduce any latency impacts from CAN activities

For an explanation of how Advanced Features are determined, see Information Presentation – Feature Ranks (Stoplights) in the Appendix.

Vendor scoring focused on overall product attributes and vendor performance in the market

4.2 Vendor Landscape Overview

Scoring Methodology

Info-Tech Research Group scored each vendor's overall product attributes, capabilities, and market performance.

Features are scored individually as mentioned in the previous slide. The scores are then modified by the individual scores of the vendor across the product and vendor performance features.

Usability, overall affordability of the product, and the technical features of the product are considered, and scored on a five-point scale. The score for each vendor will fall between worst and best in class.

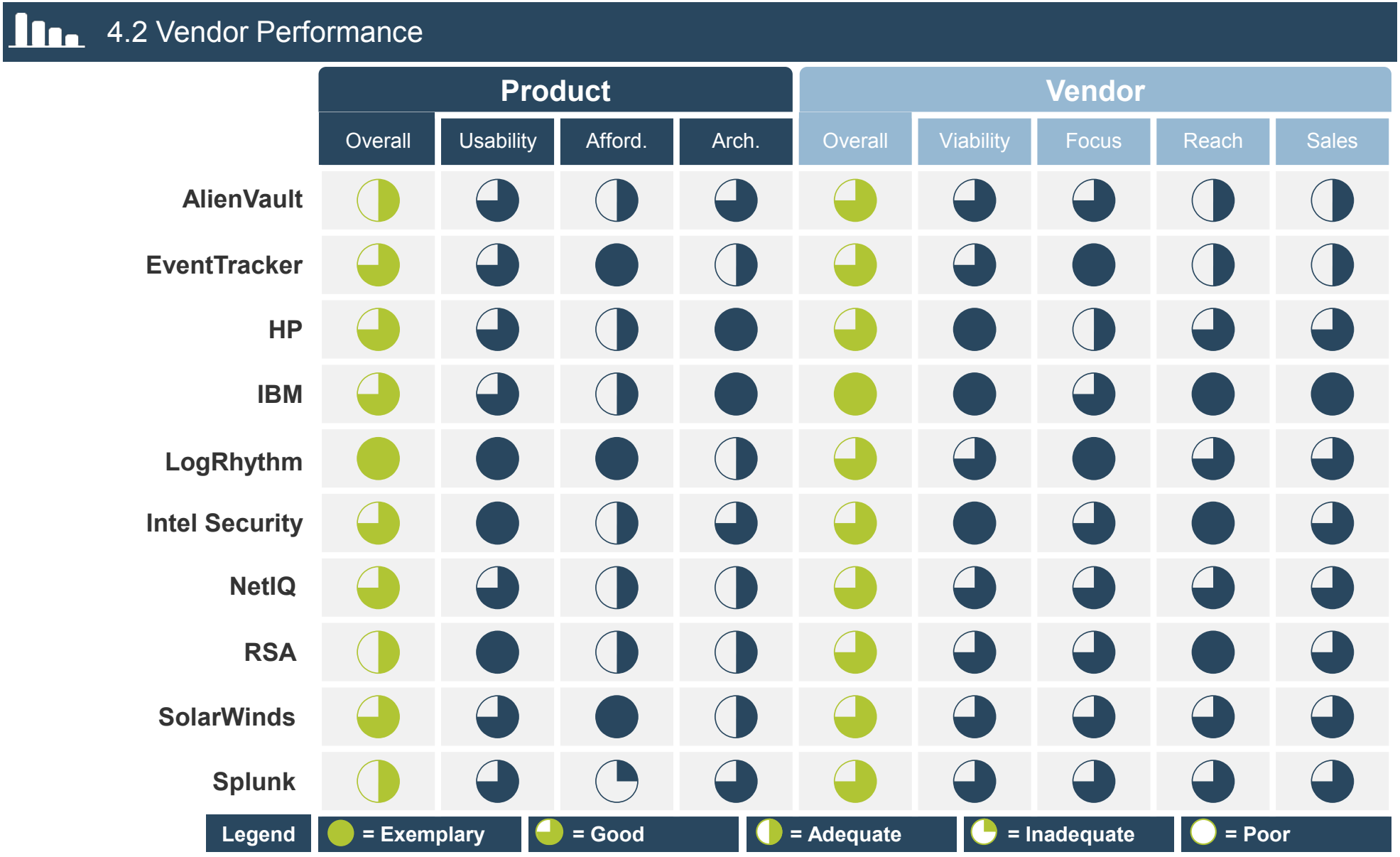
The vendor's performance in the market is evaluated across four dimensions on a five-point scale. Where the vendor places on the scale is determined by factual information, industry position, and information provided by customer references, and/or available from public sources.

Product Evaluation Features	
Usability	The administrative interfaces are intuitive and offer streamlined workflow.
Affordability	Implementing and operating the solution is affordable given the technology.
Architecture	Multiple deployment options, platform support, and data collection methods are available.

Vendor Evaluation Features	
Viability	Vendor is profitable, knowledgeable, and will be around for the long term.
Focus	Vendor is committed to a target market and the space with a product and portfolio roadmap.
Reach	Vendor offers tiered global support coverage that is easily accessible.
Sales	Vendor channel partnering, sales strategies, and sales process allow for flexible product acquisition.

Balance individual strengths to find the best fit for your enterprise

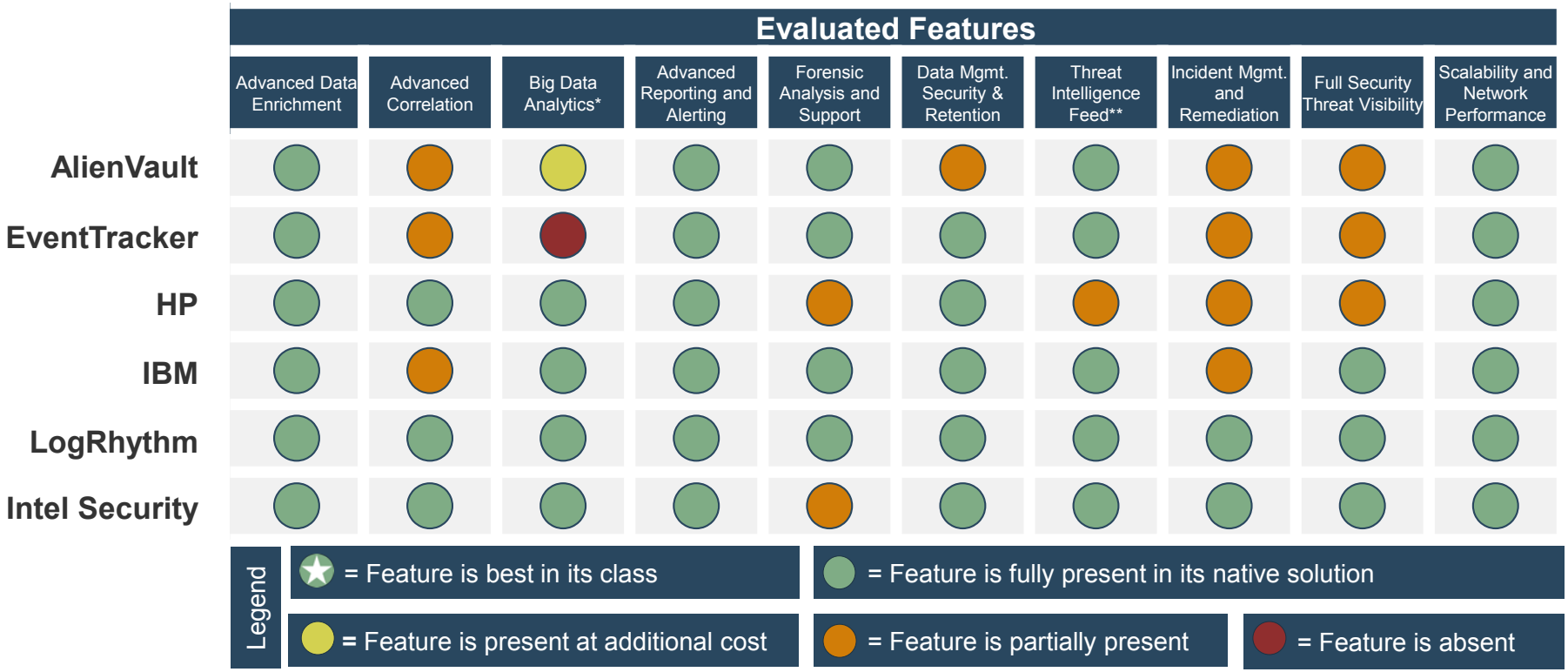
4.2 Vendor Performance



For an explanation of how the Info-Tech Harvey Balls are calculated, see Information Presentation – Criteria Scores (Harvey Balls) in the Appendix.

Balance individual strengths to find the best fit for your enterprise

4.2 Vendor Performance

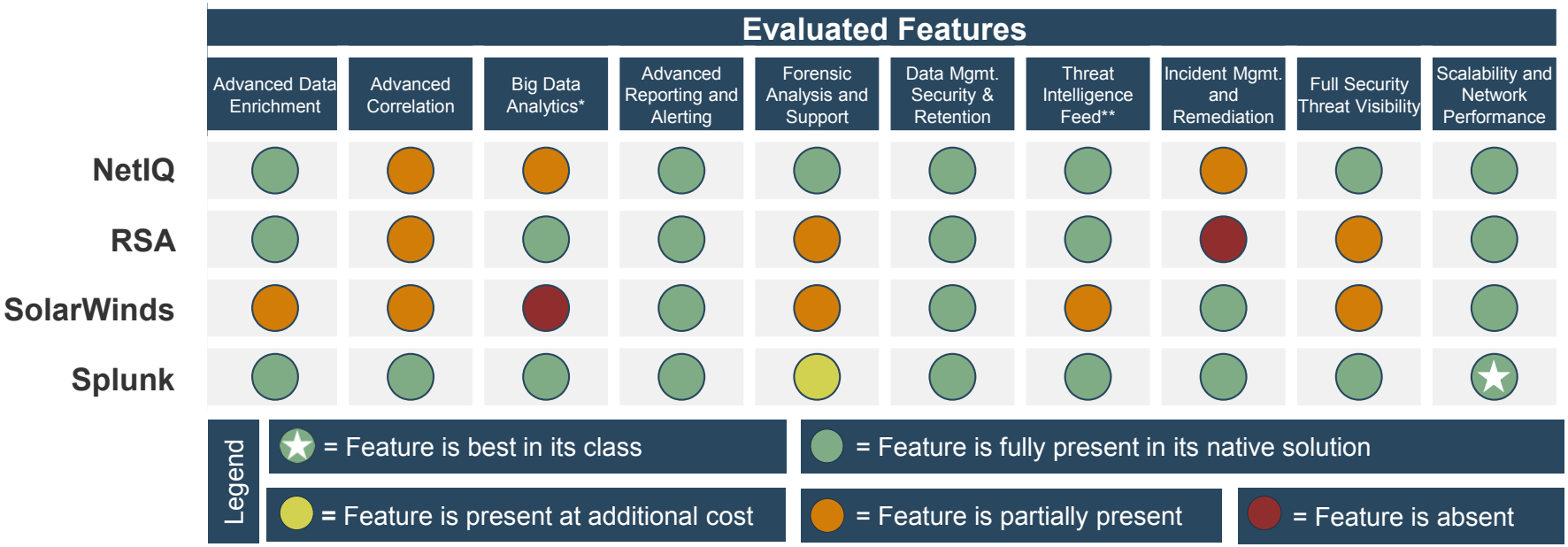


* Yellow denotes additional functionality has to be added at cost to accept big data functionality. Yellow DOES NOT denote additional cost for big data functionality, as this is true for all vendors.
** Yellow denotes an additional functionality has to be added to accept a threat intelligence feed. It DOES NOT denote additional cost for threat intelligence, as this is the case for all vendors.

For an explanation of how Advanced Features are determined, see Information Presentation – Feature Ranks (Stoplights) in the Appendix.

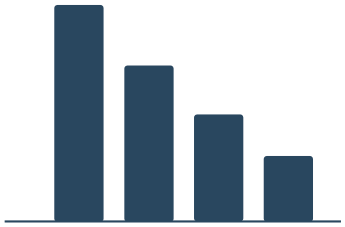
Balance individual strengths to find the best fit for your enterprise

4.2 Vendor Performance



* Yellow denotes additional functionality has to be added at cost to accept big data functionality. Yellow DOES NOT denote additional cost for big data functionality, as this is true for all vendors.
** Yellow denotes an additional functionality has to be added to accept a threat intelligence feed. It DOES NOT denote additional cost for threat intelligence, as this is the case for all vendors.

For an explanation of how Advanced Features are determined, see Information Presentation – Feature Ranks (Stoplights) in the Appendix.



4.3.1: Threat Management Use-Case Scenario

The following vendors qualified for the Threat Management use case based on their evaluation results

Qualifying Vendors

Intel Security

LogRhythm

IBM

HP

Splunk

RSA

NetIQ

AlienVault

Feature Weightings for Threat Management use-case scenario

4.3.1

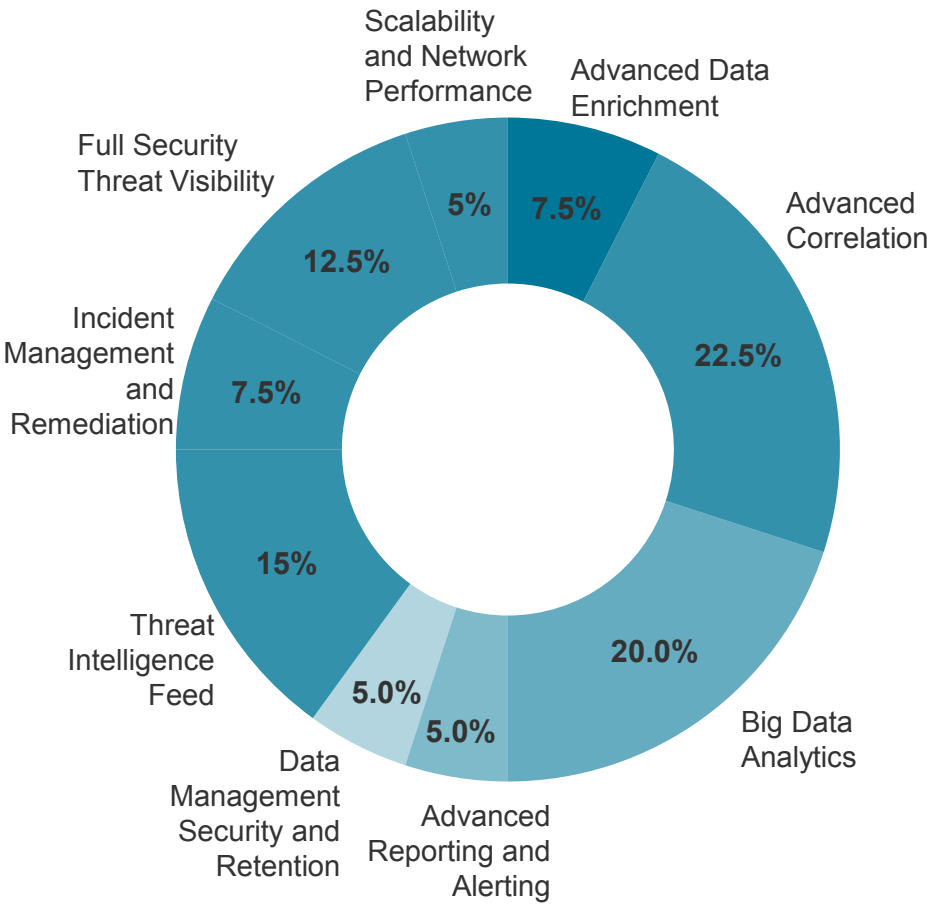
Core Features

Advanced Correlation	Advanced pre-built policies, user-defined policies, behavioral policies, machine learning style policies, and host criticality information inclusion
Threat Intelligence Feed	Security threat intelligence feed integration with ability to update multiple uses and control updating behaviors
Big Data Analytics	Use of big data style analytics through integration into purpose-built big data tools or native capabilities, all based on advanced security style analytic methods
Full Security Threat Visibility	Integration with security technologies for monitoring, incident analysis, and data enrichment to support ability to track and analyze series of related events
Incident Management and Remediation	Advanced detection and incident management with pre-built and customizable remediation capabilities, integration into workflow systems, and optional automatic remediation through integration

Additional Features

Advanced Data Enrichment
Advanced Reporting and Alerting
Scalability and Network Performance

Feature Weightings



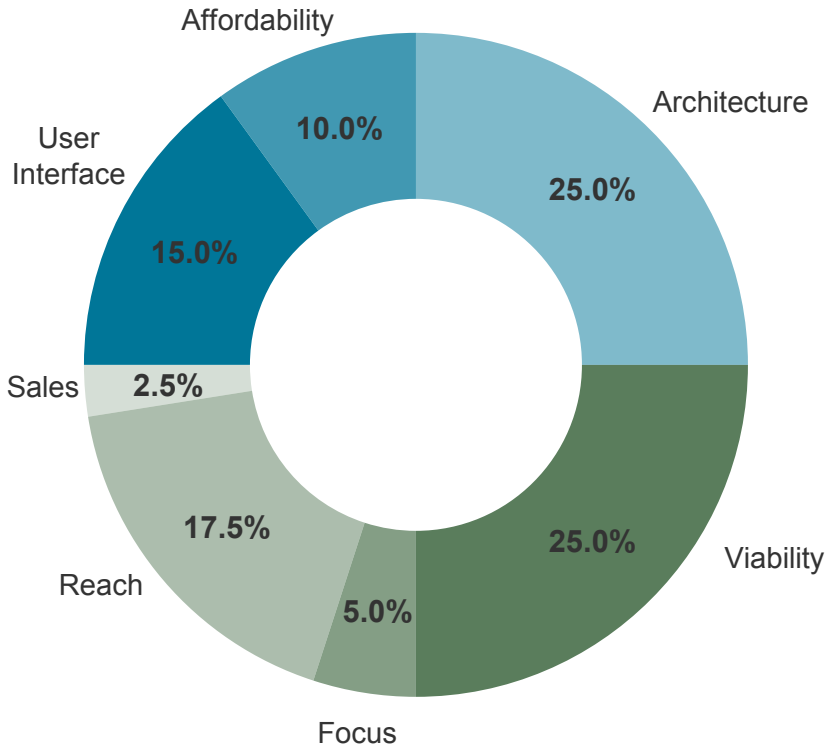
Note that vendors were also evaluated on Forensic Analysis Support, but this feature was not evaluated in this scenario.

Vendor considerations for Threat Management use-case scenario

4.3.1

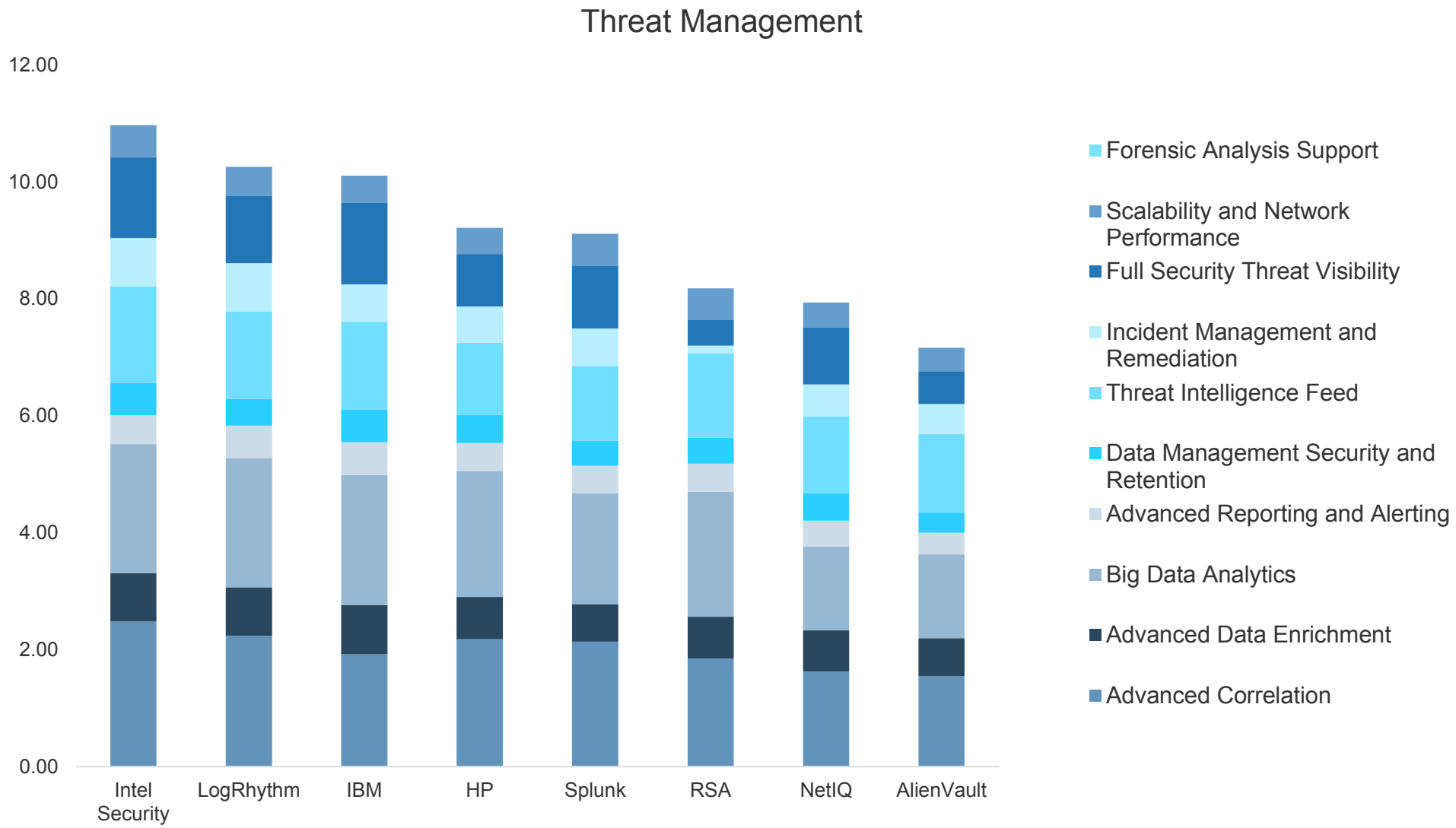
Product Evaluation Features	
Usability	Medium consideration as organizations primarily concerned with this use case often have adequate staffing and internal expertise.
Affordability	Implementing and operating the solution is affordable given the technology.
Architecture	Multiple deployment and management options on premise, off premise, and through third parties are available.

Vendor Evaluation Features	
Viability	An important consideration that demonstrates the vendor's profitability, knowledgeable base with a proven track record, and longevity.
Focus	Minor consideration to ensure the vendor is committed to their market space and building SIEM capabilities with long-term planning.
Reach	High security demand organizations need global coverage with the vendor being able to sell and provide post-sales support.
Sales	Vendor channel strategy is appropriate and the channels themselves are strong.



Vendor performance for the Threat Management use-case scenario

4.3.1



Value Index for the Threat Management use-case scenario

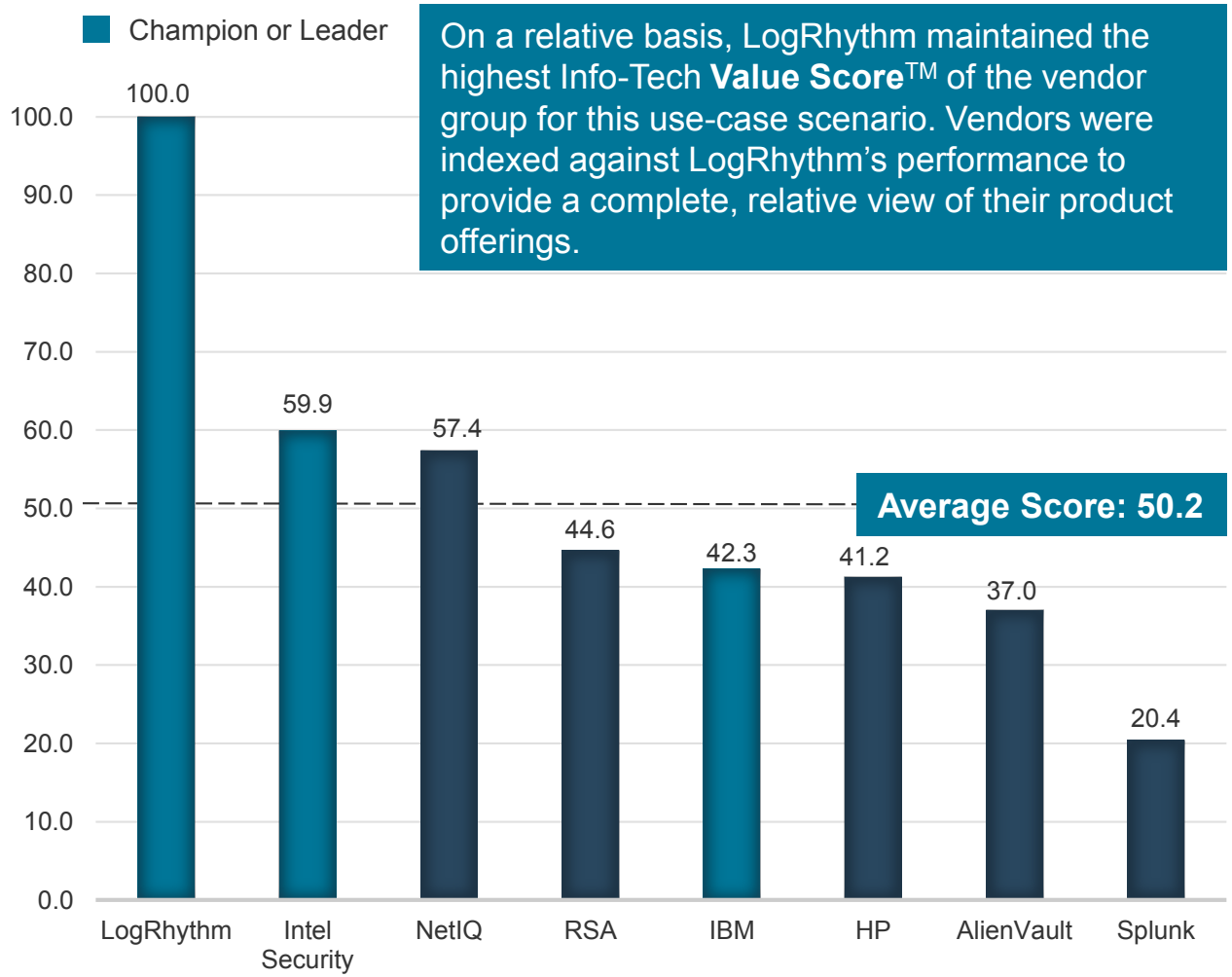
4.3.1

What is a Value Score?

The Value Score indexes each vendor's product offering and business strength **relative to its price point.** It **does not** indicate vendor ranking.

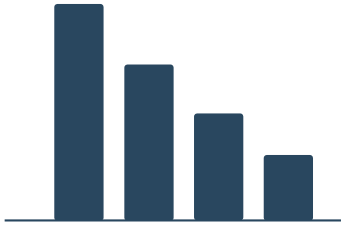
Vendors that score high offer more **bang-for-the-buck** (e.g. features, usability, stability, etc.) than the average vendor, while the inverse is true for those that score lower.

Price-conscious enterprises may wish to give the Value Score more consideration than those who are more focused on specific vendor/product attributes.



For an explanation of how Price is determined, see Information Presentation – Price Evaluation in the Appendix.

For an explanation of how the Info-Tech Value Index is calculated, see Information Presentation – Value Index in the Appendix.



4.3.2: Compliance Management Use-Case Scenario

The following vendors qualified for the Compliance Management use case based on their evaluation results

Qualifying Vendors

LogRhythm

IBM

Intel Security

EventTracker

NetIQ

SolarWinds

RSA

Feature Weightings for Compliance Management use-case scenario

4.3.2

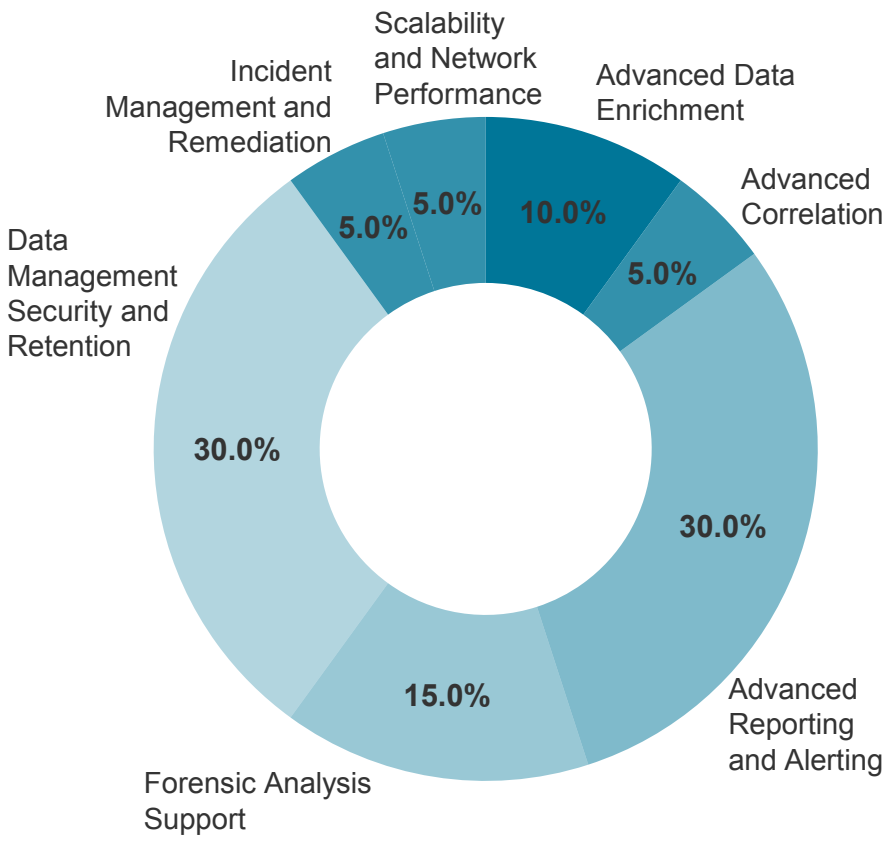
Core Features

Advanced Reporting and Alerting	Pre-built reporting and alerting libraries, customizable dashboards, compliance use-case support, various alerting options, and integration into external reporting and third-party workflow tools
Data Management Security and Retention	Granular access controls to system data, protection of SIEM data, system access monitoring, external storage integration, and efficient data compression
Advanced Data Enrichment	Advanced CAN from various log and non-log data sources (identity, database, application, configuration, netflow, cloud, file integrity, etc.) with full packet capture ability
Forensic Analysis Support	Advanced query capabilities against all collected data with pre-built and custom drill down, pivot, and parsing with export functions, and event session reconstruction

Additional Features

Advanced Correlation
Incident Management and Remediation
Scalability and Network Performance

Feature Weightings



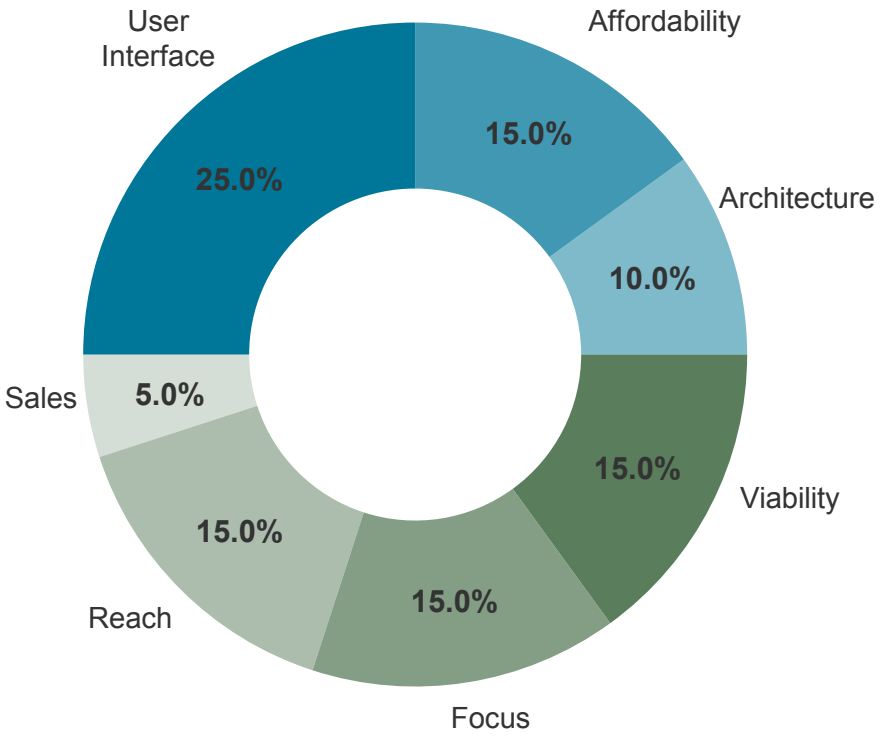
Note that vendors were also evaluated on Big Data Analytics, Threat Intelligence Feed, and Full Security Threat Visibility, but these features were not evaluated in this scenario.

Vendor considerations for the Compliance Management use-case scenario

4.3.2

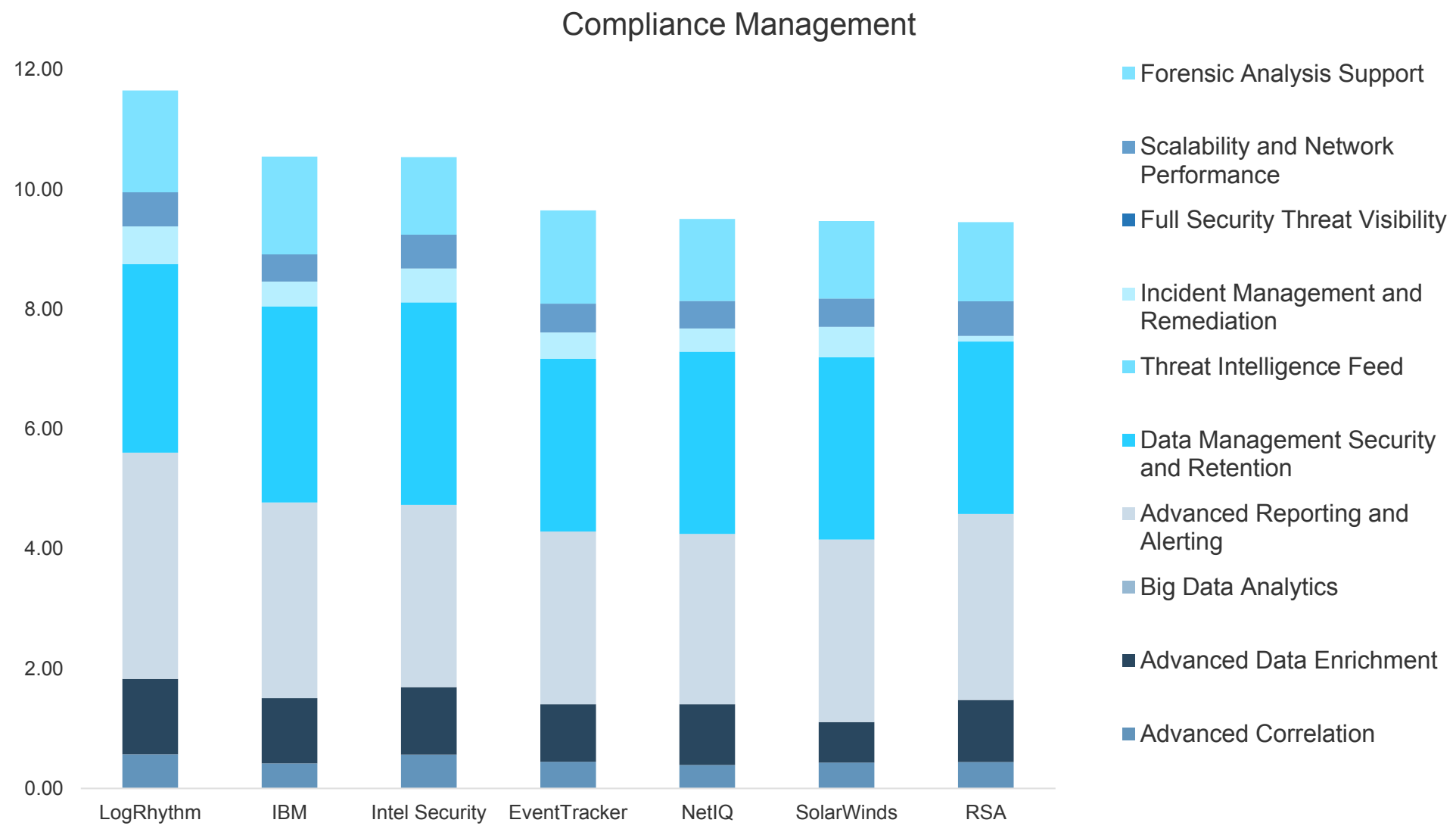
Product Evaluation Features	
Usability	An important consideration as organizations that need to prove compliance adherence require intuitive, aesthetic, and streamlined interfaces.
Affordability	Implementing and operating the solution is affordable given the technology.
Architecture	Multiple deployment and management options on premise, off premise, and through third parties are available.

Vendor Evaluation Features	
Viability	Vendor is profitable and knowledgeable and will be around for the long term.
Focus	Native compliance functionality is supported by vendor commitment to the space.
Reach	Vendor support through global coverage with post-sales support is critical when demonstrating compliance adherence.
Sales	Vendor channel partnering, sales strategies, and sales process allow for flexible product acquisition.



Vendor performance for the Compliance Management use-case scenario

4.3.2



Value Index for the Compliance Management use-case scenario

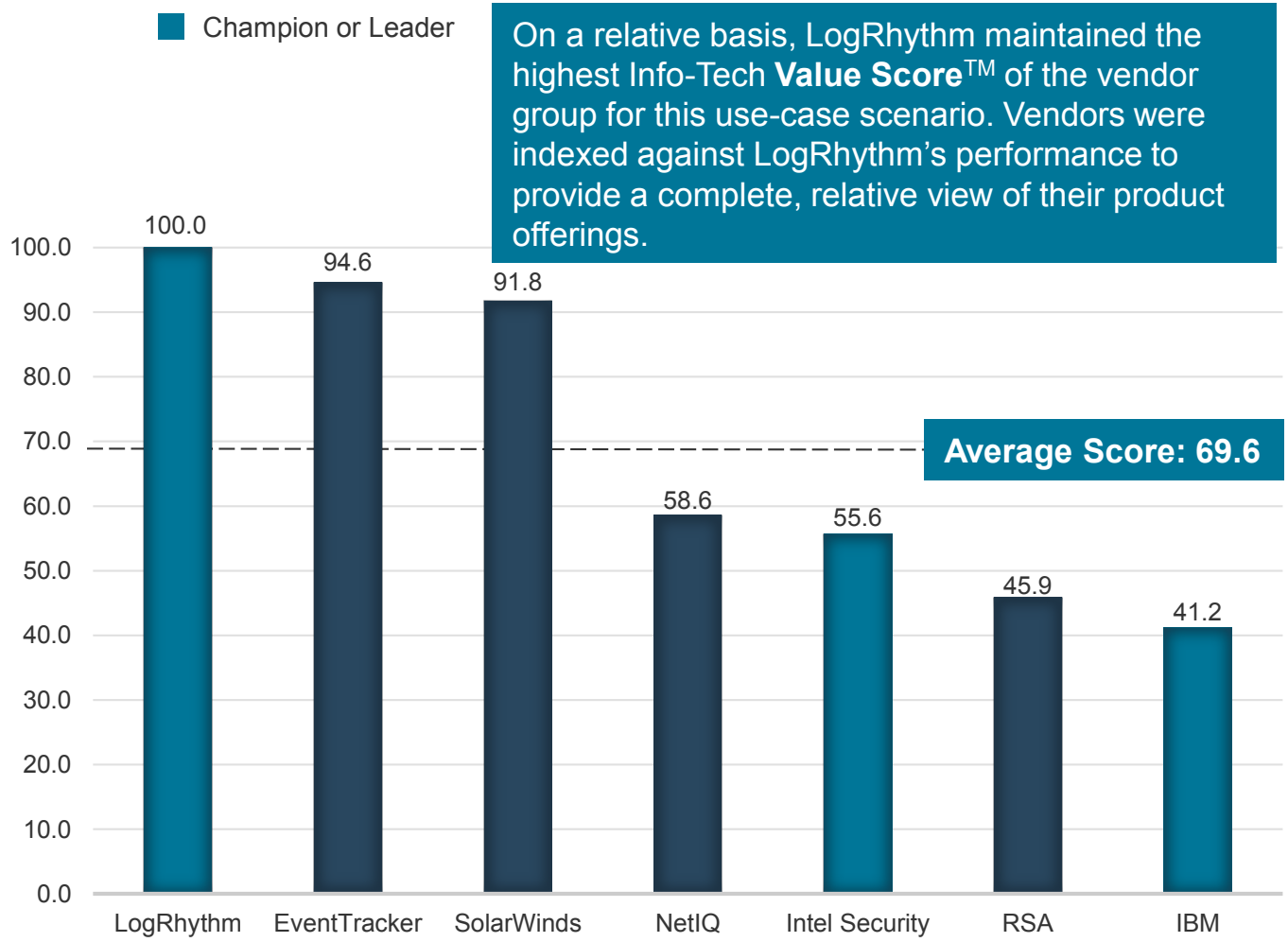
4.3.2

What is a Value Score?

The Value Score indexes each vendor's product offering and business strength **relative to its price point.** It **does not** indicate vendor ranking.

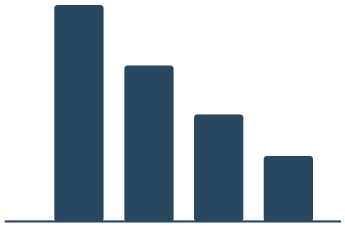
Vendors that score high offer more **bang-for-the-buck** (e.g. features, usability, stability, etc.) than the average vendor, while the inverse is true for those that score lower.

Price-conscious enterprises may wish to give the Value Score more consideration than those who are more focused on specific vendor/product attributes.



For an explanation of how Price is determined, see Information Presentation – Price Evaluation in the Appendix.

For an explanation of how the Info-Tech Value Index is calculated, see Information Presentation – Value Index in the Appendix.



4.3.3: Management of Security Events Use-Case Scenario

The following vendors qualified for the Management of Security Events use case based on their evaluation results

Qualifying Vendors

LogRhythm

Intel Security

IBM

RSA

Splunk

HP

NetIQ

Feature Weightings for Management of Security Events use-case scenario

4.3.3

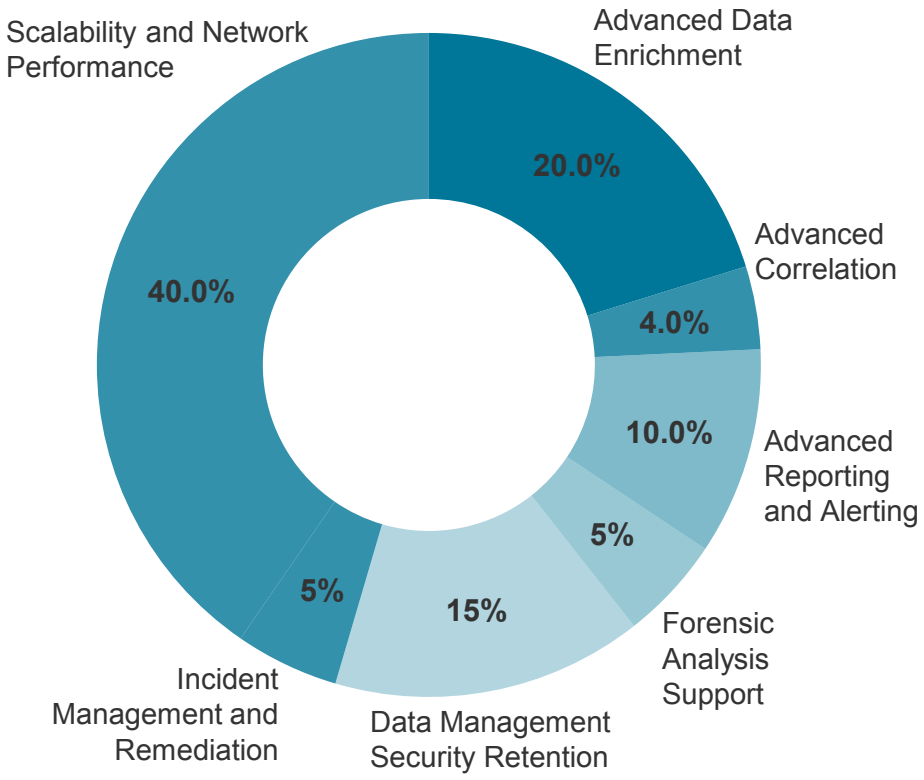
Core Features

Scalability and Network Performance	The product's ability to scale horizontally and vertically, while employing various methods to reduce any latency impacts from CAN activities, is critical for high capacity and performance-based SIEM solutions
Advanced Data Enrichment	Advanced CAN from various log and non-log data sources (identity, database, application, configuration, netflow, cloud, file integrity, etc.) with full packet capture ability
Data Management Security and Retention	Granular access controls to system data, protection of SIEM data, system access monitoring, external storage integration, and efficient data compression

Additional Features

Advanced Correlation
Advanced Reporting and Alerting
Forensic Analysis Support
Incident Management and Remediation

Feature Weightings



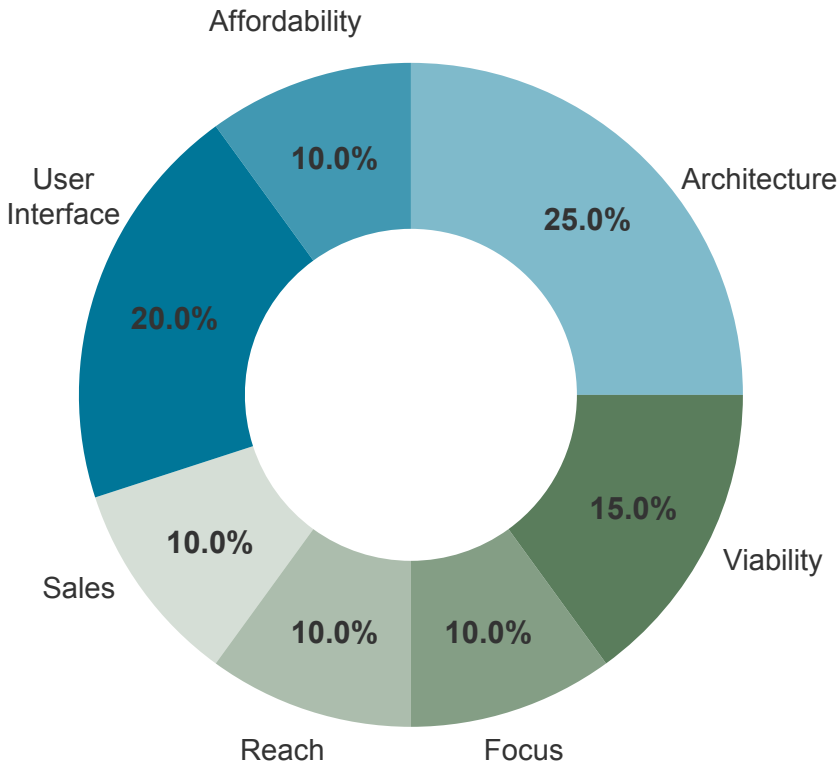
Note that vendors were also evaluated on Big Data Analytics, Threat Intelligence Feed, and Full Security Threat Visibility, but these features were not evaluated in this scenario.

Vendor considerations for Management of Security Events use-case scenario

4.3.3

Product Evaluation Features	
Usability	The administrative interfaces are intuitive, aesthetically pleasing, and offer streamlined workflow.
Affordability	Implementing and operating the solution is affordable given the technology.
Architecture	Critical component to allow scalability and flexibility through multiple deployment and management options on premise, off premise, and through third parties.

Vendor Evaluation Features	
Viability	Vendor is profitable and knowledgeable and will be around for the long term.
Focus	Important component to ensure the vendor is committed to high demand use-case support with a supporting portfolio roadmap.
Reach	Important component due to customers' complex, often distributed, IT environments requiring full support capabilities.
Sales	Vendor channel strategy is appropriate and the channels themselves are strong.



Vendor performance for the Management of Security Events use-case scenario

4.3.3

Value Index for the Management of Security Events use-case scenario

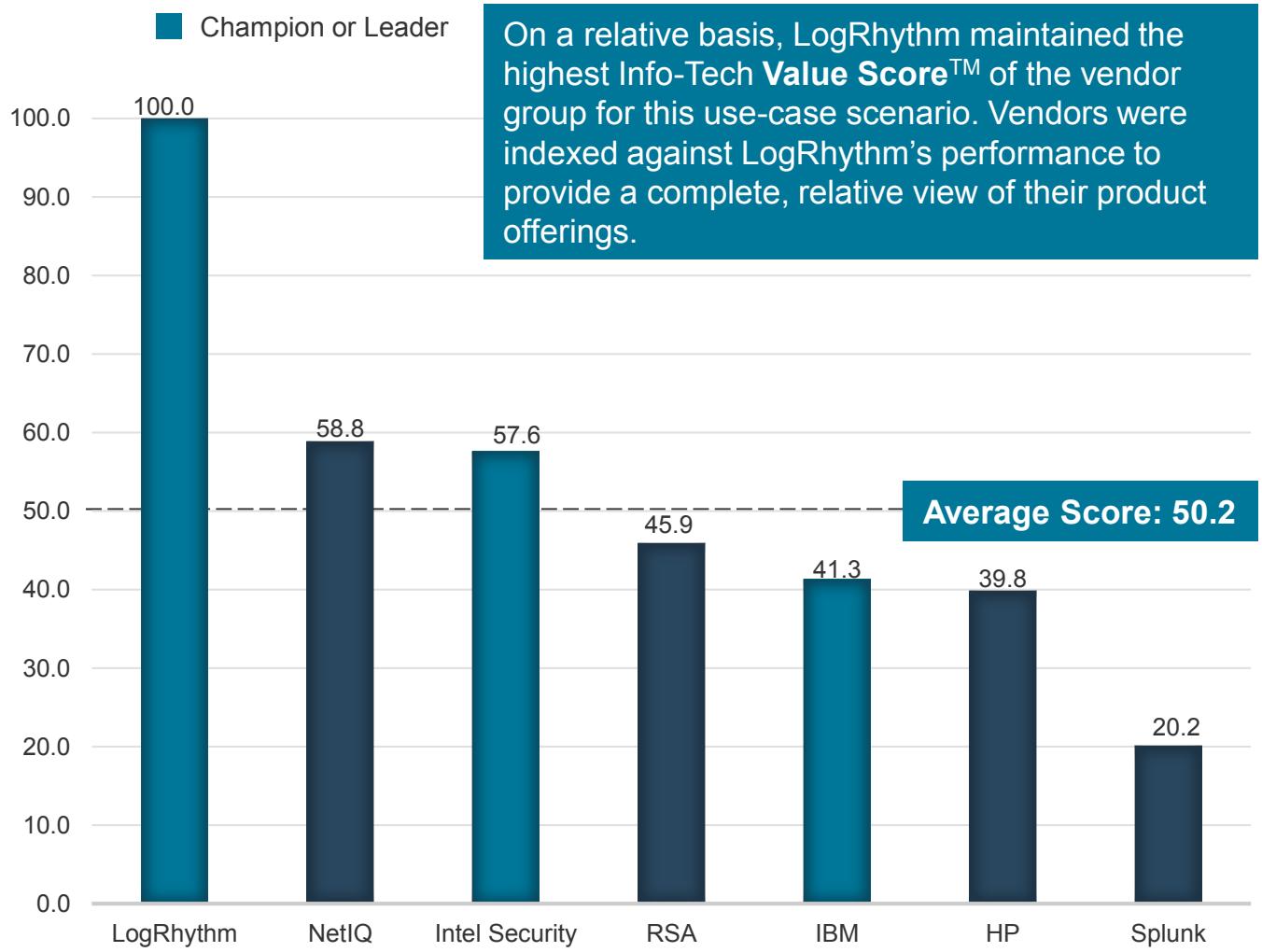
4.3.3

What is a Value Score?

The Value Score indexes each vendor's product offering and business strength **relative to its price point.** It **does not** indicate vendor ranking.

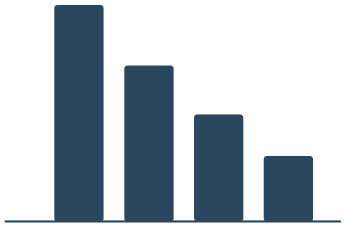
Vendors that score high offer more **bang-for-the-buck** (e.g. features, usability, stability, etc.) than the average vendor, while the inverse is true for those that score lower.

Price-conscious enterprises may wish to give the Value Score more consideration than those who are more focused on specific vendor/product attributes.



For an explanation of how Price is determined, see Information Presentation – Price Evaluation in the Appendix.

For an explanation of how the Info-Tech Value Index is calculated, see Information Presentation – Value Index in the Appendix.



4.3.4: SIEM Small Deployment Use-Case Scenario

The following vendors qualified for the SIEM Small Deployment use case based on their evaluation results

Qualifying Vendors

LogRhythm

SolarWinds

EventTracker

Intel Security

NetIQ

IBM

HP

Feature Weightings for SIEM Small Deployment use-case scenario

4.3.4

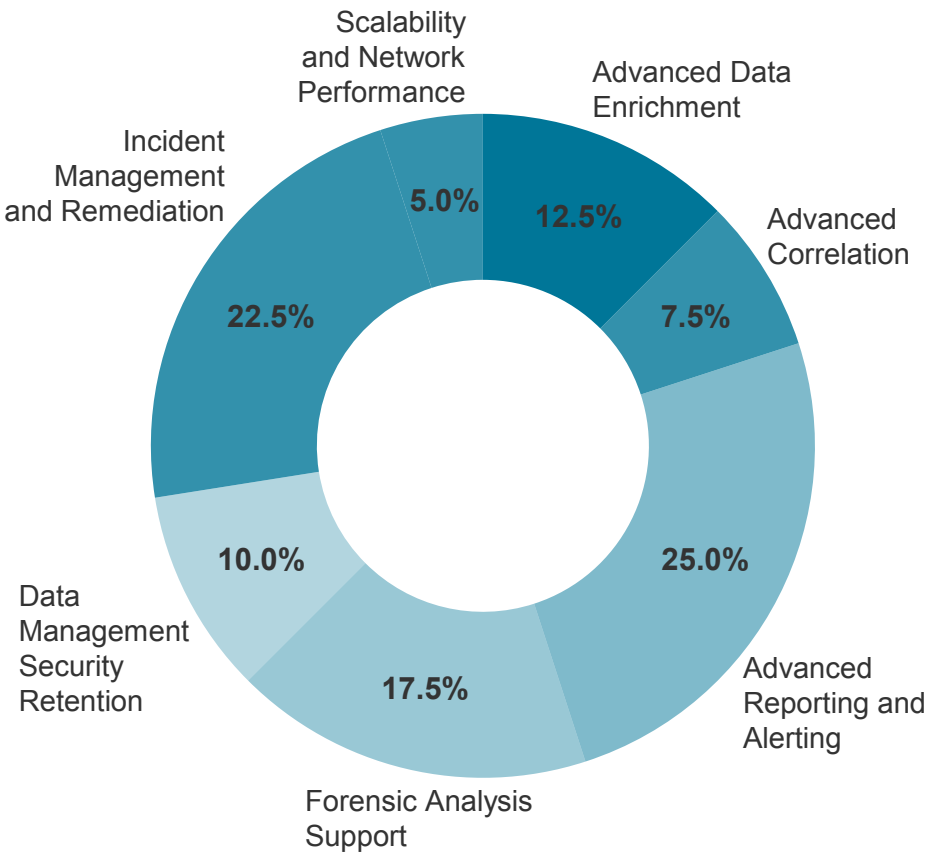
Core Features

Incident Management and Remediation	Advanced detection and incident management with pre-built and customizable remediation capabilities, integration into workflow systems, and optional automatic remediation through integration
Advanced Reporting and Alerting	Pre-built reporting and alerting libraries, customizable dashboards, compliance use-case support, various alerting options, and integration into external reporting and third-party workflow tools
Forensic Analysis Support	Advanced query capabilities against all collected data with pre-built and custom drill down, pivot, and parsing with export functions and event session reconstruction
Advanced Data Enrichment	Advanced CAN from various log and non-log data sources (identity, database, application, configuration, netflow, cloud, file integrity, etc.) with full packet capture ability

Additional Features

Advanced Correlation
Data Management Security and Retention

Feature Weightings



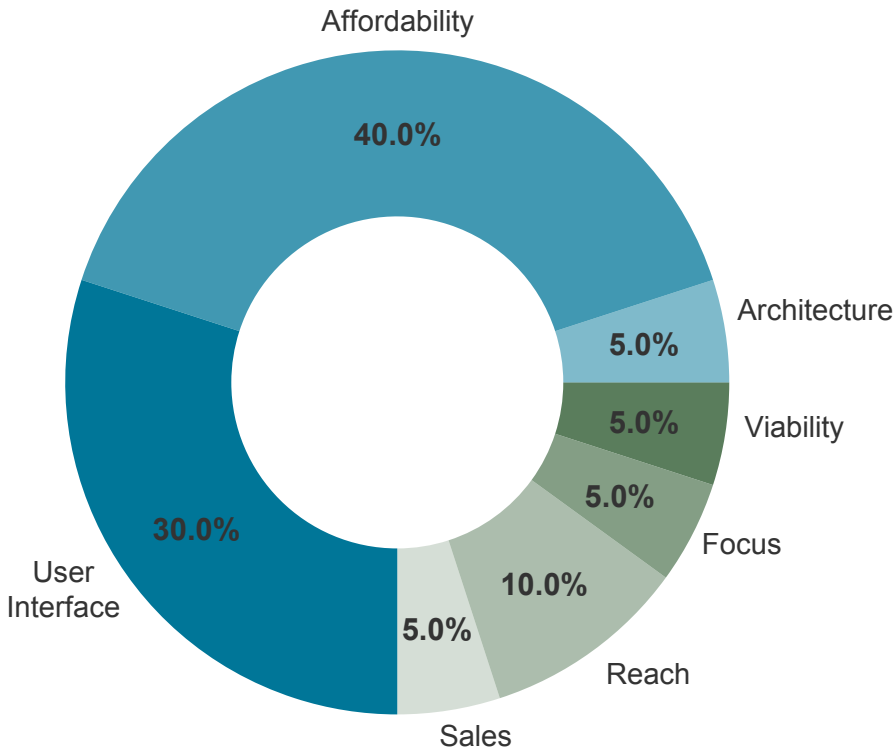
Note that vendors were also evaluated on Big Data Analytics, Threat Intelligence Feed, and Full Security Threat Visibility, but these features were not evaluated in this scenario.

Vendor considerations for SIEM Small Deployment use-case scenario

4.3.4

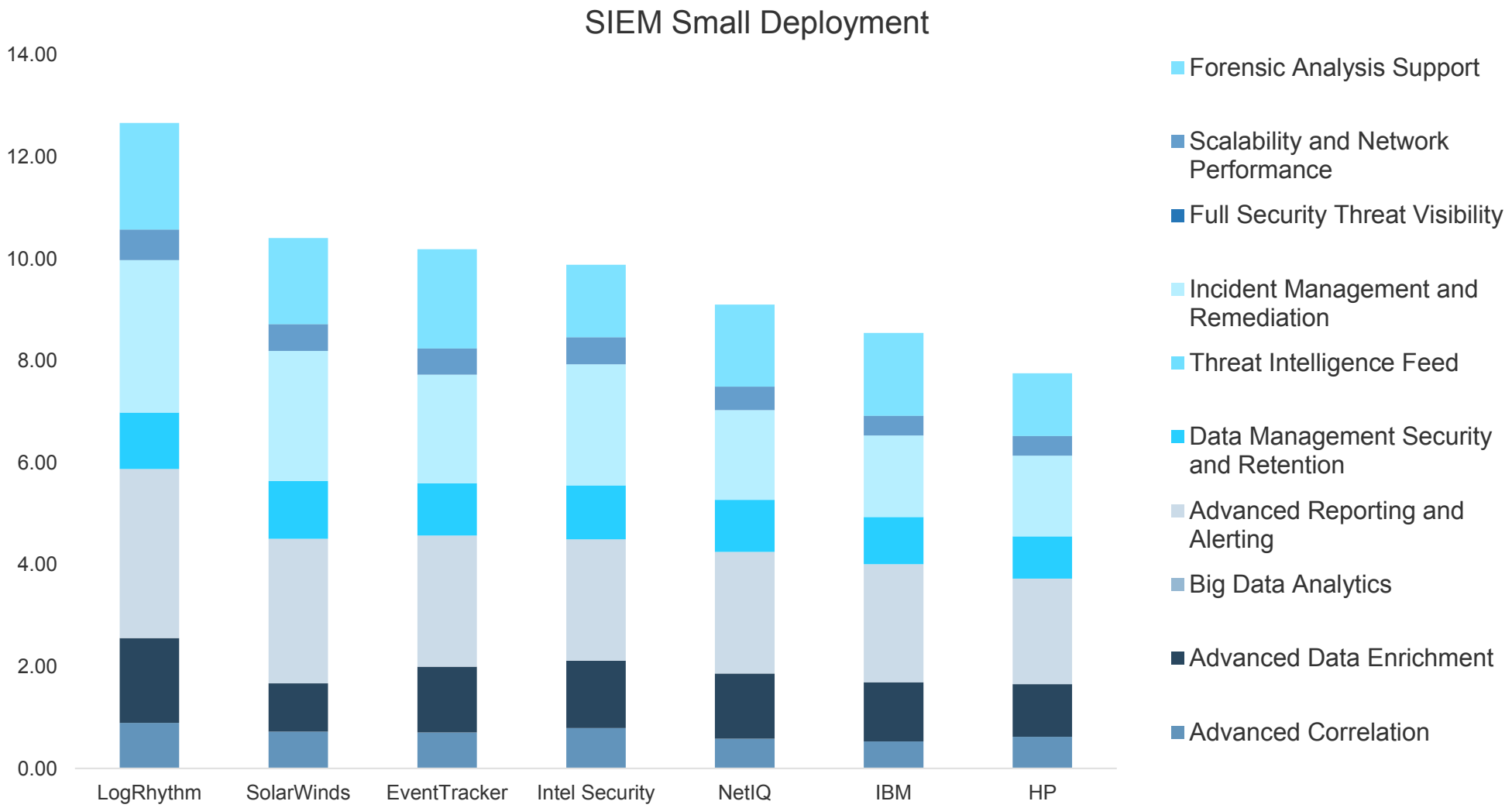
Product Evaluation Features	
Usability	Critical component to ensure resource- or expertise-constrained organizations may still realize strong value.
Affordability	Smaller deployments need a low price tag to support low budget organizations' business cases for SIEM technology.
Architecture	Multiple deployment and management options on premise, off premise, and through third parties are available.

Vendor Evaluation Features	
Viability	Vendor is profitable and knowledgeable and will be around for the long term.
Focus	Vendor is committed to a target market and the space with a product and portfolio roadmap.
Reach	Resource constrained organizations need strong support coverage.
Sales	Vendor channel partnering, sales strategies, and sales process allow for flexible product acquisition.



Vendor performance for the SIEM Small Deployment use-case scenario

4.3.4



Value Index for the SIEM Small Deployment use-case scenario

4.3.4

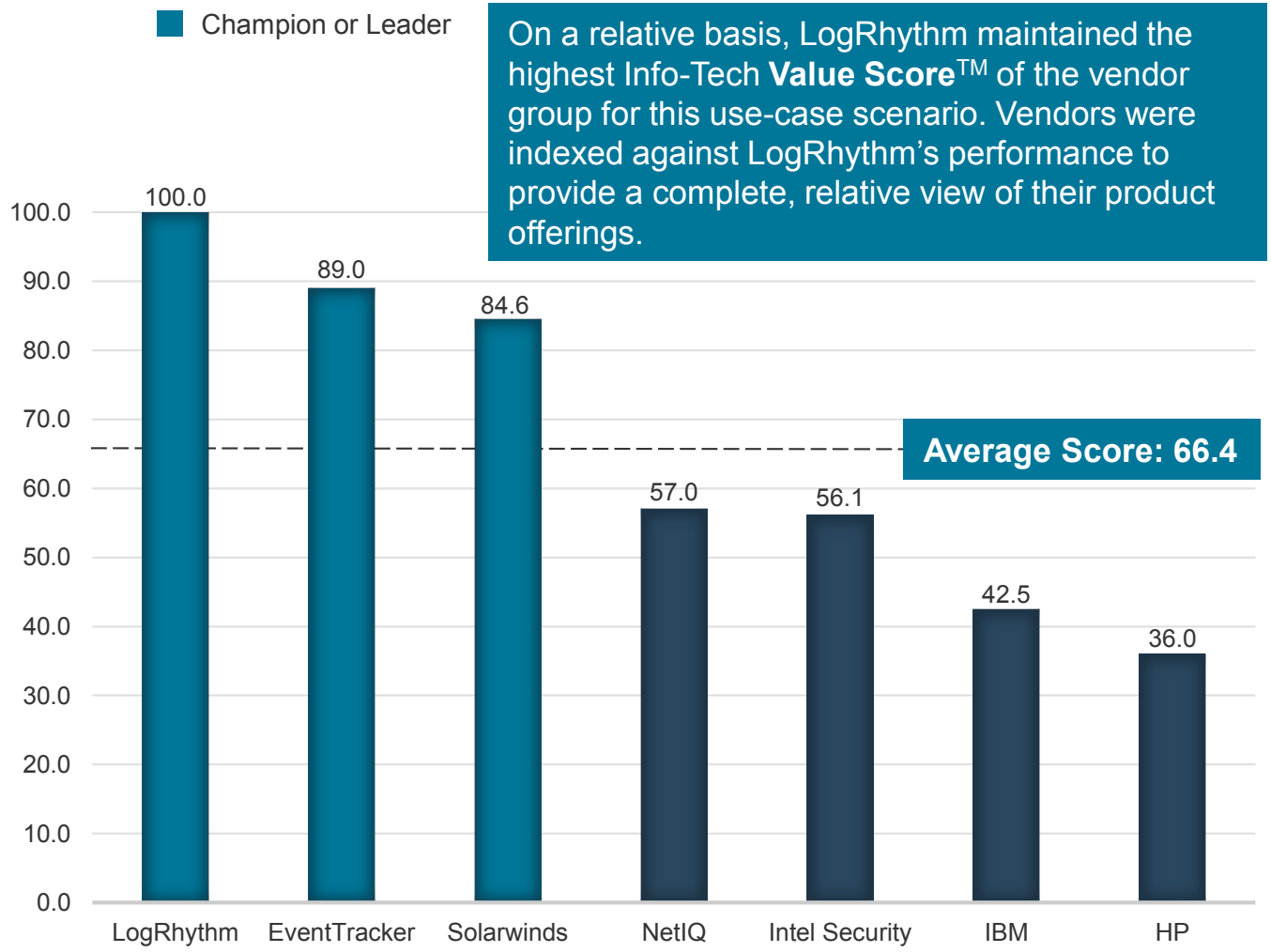
What is a Value Score?

The Value Score indexes each vendor's product offering and business strength **relative to its price point.** It **does not** indicate vendor ranking.

Vendors that score high offer more **bang-for-the-buck** (e.g. features, usability, stability, etc.) than the average vendor, while the inverse is true for those that score lower.

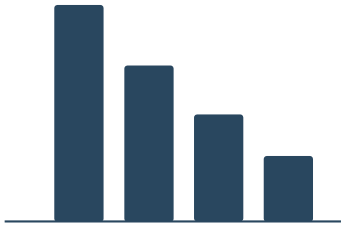
Price-conscious enterprises may wish to give the Value Score more consideration than those who are more focused on specific vendor/product attributes.

On a relative basis, LogRhythm maintained the highest Info-Tech **Value Score**™ of the vendor group for this use-case scenario. Vendors were indexed against LogRhythm's performance to provide a complete, relative view of their product offerings.



For an explanation of how Price is determined, see Information Presentation – Price Evaluation in the Appendix.

For an explanation of how the Info-Tech Value Index is calculated, see Information Presentation – Value Index in the Appendix.



4.3.5: Risk Management Use-Case Scenario

The following vendors qualified for the Risk Management use case based on their evaluation results

Qualifying Vendors

LogRhythm

Intel Security

IBM

HP

Splunk

NetIQ

RSA

Feature Weightings for the Risk Management use-case scenario

4.3.5

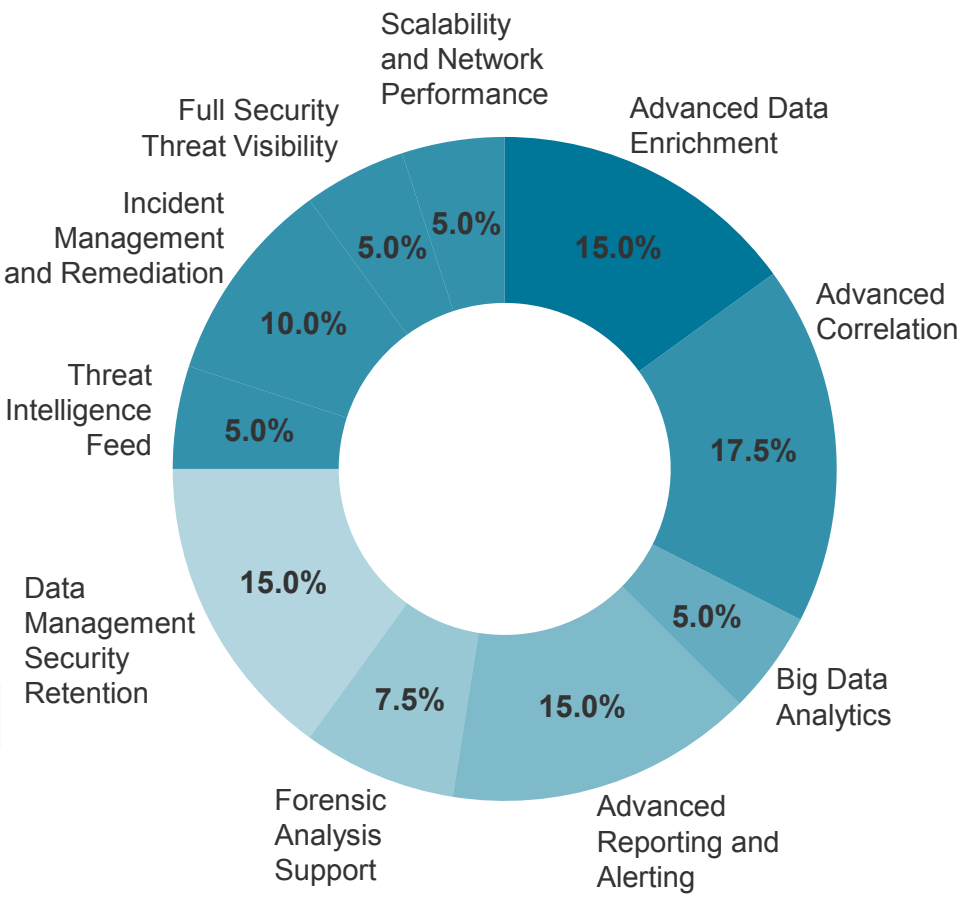
Core Features

Advanced Reporting & Alerting	Pre-built reporting and alerting libraries, customizable dashboards, compliance use-case support, various alerting options, and integration into external reporting and third-party workflow tools
Advanced Data Enrichment	Advanced CAN from various log and non-log data sources (identity, database, application, configuration, netflow, cloud, file integrity, etc.) with full packet capture ability
Forensic Analysis Support	Advanced query capabilities against all collected data with pre-built and custom drill down, pivot, and parsing with export functions and event session reconstruction
Data Mgmt. Security & Retention	Granular access controls to system data, protection of SIEM data, system access monitoring, external storage integration, and efficient data compression
Incident Management & Remediation	Advanced detection and incident management with pre-built and customizable remediation capabilities, integration into workflow systems, and optional automatic remediation through integration

Additional Features

Advanced Correlation
Big Data Analytics
Threat Intelligence Feed
Full Security Threat Visibility
Scalability and Network Performance

Feature Weightings

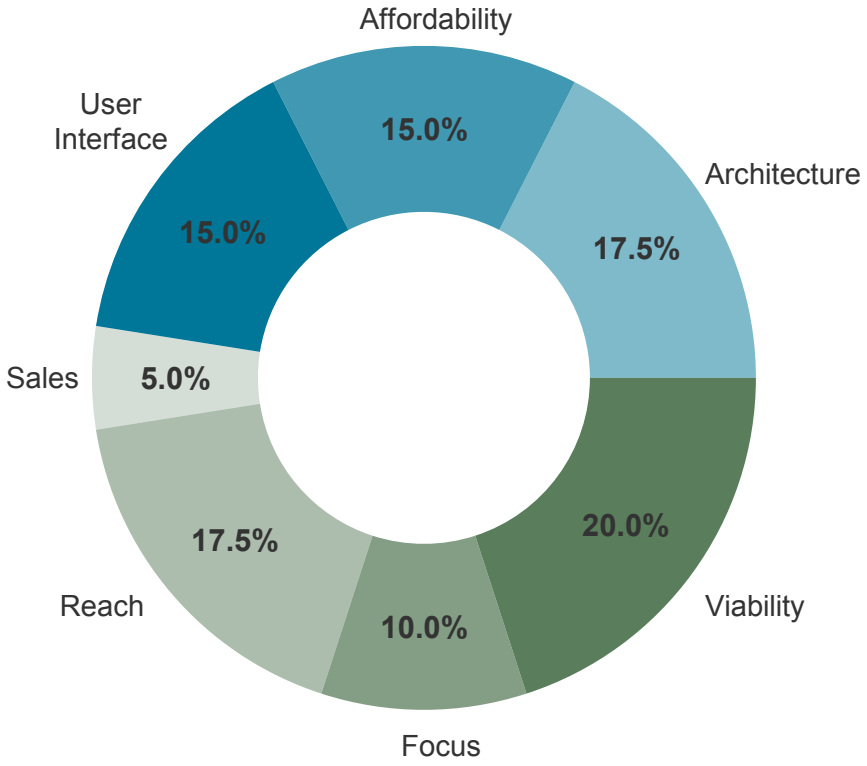


Vendor considerations for the Risk Management use-case scenario

4.3.5

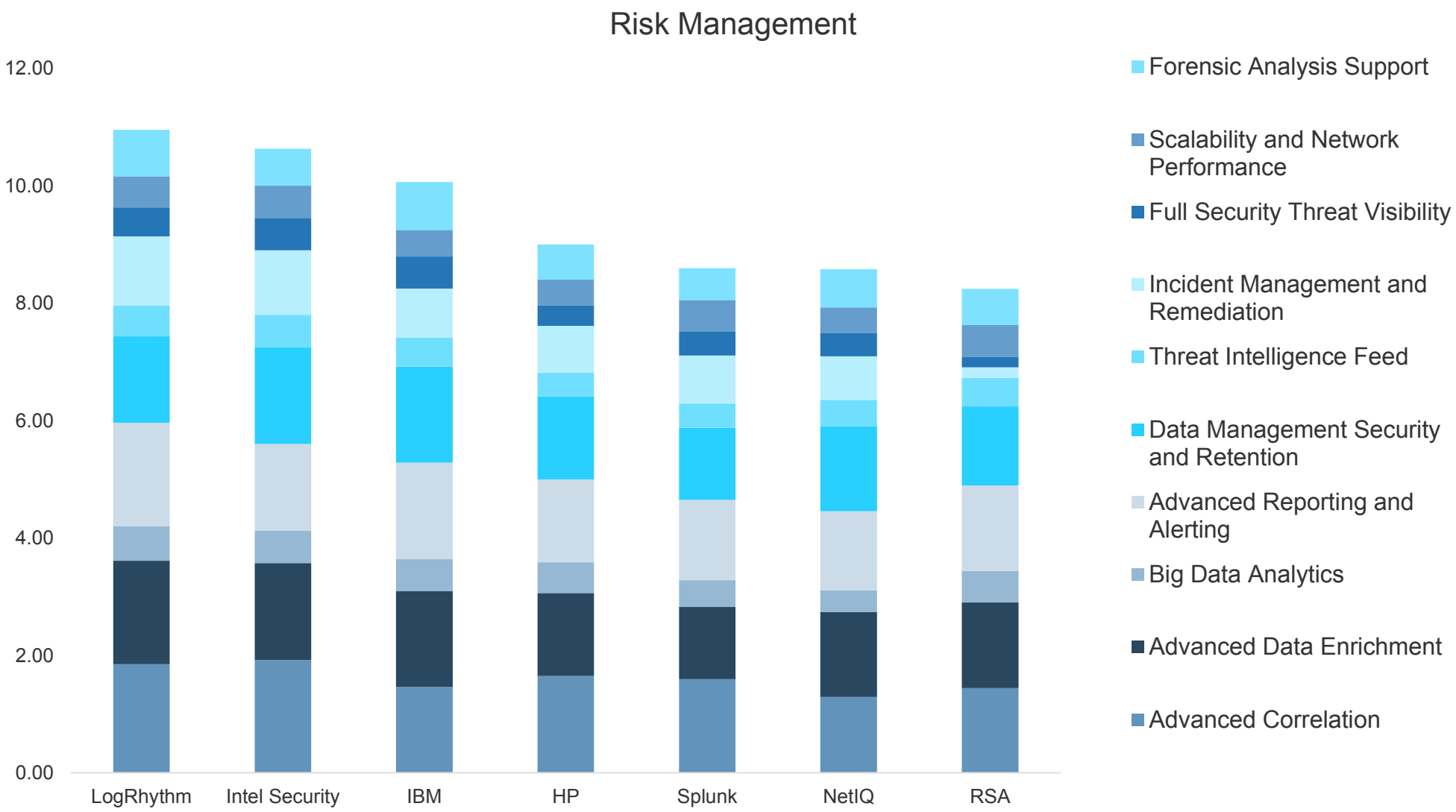
Product Evaluation Features	
Usability	The administrative interfaces are intuitive, aesthetically pleasing, and offer streamlined workflow.
Affordability	Implementing and operating the solution is affordable given the technology.
Architecture	Multiple deployment and management options on premise, off premise, and through third parties are available.

Vendor Evaluation Features	
Viability	Vendor is profitable and knowledgeable and will be around for the long term.
Focus	Vendor is committed to a target market and the space with a product and portfolio roadmap.
Reach	Vendor offers tiered global support coverage that is easily accessible.
Sales	Vendor channel partnering, sales strategies, and sales process allow for flexible product acquisition.



Vendor performance for the Risk Management use-case scenario

4.3.5



Value Index for the Risk Management scenario

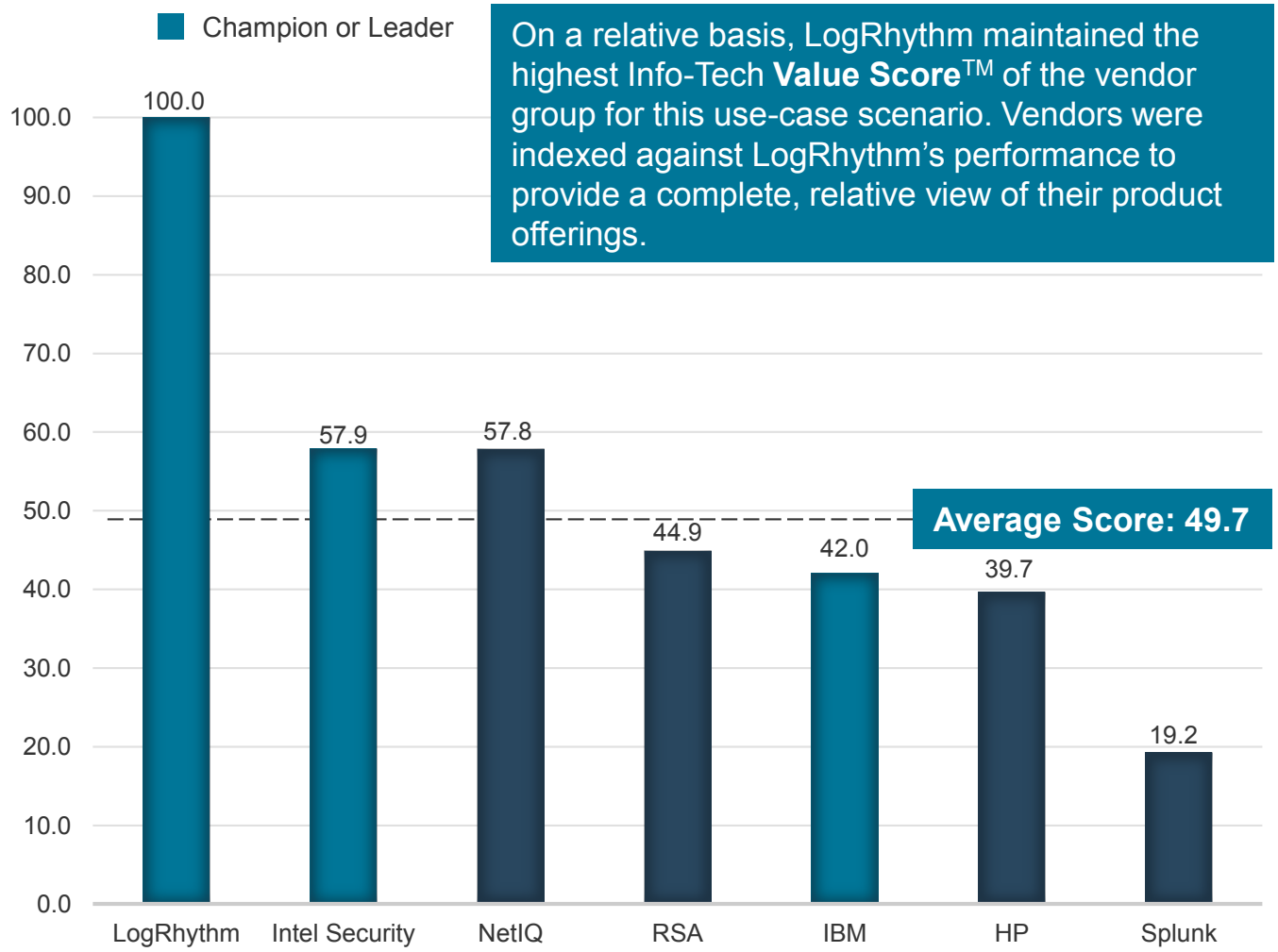
4.3.5

What is a Value Score?

The Value Score indexes each vendor's product offering and business strength **relative to its price point.** It **does not** indicate vendor ranking.

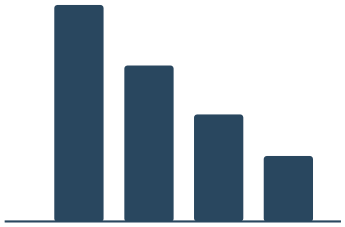
Vendors that score high offer more **bang-for-the-buck** (e.g. features, usability, stability, etc.) than the average vendor, while the inverse is true for those that score lower.

Price-conscious enterprises may wish to give the Value Score more consideration than those who are more focused on specific vendor/product attributes.



For an explanation of how Price is determined, see Information Presentation – Price Evaluation in the Appendix.

For an explanation of how the Info-Tech Value Index is calculated, see Information Presentation – Value Index in the Appendix.



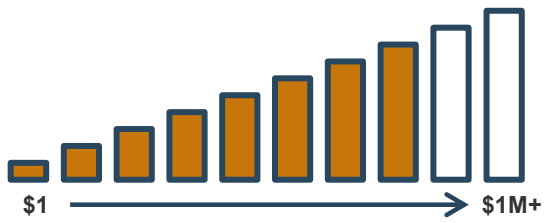
4.4: Vendor Profiles and Scoring

The USM platform offers traditional SIEM functionality with other major security capabilities built into the product

Vendor Landscape

Product:	AlienVault Unified Security Management (USM)
Employees:	175
Headquarters:	San Mateo, CA
Website:	alienvault.com
Founded:	2007, SIEM market in 2011
Presence:	Privately held

3 year TCO for this solution falls into pricing tier 8, between $250,000 and $500,000



Pricing provided by vendor

Overview

- AlienVault's USM is an all-in-one platform that combines several security capabilities (asset discovery, threat detection, vulnerability assessment, behavioral monitoring, in addition to SIEM) with integrated expert threat intelligence.

Strengths

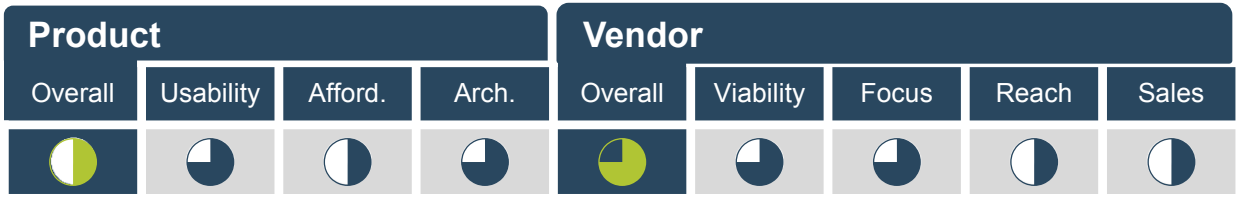
- Combining strong detection, monitoring and continuously updated threat intelligence, AlienVault USM has shown to provide robust data enrichment and advanced event correlation.
- In particular, AlienVault has an extensive threat intelligence feed that is regularly updated from open sources, as well as its own research lab.

Challenges

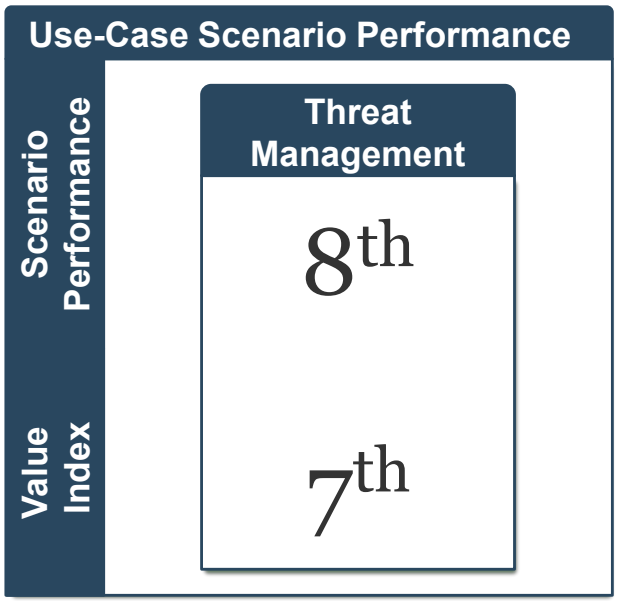
- The AlienVault USM lacks native integration to big data integration, which is a step that many SIEM providers have been taking advantage of in the past year.
- AlienVault as a vendor does not have a great deal of international support in varying countries and has a lack of different languages.

The USM platform is designed so that mid-market organizations can defend themselves under one pane of glass

Vendor Landscape



Use-Case Scenario Performance



Info-Tech Recommends:

Organizations with mid-level threat concerns and preference to unified management tools should shortlist Alien Vault.

Although often not identified as a SIEM product, AlienVault USM is a shortlist candidate for any organization seeking a threat management use case. AlienVault can be configured to send information to a purpose-built big data repository.

AlienVault Labs' threat research team provides customers with regular updates (approx. every 30 minutes) of real-time threat data, including patterns and definitions of new threats and how to remediate those threats.

AlienVault places a high importance on the ease of use of the product and the initial deployment. This makes the USM an ideal fit for mid-market organizations that are resource-constrained in budget and staffing, but still need to protect against advanced threats.

Features

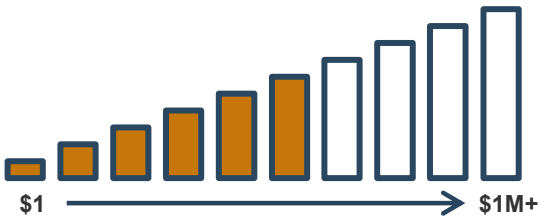
Aimed at the small to mid market, EventTracker has a quick time to value with multiple out-of-the-box features

Vendor Landscape

Product:	EventTracker Enterprise
Employees:	96
Headquarters:	Columbia, MD
Website:	eventtracker.com
Founded:	2000, SIEM market in 2001
Presence:	Privately held

EventTracker
www.eventtracker.com

3 year TCO for this solution falls into pricing tier 6, between $50,000 and $100,000



Pricing provided by vendor

Overview

- While EventTracker may be a smaller vendor, EventTracker Enterprise has proven to be a simplified SIEM that is focused on helping small to medium organizations that are often resource-constrained.

Strengths

- EventTracker enables customers to take advantage of a tailored RunBook that details the regular activities that must be carried out.
- With a strong focus on legal and regulatory compliance, EventTracker enables customers to pass audits and meet requirements.

Challenges

- Because it is a smaller organization, EventTracker does not have a large international support presence, which may be desirable for customers with worldwide offices.
- Limited data collection and enrichment narrowing network visibility.
- No integration into third-party reporting tools or ticket/workflow tools limits full reporting capabilities often required by organizations.

Basic detection and monitoring capabilities are supported by strong operations, reporting, and usability

Vendor Landscape

Product				Vendor				
Overall	Usability	Afford.	Arch.	Overall	Viability	Focus	Reach	Sales

Use-Case Scenario Performance

	Compliance Management	SIEM Small Deployment
Scenario Performance	4th	VENDOR LANDSCAPE AWARD – LEADER – INFO-TECH
Value Index	2nd	2nd

Info-Tech Recommends:

EventTracker has a very short deployment time, allowing organizations to realize a quick time to value. Designed for resource-constrained organizations, the graphic interface is a simplistic model that allows users to easily customize and define dashboards. EventTracker uniquely receives the data by the virtual collection point where data is indexed and detection analysis performed. The data is then stored and is only normalized when it is queried. This is a "fast in" model, but limits detection to only known incidents. Small to mid-sized organizations that require log management and compliance management with limited major threats should shortlist EventTracker.

Features

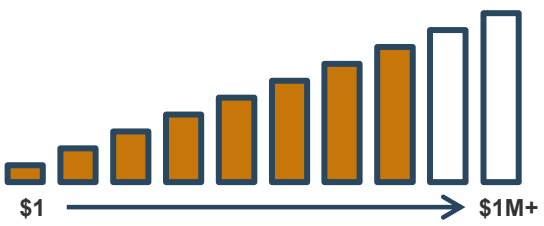
Advanced Data Enrichment	Advanced Correlation	Big Data Analytics	Reporting and Alerting	Forensic Analysis	Data Mgmt. and Retention	Threat Intelligence	Incident Mgmt. & Remediation	Full Security Threat Visibility	Scalability and Performance

Although the ESM product is still best suited for large scale use, HP offers other SIEM products for smaller deployments

Vendor Landscape

Product:	ArcSight Enterprise Security Manager (ESM)
Employees:	317,500
Headquarters:	Palo Alto, CA
Website:	arcsight.com
Founded:	2000
Presence:	NASDAQ:HPQ (Hewlett Packard)

3 year TCO for this solution falls into pricing tier 8, between $250,000 and $500,000



Pricing solicited from public sources

Overview

- ArcSight ESM is one of the log management solutions for HP's Enterprise Security Products (ESP). ArcSight offers a variety of SIEM solutions that vary for SME to enterprise businesses.

Strengths

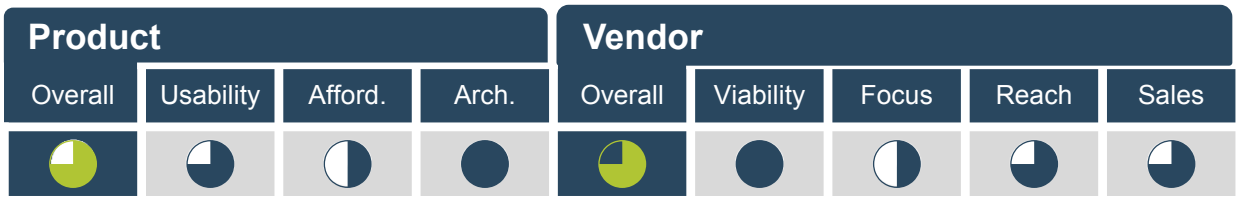
- Threat intelligence is provided by HP's own feed and by third-party feeds, providing fast and robust up-to-date threat knowledge.
- ArcSight Threat Response Manager (ArcSight TRM) allows automated remediation of threats based on actionable events.
- IdentifyView and ThreatDetector provide advanced behavior analysis functionality.
- ESM Version 6, with the Correlation Optimized Retention and Retrieval (CORR) Engine, improved EPS capacity and complexity.

Challenges

- Even with the CORR Engine reducing complexity, ArcSight EMS continues to be highly complex during deployment and operation.
- HP lacks some basic forensic analysis capabilities.
- Limited integration to third-party technologies for remediation actions limit its ability to shorten time to incident resolution.
- Correlation profiling and detection is done on historical data only.

Once a dominant player, ArcSight is now comparable to many other SIEM products

Vendor Landscape



Use-Case Scenario Performance

	Threat Management	Mgmt. of Security Events	SIEM Small Deployment	Risk Management
Scenario Performance	4th	6th	7th	4th
Value Index	6th	6th	7th	6th

Info-Tech Recommends:

ArcSight provides strong detection by tying activity monitoring to contextual events. ArcSight is a SEM-focused product. Although a strong product, a high price tag and stagnant product development is of concern. Threat management and fraud detection use cases should shortlist ArcSight.

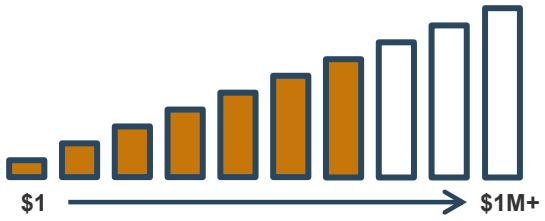
Features

QRadar continues to be one of the strongest SIEM products in the market with a tightly integrated platform

Vendor Landscape

Product:	QRadar SIEM
Employees:	400,000+
Headquarters:	Waltham, MA
Website:	ibm.com
Founded:	2001 (Q1 Labs)
Presence:	NASDAQ:IBM

3 year TCO for this solution falls into pricing tier 7, between $100,000 and $250,000



Pricing provided by vendor

Overview

- QRadar SIEM provides log, event, and incident management across heterogeneous IT environments. IBM's vast IT and security offerings, with QRadar's technology consolidation, make it a shortlist candidate for any information security need.

Strengths

- Its exceptional anomaly detection capabilities allow for the detection of internal misuse or fraud prevention within the organization, which can be extended to discover APTs.
- By commonly establishing baselines of your applications, users, and access profiles, QRadar is able to identify when something abnormal is occurring within your network.
- Simplified deployment through auto detection of all log sources and passive Netflow monitoring to detect network assets.

Challenges

- QRadar lacks the ability to provide automated remediation capabilities as part of the native SIEM function.
- Limited on-premise deployment to segmented servers limits clients' ability to scale the product in more than one way.

Robust log and event management, and simple usability are all supported by strong detection capabilities

Vendor Landscape

Product				Vendor				
Overall	Usability	Afford.	Arch.	Overall	Viability	Focus	Reach	Sales

Info-Tech Recommends:

APT, compliance management, and high capacity use cases are best suited for QRadar.

Use-Case Scenario Performance

	Threat Management	Compliance Management	Mgmt. of Security Events	SIEM Small Deployment	Risk Management
Scenario Performance	VENDOR LANDSCAPE AWARD LEADER INFO-TECH	VENDOR LANDSCAPE AWARD LEADER INFO-TECH	VENDOR LANDSCAPE AWARD LEADER INFO-TECH	6th	VENDOR LANDSCAPE AWARD LEADER INFO-TECH
Value Index	5th	7th	5th	6th	5th

Features

Advanced Data Enrichment	Advanced Correlation	Big Data Analytics	Reporting and Alerting	Forensic Analysis	Data Mgmt. and Retention	Threat Intelligence	Incident Mgmt. & Remediation	Full Security Threat Visibility	Scalability and Performance

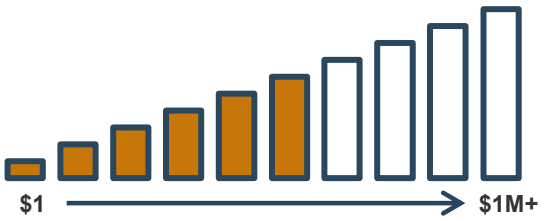
LogRhythm has consistently improved its product offering to become a dominant choice for mid-market organizations

Vendor Landscape

Product:	Security Intelligence Platform
Employees:	450
Headquarters:	Boulder, CO
Website:	logrhythm.com
Founded:	2003
Presence:	Privately held

LogRhythm®

3 year TCO for this solution falls into pricing tier 6, between $50,000 and $100,000



Pricing solicited from the vendor

Overview

- LogRhythm is a dedicated SIEM security vendor offering a solution geared towards providing simplified monitoring and management of its modular platform. Recent focus on reduced complexity and improved usability, in addition to historical focus on advanced analytics, has spurred high growth for LogRhythm.

Strengths

- LogRhythm's unified Security Analytics platform, which combines SIEM, log management, FIM, and machine analytics, provides enhanced threat visibility and management.
- Advanced correlation and pattern recognition is provided by LogRhythm's Advanced Intelligence (AI) Engine.
- Faster than typical deployment timeframes.
- A recent capability, the Identity Inference Engine, can infer missing identity information from analyzed event data.

Challenges

- LogRhythm uses less than mature machine learning style correlation policies.
- As a dedicated SIEM vendor, there is little possibility of LogRhythm being a strategic vendor in which value from multiple product purchases can be realized.

LogRhythm's ability to dedicate itself has garnered a fully featured, yet uncomplicated, product

Vendor Landscape

Product				Vendor				
Overall	Usability	Afford.	Arch.	Overall	Viability	Focus	Reach	Sales

Info-Tech Recommends:

With one of the best feature offerings paired with a surprisingly low price tag, all organizations should potentially shortlist LogRhythm.

Use-Case Scenario Performance

	Threat Management	Compliance Management	Mgmt. of Security Events	SIEM Small Deployment	Risk Management
Scenario Performance	VENDOR LANDSCAPE AWARD – LEADER – INFO-TECH	VENDOR LANDSCAPE AWARD – CHAMPION – INFO-TECH	VENDOR LANDSCAPE AWARD – CHAMPION – INFO-TECH	VENDOR LANDSCAPE AWARD – CHAMPION – INFO-TECH	VENDOR LANDSCAPE AWARD – CHAMPION – INFO-TECH
Value Index	VENDOR LANDSCAPE AWARD – BEST OVERALL VALUE – INFO-TECH	VENDOR LANDSCAPE AWARD – BEST OVERALL VALUE – INFO-TECH	VENDOR LANDSCAPE AWARD – BEST OVERALL VALUE – INFO-TECH	VENDOR LANDSCAPE AWARD – BEST OVERALL VALUE – INFO-TECH	VENDOR LANDSCAPE AWARD – BEST OVERALL VALUE – INFO-TECH

Features

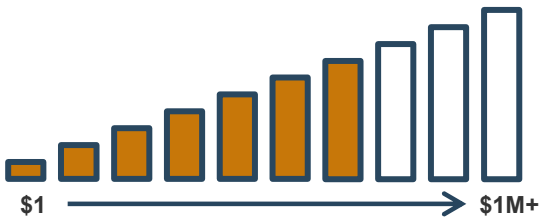
Advanced Data Enrichment	Advanced Correlation	Big Data Analytics	Reporting and Alerting	Forensic Analysis	Data Mgmt. and Retention	Threat Intelligence	Incident Mgmt. & Remediation	Full Security Threat Visibility	Scalability and Performance

Intel Security continues to realize value from embedding McAfee security into computing architecture and platforms

Vendor Landscape

Product:	McAfee Enterprise Security Manager (ESM)
Employees:	7,923
Headquarters:	Santa Clara, CA
Website:	intelsecurity.com
Founded:	1987
Presence:	NASDAQ: INTC (Intel)

3 year TCO for this solution falls into pricing tier 7, between $100,000 and $250,000



Pricing solicited from public sources

Overview

- As one of the largest security technology companies, Intel Security offers a robust SIEM solution with add-on product functionality.
- McAfee's ESM scales from medium to enterprise size, with historical focus on high security demanding organizations.

Strengths

- Correlation is distributed via Event Receivers or the Advanced Correlation Engine (ACE), which can run correlation rules in real time or against historical data.
- Intel Security allows for real-time monitoring of internal and external threats and ad hoc query capabilities of logs.
- Real-time information on searchable data is provided allowing the ability to limit queries to highly relevant data.
- McAfee Global Threat Intelligence is a reputable threat source.

Challenges

- Despite having high ingest rates and high query performance, the lack of efforts to minimize latency from event normalization is of concern.
- Currently, ESM does not offer Netflow de-duplication or support for sFlow.

Improved technology integration across Intel Security products enhances strategic vendor value

Vendor Landscape

Product			
Overall	Usability	Afford.	Arch.
			

Vendor				
Overall	Viability	Focus	Reach	Sales
				

Info-Tech Recommends:

McAfee should be a shortlist candidate for most use cases as it will predictably continue to offer strong products and will fight for market leadership.

Use-Case Scenario Performance

	Threat Management	Compliance Management	Mgmt. of Security Events	SIEM Small Deployment	Risk Management
Scenario Performance				4th	
Value Index	2nd	5th	3rd	5th	2nd

Features

Advanced Data Enrichment	Advanced Correlation	Big Data Analytics	Reporting and Alerting	Forensic Analysis	Data Mgmt. and Retention	Threat Intelligence	Incident Mgmt. & Remediation	Full Security Threat Visibility	Scalability and Performance
									

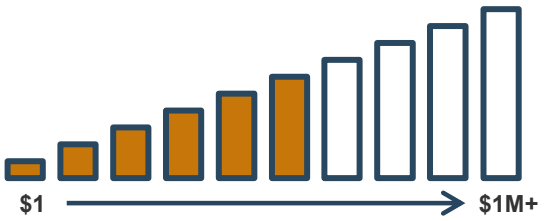
Strong identity security offerings and enhanced cross-product integration makes NetIQ a strategic vendor

Vendor Landscape

Product:	Sentinel
Employees:	4,500+
Headquarters:	Houston, TX
Website:	netiq.com
Founded:	1995
Presence:	Privately held

NetIQ®

3 year TCO for this solution falls into pricing tier 6, between $50,000 and $100,000



Pricing provided by vendor

Overview

- NetIQ, a recent acquisition and now principal brand of the Micro Focus Group, offers a broad portfolio of IT solutions and services. Sentinel is the blend of change and identity management functionality now offering a flexible SIEM solution.

Strengths

- Sentinel is able to provide an architecture that is very flexible and works in almost every environment. This is ideal for security architects looking for a great deal of customization.
- The SIEM product is easy to deploy and begins to collect data, identify devices, and manage threats almost immediately.
- Fully customizable data management policies allow for breadth of retention and storage needs.
- Sentinel offers customizable indexing and compression.

Challenges

- NetIQ supports third-party threat intelligence as a source of context, but is limited with the types of uses of that information when compared to other vendors.
- Sentinel has fewer pre-packed remediation capabilities than other vendors evaluated, limiting competitiveness on time to incident resolution.

NetIQ provides strong compliance documentation and data management for regulatory use cases

Vendor Landscape

Product				Vendor				
Overall	Usability	Afford.	Arch.	Overall	Viability	Focus	Reach	Sales
								

Info-Tech Recommends:

An overall strong feature scoring enhanced by an attractive price point means mid-market organizations should shortlist and watch for developments from the acquisition.

Use-Case Scenario Performance

	Threat Management	Compliance Management	Mgmt. of Security Events	SIEM Small Deployment	Risk Management
Scenario Performance	7th	5th	7th	5th	6th
Value Index	3rd	4th	2nd	4th	3rd

Features

Advanced Data Enrichment	Advanced Correlation	Big Data Analytics	Reporting and Alerting	Forensic Analysis	Data Mgmt. and Retention	Threat Intelligence	Incident Mgmt. & Remediation	Full Security Threat Visibility	Scalability and Performance
									

RSA Security Analytics provides event management, threat detection, and incident investigation for high demand use cases

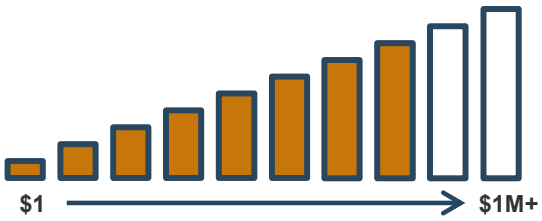
Vendor Landscape

Product:	RSA Security Analytics (SA)
Employees:	60,000 (EMC)
Headquarters:	Bedford, MA
Website:	rsa.com
Founded:	1982, SIEM market 2006
Presence:	NYSE: EMC

RSA®

The Security Division of EMC

3 year TCO for this solution falls into pricing tier 8, between $250,000 and $500,000



Pricing solicited from public sources

Overview

- RSA, the security division of EMC, is recognized as a leading security vendor. Having evolved from a SIEM product, Security Analytics is the next generation monitoring product from RSA, focusing on monitoring and investigation capabilities.

Strengths

- RSA's Security Analytics combines SIEM and network monitoring with forensic analysis into its offering as a single solution.
- With a unique architecture, large sums of data can be consumed, analyzed and investigated while it can correlate various pieces of data such as packets, logs, Netflow, and endpoint data.
- Comprehensive data analysis can be done on the Warehouse component that is based on Pivotal, a Hadoop system.

Challenges

- RSA is primarily focused on security monitoring deployments for mid-size and large with organizations that are security-focused.
- RSA Security Analytics is a modular solution that increases in complexity as the requirement for data ingestion, analysis, and investigation increases.
- Due to SA's focus on advanced monitoring and forensic investigations, it lacks any comparable incident remediation.

With support for high capacity, heterogeneous network security use cases, smaller organizations should be wary

Vendor Landscape

Product				Vendor				
Overall	Usability	Afford.	Arch.	Overall	Viability	Focus	Reach	Sales
								

Use-Case Scenario Performance

	Threat Management	Compliance Management	Mgmt. of Security Events	Risk Management
Scenario Performance	6th	7th	4th	7th
Value Index	4th	6th	4th	4th

Info-Tech Recommends:

Security Analytics is a modular product with a focus on detection and investigation that's paired with high scalability. Large enterprises with high security demands that already have SOC style capabilities in-house or have large staffing resources to dedicate should shortlist RSA.

Features

Advanced Data Enrichment	Advanced Correlation	Big Data Analytics	Reporting and Alerting	Forensic Analysis	Data Mgmt. and Retention	Threat Intelligence	Incident Mgmt. & Remediation	Full Security Threat Visibility	Scalability and Performance
									

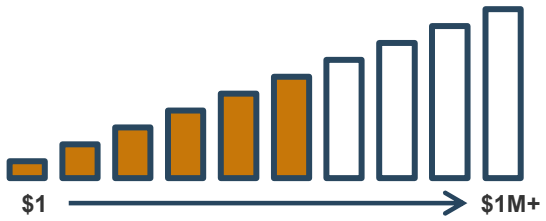
LEM offers traditional SIEM capabilities with embedded log management, file integrity monitoring, and active response

Vendor Landscape

Product:	Log & Event Manager (LEM)
Employees:	1,600+
Headquarters:	Austin, TX
Website:	solarwinds.com
Founded:	1999, SIEM market 2011
Presence:	NASDAQ: SWI

solarwinds

3 year TCO for this solution falls into pricing tier 6, between $50,000 and $100,000



Pricing provided by vendor

Overview

- SolarWinds traditionally serves the mid-market by providing a simple SIEM solution for IT departments that are resource-constrained, and integrates with other security technologies to provide a holistic security view.

Strengths

- SolarWinds LEM provides advanced reporting that contains multiple different reports that can be customized to view historical and compliance data.
- SolarWinds LEM provides advanced correlation rules out-of-the-box that offer insights into suspicious behavior, insider abuse, and change management.
- High usability, easy implementation, and pre-packed content ensure a quick time to value realization.

Challenges

- SolarWinds does not have an automated threat intelligence feed as it needs to be manually imported by users,
- The product does not officially expose any APIs that can be leveraged by other applications and middleware for the purpose of integration.
- Limited data collection sources can impede full network visibility.

A strong focus on usability and deployment limits additional costs for consulting, training, or internal resource dedication

Vendor Landscape

Product				Vendor				
Overall	Usability	Afford.	Arch.	Overall	Viability	Focus	Reach	Sales

Use-Case Scenario Performance

	Compliance Management	SIEM Small Deployment
Scenario Performance	6th	VENDOR LANDSCAPE AWARD – LEADER – INFO-TECH
Value Index	3rd	3rd

Info-Tech Recommends:

SolarWinds LEM focuses on being easy to deploy and use – perfect for resource-constrained organizations that will not want to spend extra on consulting or training. Many out-of-the-box features such as threat intelligence deliver a quick time to value. USB access is blocked with its USB Defender, making LEM suited for organizations concerned with removable media data theft. The LEM offers traditional SIEM functionality plus other functions such as automated remediation capabilities and file integrity monitoring. SolarWinds is a good fit for small to mid-sized companies that require a SIEM with easy deployment and easy operations, and at the lower price end.

Features

Advanced Data Enrichment	Advanced Correlation	Big Data Analytics	Reporting and Alerting	Forensic Analysis	Data Mgmt. and Retention	Threat Intelligence	Incident Mgmt. & Remediation	Full Security Threat Visibility	Scalability and Performance

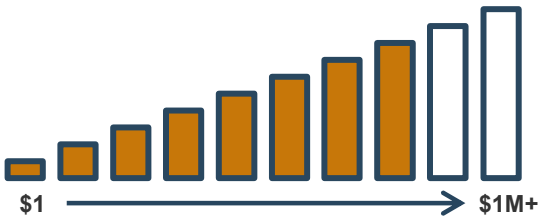
Splunk has developed all of its product capabilities rapidly in recent years, but it is still extremely complex and costly

Vendor Landscape

Product:	Splunk Enterprise
Employees:	1,700
Headquarters:	San Francisco, CA
Website:	splunk.com
Founded:	2004
Presence:	NASDAQ: SPLK

splunk>

3 year TCO for this solution falls into pricing tier 8, between $250,000 and $500,000



Pricing provided by vendor

Pricing provided is based on a security pricing scenario, pricing factoring in use cases that are commonly supported by the Splunk platform will potentially lead to lower tiers.

Overview

- Splunk is known for its ability to enhance IT operations through analytics, but it can be dedicated and used for SIEM-related tasks and help to provide advanced threat detection. Security is now a major focus of Splunk in contrast to earlier solutions and efforts.

Strengths

- Splunk's wide offerings and add-ons allow it to move beyond just a simple SIEM function, but can affect many different business operations and capabilities.
- With flexible and customizable analytics, Splunk proves to be one of the leaders in advanced correlation.
- Splunk is one of the few vendors that provides hybrid deployments that examine the cloud and on-premise hardware.

Challenges

- Splunk Enterprise can be complex and time consuming to implement, especially as there is a great deal of customization needed.

Splunk is best suited for heterogeneous, high capacity, security-demanding organizations with unstructured data

Vendor Landscape

Product				Vendor				
Overall	Usability	Afford.	Arch.	Overall	Viability	Focus	Reach	Sales
								

Use-Case Scenario Performance

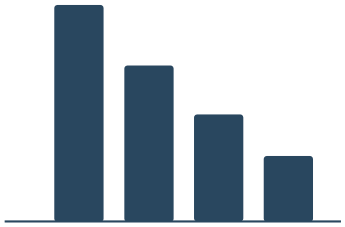
Scenario Performance	Threat Management	Mgmt. of Security Events	Risk Management
Value Index	5th	5th	5th
	8th	7th	7th

Info-Tech Recommends:

Splunk offers some of the industry's best query capabilities. Splunk doesn't use a relational database that allows all the data that is indexed to have all fields available for query quickly. This fast query is best suited for organizations concerned with a quick incident and breach response time. Originally not designed for security, Splunk can offer business intelligence capabilities providing a multi-purposed solution. Splunk is deployed by operations teams to support log management, correlation analysis, and incident or breach investigations. With high staffing and cost deployment, organizations looking to shortlist Splunk should consider also taking advantage of Spunk's non-security products.

Features

Advanced Data Enrichment	Advanced Correlation	Big Data Analytics	Reporting and Alerting	Forensic Analysis	Data Mgmt. and Retention	Threat Intelligence	Incident Mgmt. & Remediation	Full Security Threat Visibility	Scalability and Performance
									



4.5: Create a Custom Shortlist

Use the SIEM *Vendor Shortlist and Detailed Analysis Tool* to customize the vendor analysis for your organization

4.5 1 hour

Instructions

1. Create your own evaluation framework

Tailor the vendor evaluation to include your own product and vendor considerations on *Tab 3. Weightings.*

Identify the significance of advanced features for your own procurement on a scale of **Mandatory, Optional,** and **Not Required** on *Tab 4. Detailed Feature Analysis*.

2. Review the results of your customized evaluation

Review your custom vendor shortlist on *Tab 5. Results.*

Detailed Feature Analysis Worksheet

In the column *Client Importance,* select the value that most closely reflects your organization's requirements for each specific feature. Values are defaulted to "Optional."
Mandatory items are those that are absolutely required for your organization; products which do not have this capability will be eliminated from consideration.
Optional items are those that would be desirable, but are not absolutely required.
Not required items are dropped from calculations of feature-specific outputs.

Vendors will be ranked based on the provided Feature Importance. A feature-dependent customized Vendor Shortlist of weighted scores will be generated, along with a feature-dependent Value Index. Results are displayed on the *Results* tab.

Feature	Feature Description	Client Importance
Advanced Data Enrichment	Advanced CAN from various log and non log data sources (identity, database, application, configuration, netflow, cloud, file integrity, etc.) with full packet capture ability.	Mandatory
Advanced Correlation	Advanced pre-built policies, user-defined policies, behavioural policies, machine learning style policies and host criticality information inclusion.	Mandatory
Big Data Analytics	Use of big data style analytics through integration into purpose built big data tools or native capabilities, all based on advanced security style analytic methodologies.	Mandatory
Advanced Reporting and Alerting	Pre-built reporting and alerting libraries, customizable dashboards, compliance use case support, various alerting options, and integration into external reporting and third party workflow tools.	Mandatory
Forensic Analysis Support	Advanced query capabilities against all collected data with pre-built and custom drill down, pivot, and parsing with export functions and event session reconstruction.	Mandatory
Data Management Security and Retention	Granular access controls to system data, protection of SIEM data, system access monitoring, external storage integration and efficient data compression.	Mandatory
Threat Intelligence Feed	Security threat intelligence feed integration with ability to update multiple uses and control updating behaviours.	Mandatory
Incident Management and Remediation	Advanced detection and incident management with pre-built and customizable remediation capabilities, integration into workflow systems, and optional automatic remediation through integration.	Mandatory
Full Security Threat Visibility	Integration with security technologies for monitoring, incident analysis and data enrichment to support ability to track and analyze the progression of an attack, the activity of a user, and/or a series of related events.	Mandatory
Scalability and Network Performance	Ability for SIEM system to scale horizontally and vertically, while employing various methods to reduce any latency impacts from CAN activities.	Mandatory

Sample Feature from Tab 3. Detailed Feature Analysis

Vendor Shortlist				
Vendor	Rank	Product Score	Vendor Score	Feature Score
Splunk	1	-5.0	-5.0	8.0
SolarWinds	2	-5.0	-5.0	10.7
RSA	3	-5.0	-5.0	8.7
NetIQ	4	-5.0	-5.0	9.5
Intel Security	5	-5.0	-5.0	0.0
LogRhythm	6	-5.0	-5.0	9.7
IBM	7	-5.0	-5.0	0.0
HP	8	-5.0	-5.0	9.0
EventTracker	9	-5.0	-5.0	0.0
AlienVault	10	-5.0	-5.0	8.3

Sample Vendor Shortlist from Tab 5. Results

Use Info-Tech's *SIEM Vendor Shortlist and Detailed Analysis Tool* to assist in this stage of the project.

Honourable Mention: Trustwave focuses on a managed SIEM purposed for PCI compliance

4.5

Trustwave historically has performed well in PCI compliance and managed security services

Product:	SIEM Enterprise
Employees:	1,200
Headquarters:	Chicago, IL
Website:	trustwave.com
Founded:	1995
Presence:	Privately held

Info-Tech Recommends:

Trustwave offers a product suited for customers that are PCI-compliant and looking to outsource management. Although self-managed on-premise offerings are available for non-PCI uses cases, Trustwave does not focus on this nor do they market to these customers. The managed service option is an attractive offering for organizations lacking internal resources or expertise. Trustwave's customers are PCI customers who don't want to dedicate resources to monitoring and proving adherence in-house.

Overview

- Trustwave focuses on security services and is well suited for compliance use cases while being able to provide SIEM as a managed security service.

Strengths

- With more than 600 compliance-based reports, Trustwave stands out as a SIEM that is focused on compliance reporting, which is extremely useful for those organizations that are regularly audited.
- By offering its product as a managed service, Trustwave oversees the SIEM product to reduce the need for full-time employees to be staffed on the SIEM in-house.
- Trustwave offers a wide variety of security products beyond just SIEM, such as DLP, NAC, and UTM.

Challenges

- It can be difficult to integrate SIEM with other security technologies from other vendors and receive the same level of support.
- Trustwave can struggle at times with integrating all of its products as many were acquired from other organizations.

Evaluate alternative SIEM vendors not included in Info-Tech's Vendor Landscape

Info-Tech only evaluated a portion of vendors in the SIEM market. Don't narrow your SIEM procurement project to only include vendors recognized in Info-Tech's Vendor Landscape.

Additional Vendors in the SIEM Market

ALERTLOGIC
Security. Compliance. Cloud.

GFI®

accelops

BlackStratus™

tenable
network security

tripwire™

QUEST SOFTWARE
Owned by Dell

To name a few…

Workshop Scope for Step 4

Call 1-888-670-8889 or email Workshops@InfoTech.com for more information

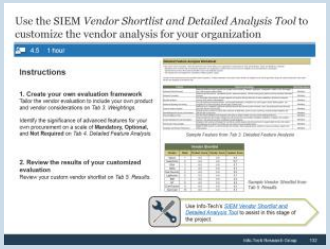
An Info-Tech Analyst would facilitate the following activities during an onsite workshop:

4.3-4.4

Review Info-Tech's Vendor Landscape results

Using Info-Tech's Vendor Landscape analysis and the results of your use-case assessment results, the facilitator will guide your business through information related to the vendors in the SIEM market and focus on vendors whose solution best aligns with your requirements.

4.5



Create a custom shortlist of SIEM vendors

The facilitator will guide your project team in identifying your own shortlist of evaluated vendors. The facilitator will use an Excel tool that will allow the team to select their own weightings for product and vendor considerations, and also provide the team with the option to adjust the advanced feature prioritization based on their own solution requirements.

4.5

Review additional SIEM vendors for consideration

Based on your organization's own research and expressed interests, the Info-Tech analyst will take time to review additional vendors in the market that may also be considered by your team as you perform your evaluation and procurement. To support your project team's information gathering and selection, the analyst will use their market knowledge and also conduct a deeper review of the vendors to assess fit based on the requirements identified by the team during the workshop.

Step 5: Select a SIEM solution

1. Assess value and identify fit
2. Build the procurement team and project plan
3. Identify the requirements for the SIEM
4. Produce the vendor shortlist
5. **Select a SIEM solution**
6. Create an implementation plan
7. Measure the value of the SIEM solution

This step will walk you through the following activities:

- 5.1: Determine your procurement strategy
- 5.2: Create and prioritize your solution requirements
- 5.3: Create an RFP to submit to vendors
- 5.4: Evaluate the RFPs
- 5.5: Create a demo script
- 5.6: Conduct onsite vendor presentations and demos
- 5.7: Conduct client reference interviews
- 5.8: Select your SIEM suite

Info-Tech suggests involving the following participants in this step of the project:

- Project manager
- Subject matter experts
- Evaluation team
- Vendor representatives
- Steering committee/PMO

Outcomes of this step:

- Identification of the opportunities associated with SIEM
- Confirmation of the business's suitability for a SIEM investment
- An appraisal of Info-Tech's Vendor Landscape market overview for SIEM
- Determination if now is the right time to proceed with this project

Kick off your selection process by determining your procurement strategy

- Follow your own organization's procurement procedures to ensure that you adhere to your organization's policies.
- Review Info-Tech's Procurement Process below and focus on completing Steps 7-15, as you will have already completed 1-6.

Info-Tech's 15-Step Procurement Process

Use Info-Tech's Procurement Process to ensure that your SIEM selection is properly planned and executed.

1. Initiate procurement
2. Select procurement manager
3. Prepare for procurement; check that prerequisites are met
4. Select appropriate procurement vehicle
5. Assemble procurement teams
6. Create procurement project plan
7. **Identify and notify vendors about procurement**
8. **Configure procurement process**
9. **Gather requirements**
10. **Prioritize requirements**
11. **Build the procurement documentation package**
12. **Issue the procurement**
13. **Evaluate proposals**
14. **Recommend a vendor**
15. **Present to management**

Additional vendor selection research

If your organization lacks a clear procurement process, refer to Info-Tech's *Optimize IT Procurement* research to help construct a formal process for selecting application technology.

Optimize IT Procurement

Info-Tech Insight

- Involving a third-party firm to support your organization's evaluation of SIEM vendors can be valuable as they will have expertise and insights into vendor solutions that extend past the knowledge of your in-house staff.
- Beware of relationships between vendors and third parties to ensure that vendors are fairly evaluated based on your organization's own needs.

Create and prioritize your solution requirements based on your business and technical assessments

5.2 Variable time commitment

1. Identify Your Requirements

- Use the findings of your process mapping and interviews to uncover the requirements for the future SIEM solution.
- Research market trends and additional opportunities with SIEM.
- Use your use-case findings to further develop your solution requirements.

2. Prioritize Your Requirements

- Identify the significance of each requirement for your solution evaluation.
- Info-Tech recommends identifying features and requirements as *mandatory*, *important*, or *optional.*
- Control the number of mandatory requirements you document. Too many mandatory requirements could create an unrealistic framework for evaluating solutions.

3. Create a Requirements Package

- Consolidate your identified requirements into one list, removing redundancies and conflicts.
- Categorize the requirements based on their priority and nature.

Use this requirements package as you evaluate vendors and create your RFP for shortlisted vendors.

Info-Tech Insight

No solution will meet 100% of your requirements. Control the number of mandatory requirements you place in your procurement process to ensure that vendors that are the best fit for your organization are not eliminated unnecessarily.

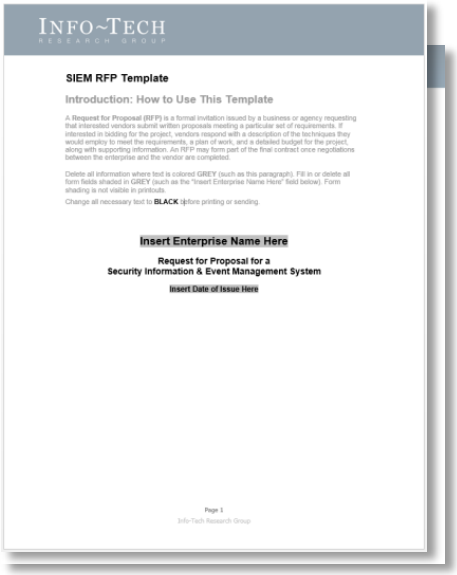
Categorize Your Requirements as:

- Mandatory requirements
- Functional requirements
- Technical requirements
- Capability requirements

Create an RFP to submit to vendors

5.3 *SIEM RFP Template*

Use an RFP template to convey your desired suite requirements to vendors and outline the proposal and procurement steps set by your organization.



SIEM RFP Template

Instructions

Build Your RFP

1. Outline the organization's procurement instructions for vendors (Sections 1,3,5).
2. Input the requirements package created in Activity 5.2 into your RFP. (Section 4).
3. Create a scenario overview to provide vendors an opportunity to give an estimated price.

Approval Process

Each organization has a unique procurement process; follow your own organization's process as you submit your RFPs to vendors.

1. Ensure compliance with your organization's standards and gain approval for submitting your RFP.

Call an analyst to assist in the creation and review of your SIEM RFP.

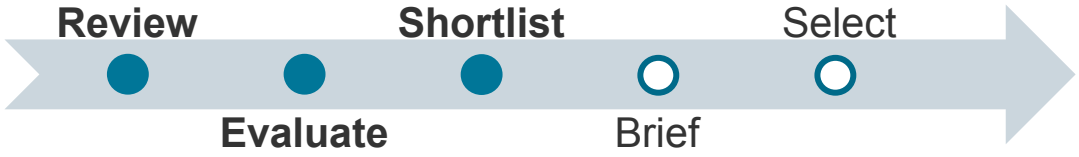
Info-Tech RFP Table of Contents

1. Statement of Work
2. General Information
3. Proposal Preparation Instructions
4. Scope of Work, Specifications, and Requirements
5. Vendor Qualifications and References
6. Budget and Estimated Pricing
7. Vendor Certification

Evaluate the RFPs you receive within a clear scoring process

5.4 *SIEM Suite Evaluation and Scoring Tool*

Build a fair evaluation framework that evaluates vendor solutions against a set criteria rather than relative comparisons.

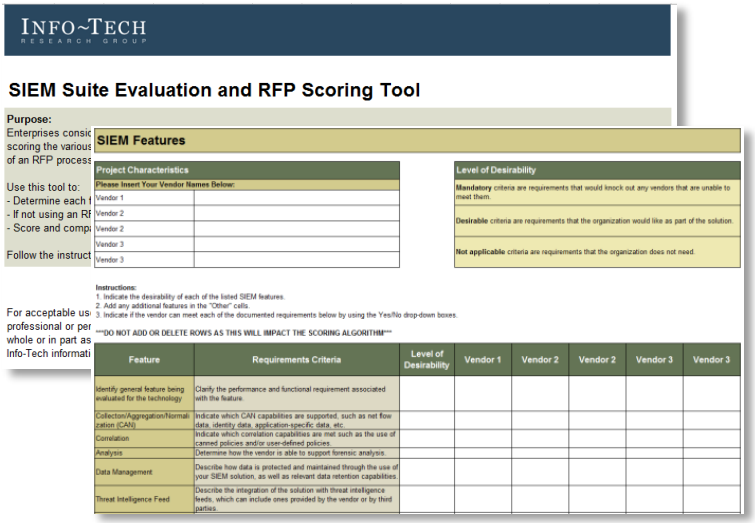


Instructions

1. Have members of the procurement project team review the RFP responses given by vendors.
2. Input vendor solution information into *the SIEM Suite Evaluation and Scoring Tool.*
3. Analyze the vendors against your identified evaluation framework tool.
4. Identify vendors with whom you wish to arrange vendor briefings.
5. Contact vendors and arranging briefings.

How to use this tool

1. Review the feature list and select where each feature is mandatory, desirable, or not applicable.
2. Indicate if each feature has been met by the vendor RFP response.
3. Enter the costing information provided by each vendor.
4. Determine the relative importance of the features, architecture, and support.



Info-Tech's SIEM Suite Evaluation and RFP Scoring Tool

Tool Output

- Feature Score
- Architecture Score
- Support Score
- Costing
- Overall Score

The scoring system removes subjectivity from the equation and allows you to compare the offering to the cost.

Create a vendor demo script

5.5 *SIEM Vendor Demo Script Template*

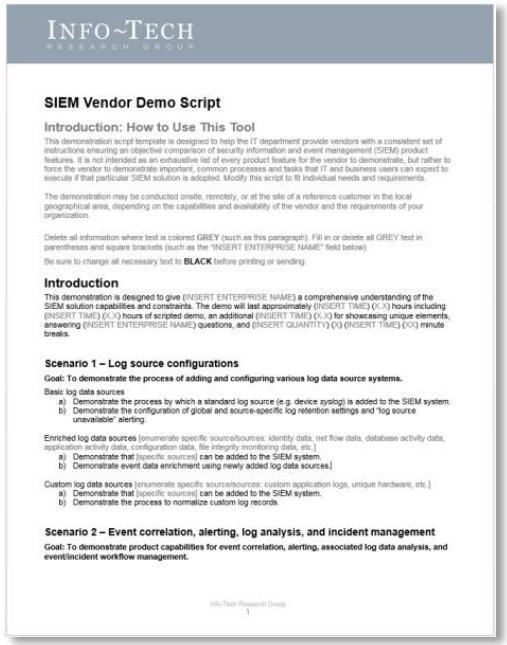
Use a demo script to help identify how a vendor's solution will fit your organization's particular capability needs.

Ask for a display of the tool's interface and capabilities.

Provide prompts to display:

- A view of the user interface
- A view of the monitoring dashboards and management interfaces.
- An understanding of the data management techniques being used.
- A view of how different reporting capabilities and techniques are used.
- An understanding of the correlation policies in the solution.

Use Scenarios 1–5 in the *SIEM Vendor Demo Script Template* to support your review of the tool's capabilities.


INFO-TECH RESEARCH GROUP

SIEM Vendor Demo Script

Introduction: How to Use This Tool

This demonstration script template is designed to help the IT department provide vendors with a consistent set of instructions ensuring an objective comparison of security information and event management (SIEM) product features. It is not intended as an exhaustive list of every product feature for the vendor to demonstrate, but rather to force the vendor to demonstrate important, common processes and tasks that IT and business users can expect to execute if that particular SIEM solution is adopted. Modify this script to fit individual needs and requirements.

The demonstration may be conducted onsite, remotely, or at the site of a reference customer in the local geographical area, depending on the capabilities and availability of the vendor and the requirements of your organization.

Delete all information where text is colored GREY (such as this paragraph). Fill in or delete all GREY text in parentheses and square brackets (such as the "[INSERT ENTERPRISE NAME]" field below).

Be sure to change all necessary text to **BLACK** before printing or sending.

Introduction

This demonstration is designed to give [INSERT ENTERPRISE NAME] a comprehensive understanding of the SIEM solution capabilities and constraints. The demo will last approximately [INSERT TIME] (XX) hours including [INSERT TIME] (XX) hours of scripted demo, an additional [INSERT TIME] (XX) for showcasing unique elements, answering [INSERT ENTERPRISE NAME] questions, and [INSERT QUANTITY] (X) [INSERT TIME] (XX) minute breaks.

Scenario 1 – Log source configurations

Goal: To demonstrate the process of adding and configuring various log data source systems.

Basic log data sources

a) Demonstrate the process by which a standard log source (e.g. device *syslog*) is added to the SIEM system.
b) Demonstrate the configuration of global and source-specific log retention settings and "log source unavailable" alerting.

Enriched log data sources [enumerate specific source/sources: identity data, net flow data, database activity data, application activity data, configuration data, file integrity monitoring data, etc.]

a) Demonstrate that [specific sources] can be added to the SIEM system.
b) Demonstrate event data enrichment using newly added log data sources.]

Custom log data sources [enumerate specific source/sources: custom application logs, unique hardware, etc.]

a) Demonstrate that [specific sources] can be added to the SIEM system.
b) Demonstrate the process to normalize custom log records.

Scenario 2 – Event correlation, alerting, log analysis, and incident management

Goal: To demonstrate product capabilities for event correlation, alerting, associated log data analysis, and event/incident workflow management.

Info-Tech Research Group
1

SIEM Vendor Demo Script Template

Instructions

1. Create a demo script to send to vendors that outlines a mapped process from your organization.
2. Construct the demo script with your project team, providing both prompts for the vendor to display the capabilities and a process scenario for the vendor to model.

Information Sources

- Requirements package
- Use-case results

Conduct onsite vendor presentations and demos

5.6

Vendor demonstrations create a valuable opportunity for your organization to confirm that the vendor's claims in the RFP are actually true.

A display of the vendor's functional capabilities and their execution of the scenarios given in your demo script will help to support your assessment of whether a vendor aligns with your SIEM suite requirements.

Examine how the vendor's solution performs against your evaluation framework.

Who to engage

Have your evaluation team, selected at the outset of the project, present to evaluate each vendor's presentation. In specific cases you may choose to bring in a SME to evaluate a specific area of the tool.

Evaluation Team

- Project manager
- Business representative
- SMEs
- IT manager

What should be included in a vendor demonstration?

- Vendor's display of their solution for the scenarios provided in the demo script.
- Display of functional capabilities of the tool.
- Briefing on architectural and integration capabilities.

Conduct client reference interviews to identify how other organizations have successfully used the vendor's solution

Have vendors supply client references to confirm the value of their implemented solution.

Vendors are inevitably going to provide references that will give positive feedback, but don't be afraid to dig into the interviews to understand some of the limitations related to the solution.

- **Even if a vendor is great for one client, that doesn't necessarily mean it will fit for you.** Ask the vendor to provide references to organizations in your own or a similar industry, or someone who has automated similar business processes or outlined similar expectations.
- Use these reference calls as an opportunity to gain a more accurate understanding of the quality of the vendor's service support and professional services.

If you are looking to include a high level of customization in your SIEM solution, pay particular attention to this step and the client responses, as these will help you understand how easy a vendor is to work with.

Make the most of your client reference interviews by preparing your questions in advance and following a specific script.

Select the SIEM suite that best fits your organization

Don't just choose the vendor that gave the best presentation. Instead, select the vendor that meets your functional requirements and organizational needs.

Tab 5. Overall Score from the *SIEM Suite Evaluation and Scoring Tool*

Category	Weight	Vendor 1	Vendor 2	Vendor 3	Vendor 4	Vendor 5
SIEM Features	60%	30%	90%	50%	90%	80%
Architecture	25%	30%	70%	60%	90%	80%
Support	15%	56%	100%	56%	78%	78%
Total Score	**100%**	**34%**	**87%**	**53%**	**88%**	**80%**

Use your objective evaluation to select a vendor to recommend to management for procurement.

Don't automatically decide to go with the highest score; validate that the vendor is an organization you can envision working with for a long time.

- Select a vendor based not only on their evaluation performance, but also on your belief that you could form a lasting and supportive relationship.
  - With its evolving functionality and process modelling support, SIEM suites may require more vendor engagement and partnering than many other application suites.

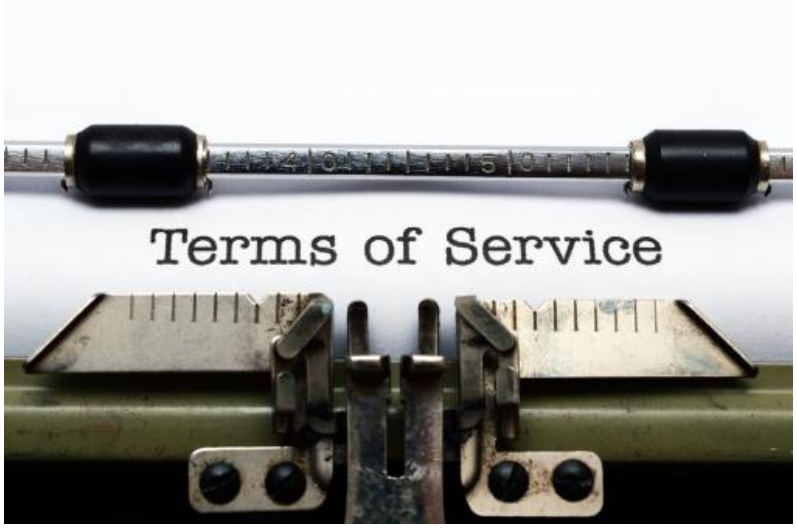
Following the identification of your selected suite, submit your recommendation to the organization's management or procurement committee for final approval.

Negotiate and finalize a contract outlining the terms of service for your SIEM solution

Defer First to Your Organization's Process

Follow your own organization's contract negotiation and approval process as you finalize the deal with your selected SIEM vendor.

- Each industry and organization has different requirements and considerations that will alter how a contract negotiation and approval process are performed.



Info-Tech's Contract Negotiation Tips and Reminders

Explore discounting options.

- Most vendors offer some form of discounting based on volume of users or the nature of your industry. Explore how the vendor's discounting model can improve the ROI of your investment.

Value is captured not only in the functional capabilities of the tool, but also in its ongoing support and utilization.

- **Training:** Determine the mode and rigor of end-user and developer training.
- **Implementation:** Outline the vendor's role and the expected results related to the configuration and implementation of the SIEM solution.
- **Service Support:** Identify the level of support your organization requires for the ongoing maintenance and performance of the tool.

Info-Tech Insight

Offering to be a potential reference after a successful deployment could help secure higher quality service during implementation and post deployment. Just be clear that the offer is *contingent* on a successful implementation.

Call an analyst to perform a SIEM contract review.

Ensure your project oversight and business is on-board with your selected solution

Please Note: This blueprint's steps and structure are built on the assumption that a budget for your SIEM investment has already been approved and laid out for the project.

If your project still requires budget allocation and approval at the end, use Info-Tech's *IT Procurement Presentation Template* and the supported instructions to propose your selected solution as an investment for the organization.

IT Procurement Presentation Template

Present the following information to ensure approval of your purchase:

- Project Context
- Project Scope and Objectives
- Procurement Process
- Evaluation Results
- Recommendations
- Next Steps & Timelines

This is where your work to ensure alignment and engagement with the business will pay off.

Since you have been engaging critical stakeholders throughout the project, this step should not be difficult, with no surprises experienced on either slide.

To ensure the value for the business is properly conveyed, discuss how this solution will execute on the objectives identified at the beginning of your project scoping.

Critical Preceding Activities

- **2.1:** Identify the scope and purpose of your SIEM selection process
- **2.3:** Identify the stakeholders whose support will be critical for securing investment approval
- Procurement steps **5.1-5.8**

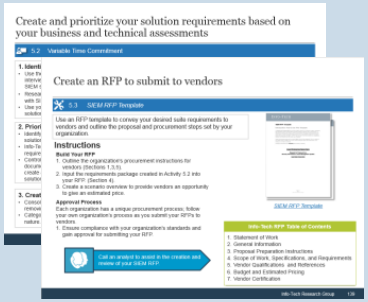
Workshop Scope for Step 5

An Info-Tech Analyst would facilitate the following steps during an on site workshop:

Working Day

- As part of the wrap-up of the SIEM selection workshop, the Info-Tech analyst will work with your project team to prepare for the next steps in your procurement project.
- Supporting your project team in working sessions, the analyst will help your project team to begin building your RFP and the structure for evaluating vendors.

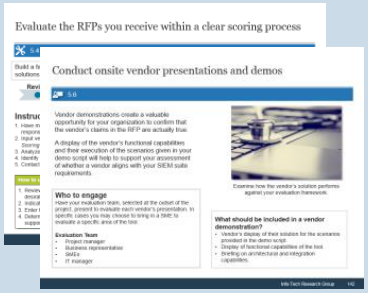
5.2-5.3



Begin creating your RFP for SIEM vendors

To organize workshop findings, the analyst will conduct working sessions with your project team to prioritize and organize requirements into a formal requirements package. In conjunction with this package, the analyst will also work with your project manager and RFP writers to begin drafting the RFP and identifying the procurement steps associated with selection.

5.4-5.6



Create the documents for evaluating your SIEM vendors

To close out the onsite engagement, the analyst will work with your project team to scope your business's process for evaluating RFPs and vendor solutions. Using workshop findings and working sessions with the project manager and the evaluation team, the analyst will help to create the framework for an objective evaluation process.

Additional Support

To further support your organization as you analyze your RFPs and conduct vendor demonstrations and solution selection, analyst follow-up calls can be arranged by the team as needed.

Call 1-888-670-8889 or email Workshops@InfoTech.com for more information.

Phase 3: Plan the SIEM implementation

Phase 1:

Launch the SIEM selection project and gather requirements

Phase 2:

Select a SIEM solution

Phase 3:

Plan the SIEM implementation

Let our analysts guide you through this phase

Call 1-888-670-8889 or email GuidedImplementations@InfoTech.com for more information

A guided implementation is a series of 2-3 advisory calls that help you execute each phase of a project. They are included in most advisory memberships.

Guided Implementation 4: Plan the SIEM Implementation

Proposed Time to Completion: 1 Month–1 Year

Step 6: Create the SIEM Implementation Plan

Create an Implementation Plan

- Plan the steps and considerations required to implement.

Activities

- Create the project plan for your implementation.
- Design your SIEM architecture.
- Optimize and improve the design.

Step 6: Create the SIEM Implementation Plan

Set up your SIEM capabilities

- Ensure that your SIEM is ready for your unique requirements in:
  - Collection and Analysis
  - Storage
  - Reporting and Alerting
- Implement a pilot process for your SIEM.

Activities

- Review your requirements and set up your SIEM solution for these requirements.
- Test your SIEM solution through a pilot process.

Step 6: Create the SIEM Implementation Plan

Hand over to operations

- Prepare to transfer management of your SIEM suite from the implementation team to IT operations.

Activities

- Create transition planning.
- Prepare to hand over to security operations.

Phase 4 Outcome:

- Comprehensive planning of your SIEM suite's implementation.

Step 6: Create a SIEM implementation plan

1. Assess value and identify fit
2. Build the procurement team and project plan
3. Identify the requirements for the SIEM
4. Produce the vendor shortlist
5. Select a SIEM solution
6. **Create an implementation plan**
7. Measure the value of the SIEM solution

This step will walk you through the following activities:

6.1: Design your SIEM architecture and identify constraints.
6.2: Optimize and improve the SIEM solution design.
6.3: Account for associated resource costs.
6.4: Implement the unique SIEM capabilities.
6.5: Avoid common SIEM deployment mistakes.
6.6: Run your implementation phases in tandem.
6.7: Implement planning and control for hand-off to operations.
6.8: Hand over the management of your SIEM suite to operations

Info-Tech suggests involving the following participants in this step of the project:

- Security manager
- Security team
- Network manager

Outcomes of this step:

- A formalized strategy for implementing the SIEM solution
- Defined next-steps for passing SIEM handling to operations

Create your project plan for guiding the implementation of your selected SIEM suite

SIEM Work Breakdown

- Design your SIEM architecture
- Identify constraints for your SIEM solution
- Optimize and improve the SIEM solution design
- Account for the resource costs that are associated with implementation
- Set up your:
  - Collection & Analysis
  - Storage
  - Reporting & Alerting
- Avoid common SIEM deployment mistakes

Considerations as you build your implementation roadmap:

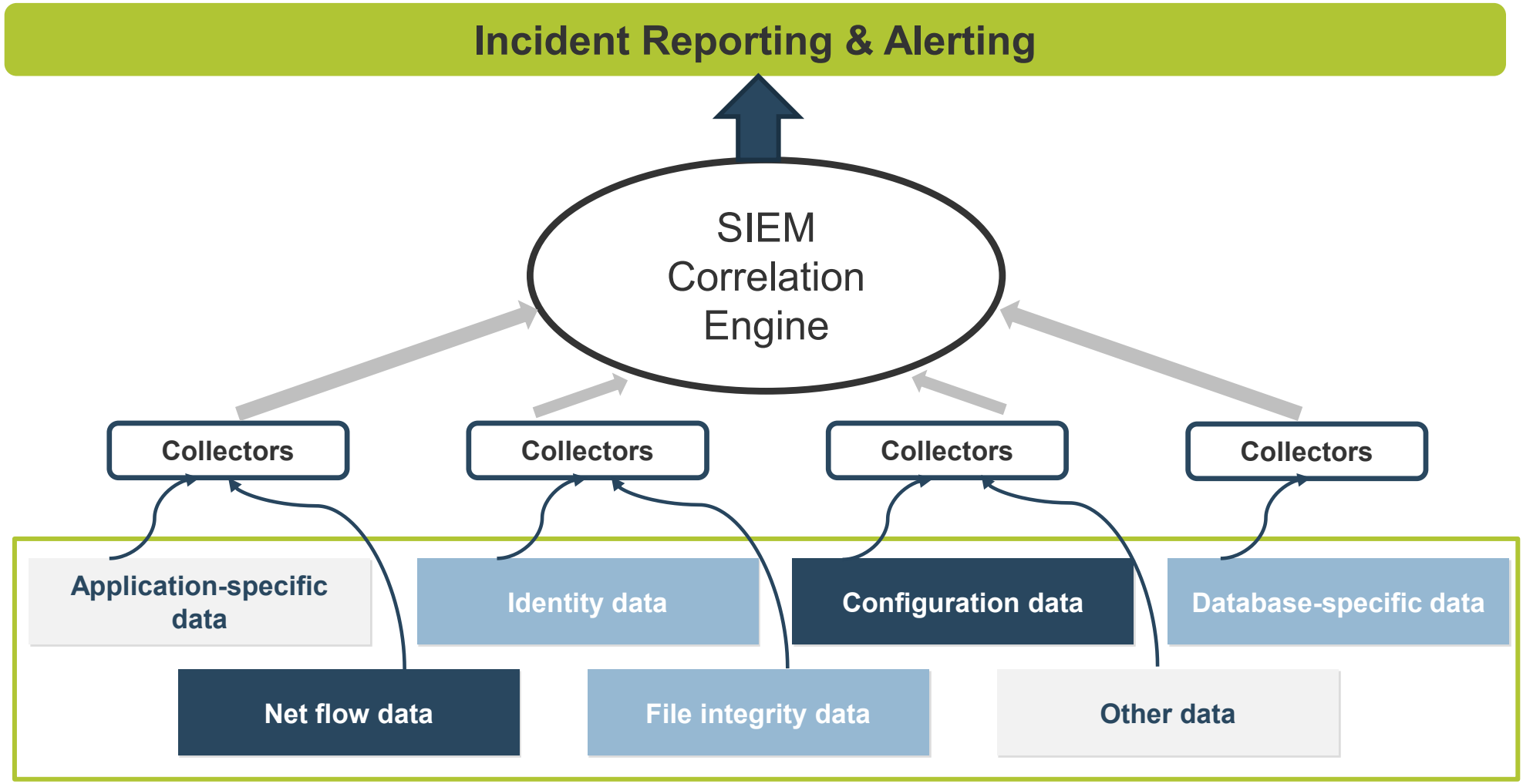
- **SIEM isn't plug-and-play technology;** spend time identifying the data integration and application interactions that will be required for successful business utilization of the SIEM suite
- The role of a third-party integrator in your steps
- The degree of vendor involvement in initial implementation, design mapping and end-user training

Call an analyst to assist in the formalization of your implementation plan.

Ongoing Operations: Steady State Production and Process Execution

Design your SIEM technology architecture

Ensure that your SIEM solution has the necessary architecture needed to support your organization.



Identify constraints for your SIEM architecture

Consider performance, capacity, and regulatory inputs in your design process.

SIEM vendors offer a variety of centralized and distributed deployment options – sometimes the best design is a mix of both.

Centralized design

Centralized components typically include log collectors, event correlation engines, and functions including alerting, reporting, and incident management tools.

- Whether all-in-one or separate but adjacent devices, deploying these components centrally reduces the management burden for SIEM.

Distributed design

Distributed designs *may* include single-purpose collectors and combination collector/correlation devices, which can support:

- Regulatory requirements (e.g. EU Safe Harbor) that restrict offshore movement of private/sensitive data.
- Performance and scalability needs by aggregating data from log sources at remote sites and offloading event correlation processing.

Server Deployment Options

Hierarchy of SIEM Servers

Tiers of systems that aggregate, correlate, and store data

Segmented Server Functions

Segmented servers for aggregation correlation, storage, reporting, and alerting

Hybrid

Combination of hierarchy and segmented

Info-Tech Insight

Cloud-based SIEM solutions (aka SIEMaaS) are maturing, but have yet to take over the market. Regulatory restrictions may limit the applicability of such services.

In contrast, managed security service provider (MSSP) solutions, in which a third party maintains and monitors a SIEM system housed on customer premises, offer greater promise today:

- Customer control over sensitive data.
- Shared access to 24/7 monitoring at a fraction of the cost.

Optimize and improve the SIEM solution design

Understand your current IT environment in order to size the SIEM solution properly and minimize WAN impact.

- SIEM deployments are sized based on two key factors: *logging rate* and *storage capacity*.
- Logging rates, or the number of log records that the system can process, are measured in *events* or *messages* per second (eps or MPS):
  - Collectors must be sized to handle the *peak* number of events per second or risk losing critical log records.
  - **Peak eps** requirements for a SIEM solution are determined by summing the peak logging rates of all source devices. Though it is unlikely that all devices will hit peak rates simultaneously, this provides the capacity to handle elevated logging demands from extraordinary events such as denial of service attacks and malware outbreaks.
- Storage capacity requirements depend on logging rates, but with a little math:
  - All SIEM solutions perform some level of log file compression, typically ranging between a 20 to 40-fold reduction in log file sizes.
  - **Total storage capacity** requirements can be calculated by summing the average daily log file size of each source device, multiplying by the required retention period, and dividing by the SIEM compression rate.
  - Some SIEM solutions allow retention periods to be defined by device (or group of devices), while others establish a single, default retention period.

Info-Tech Insight

For multi-site deployments, look to distributed components to optimize SIEM *and* network performance.

Distributed log collectors:

- Spread the peak eps load across multiple devices.
- Compress log data before forwarding on to a central collector, saving considerably on WAN traffic.

Account for the resource costs that are associated with implementation

To ensure success with your SIEM solution, make sure that all the correct parties are engaged beyond just the security team.

Consider your maintenance team

Security, network, and system administers all have notable duties for the SIEM solution:

- Identification of log data sources
- Configuration of log data sources
- Defining event security levels
- Creating reporting formals and schedules
- Setting monitoring, alerting, and escalation processes

Auditors and other personnel involved with compliance will also play important roles here:

- Creating reporting templates for compliance management
- Assisting in the design of a dashboard to review information more easily
- Defining specific requirements for the data or information that is sensitive or highly regulated

Consider your training obligations

- Training will be critical for all project team members, and associated employees.
- Specific technical and security training will be needed for any employees who are able to use the SIEM directly.
- Process and reporting training will be needed for those who just need the outputs.

Implement collection, analysis, storage, and reporting and alerting capabilities of your SIEM solution

6.4 1-2 hours

Instructions

Set up the remaining architecture pieces and features of your SIEM solution that are unique to your organization.

- The majority of these features will be focused around the previously collected requirements.

Information Sources
- SIEM vendor information
- Requirements

Time
- Varies

Result
- Technical requirements
- Implementation requirements

Collection
- Deploy your collectors in order to make sure the necessary logs are being gathered.

Analysis
- Ensure that your correlation engines have the desired policies.
- Customize your forensic analysis for relevant and pertinent information to appear.

Reporting and Alerting
- Determine when alerts should be employed to ensure that security events are remediated in a timely fashion.
- Set up your reporting functions in order to meet your specific compliance obligations and other reporting needs.

Call an analyst to assist in the creation of your SIEM capabilities.

Storage
- Ensure that log storage is properly set up in order to appropriate log management.
- Set up the timeline in which you want your logs to be stored and managed.
- Determine where storage is available in your organization and if more is needed.

Avoid common SIEM deployment mistakes

Insufficient staffing

Ensure that you have appropriate staffing for your SIEM technology. A SIEM is a tool – it is useless without individuals to track and manage security events.

No logging process in place

Without a formal logging process, you will not be collecting the information needed for a SIEM to provide strong value. Many compliance obligations require you to collect logs and for specified periods of time.

Poor management of logs

By enabling your SIEM product to collect all your logs all at once, it will quickly cause a large influx of security events. The number of false positives will also increase, which may cause your staff to disregard events, including serious threats.

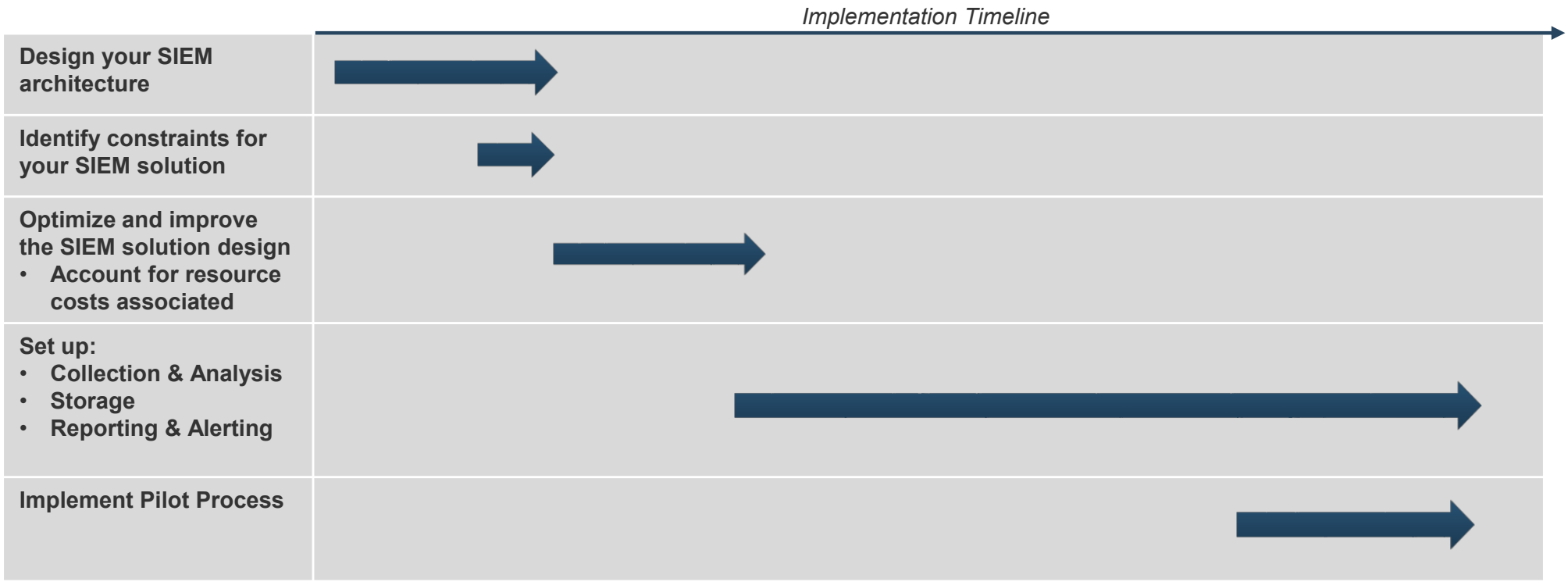
Log collection is not sufficiently comprehensive

Often, SIEM solutions are focused on collecting logs from the internal devices and from the perimeter, but can miss other critical information. Application logging is often forgotten and this can provide crucial information needed for effective analysis.

> *"You need to consider the Do's and Don'ts of any IT project – they still apply to SIEM."*
>
> - Sofiane Chtioui, IT Architect and Security Consultant, Hypratek Solutions Inc.

Run your implementation phases in tandem based on dependent activities and timeline considerations

6.6



Consider using Info-Tech's *Project Planning and Monitoring Tool* to help create an implementation plan for your organization.

> *Start with a limited set of use cases and data sources. It's then easier to move forward with phases and you can add more information. Start small, show results, make it work and then it's possible to evolve and grow.*
>
> - Sofiane Chtioui, IT Architect and Security Consultant, Hypratek Solutions Inc.

Implement planning and control for the hand-off to operations

Risk Management

- Track risks associated with your SIEM suite.
  - Assign owners and create plans for resolving open risks.

Organizational Change Management

- Train the necessary IT staff on how to support the daily operations of the suite.
- Create a communication plan to notify stakeholders and impacted users about the tool and how it will alter their workday and performance of role activities.

Project Management

- Conduct a post-mortem to evaluate the completion of the project.
- Review the project's performance against its metrics and expectations (Activity 2.5)
- Perform a formal sign-off and transfer for managing the tool.

Knowledge Transfer

Make sure the tacit knowledge and learning about the suite and process automation are not isolated to the implementation team. As you transition the support of the tool to operations, make sure that the knowledge and insight regarding the tool and SIEM technology as a whole are also conveyed.

Additional Steps

Draft a plan for any additional training that might be needed to facilitate acceptance and use of the product/service.

Hand over the management of your SIEM suite to operations

Switch IT's role from that of planter to gardener for your solution.
Prepare IT for managing the steady state production of processes and IT support for the tool.

Implementation Team	**Integrators**	***Transition***	**Service Management Staff**
Vendor Implementation Team			**Vendor Support**

Transition Planning

Prepare IT staff and the organization to manage the steady state performance of the application.

1. Create operations package.
2. Conduct operations training.
3. Determine SLAs.

Service Management

Prepare IT service management to handle the service support and service operations for the daily use of your organization's SIEM suite.

1. Develop change management procedures.
2. Identify standard changes.
3. Identify incident management procedures.
4. Create incident management records for SIEM.
5. Identify problem management procedures for SIEM.
6. Create problem management procedures for SIEM.
7. Conduct ongoing maintenance and software updates.

Info-Tech's Service Management Research

Support the creation of procedures for your SIEM with this research:

Change and Release Management

Incident and Problem Management

Step 7: Measure the value of the SIEM solution

1. Assess value and identify fit
2. Build the procurement team and project plan
3. Identify the requirements for the SIEM
4. Produce the vendor shortlist
5. Select a SIEM solution
6. Create an implementation plan
7. **Measure the value of the SIEM solution**

This step will walk you through the following activities:

7.1: Be prepared for the increased vulnerability that comes with a SIEM.
7.2: Count the metrics that matter to your business.
7.3: Continue to grow the scope and impact of your SIEM suite.

Info-Tech suggests involving the following participants in this step of the project:

- Project sponsor
- Project manager

Outcomes of this step:

- Selection and application of process and suite metrics that will gauge the value and effectiveness of the SIEM investment
- Identification of how to review the opportunities related to SIEM and creation of a plan/perspective that will allow the suite to increase its scope and impact within the business

Be prepared for the impact of having the visibility that comes with a SIEM solution

Once your SIEM solution is implemented, there will be visibility into events and incidents that you were previously unaware of.

Pre-SIEM

- Hidden security threats are able to exploit your network.
- Risks and costs continue to rise, especially as these threats are difficult to identify.

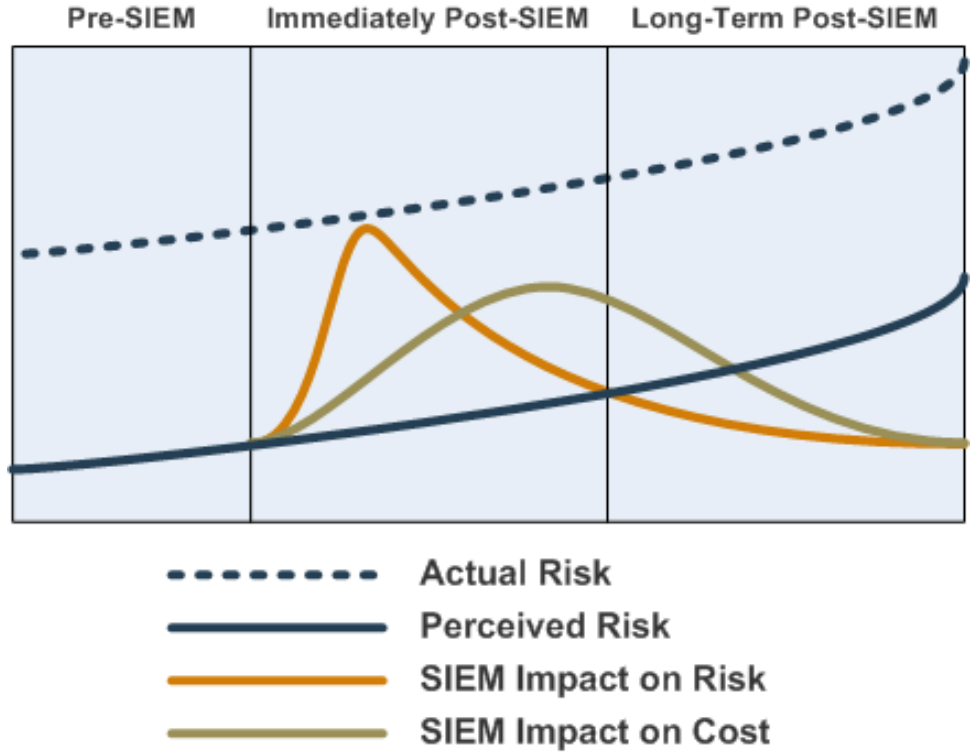
Immediately Post-SIEM

- Sophisticated and more advanced threats become visible to the organization, which were previously undetected.
- However, costs will increase as well as these threats need to be managed:
  - Ignorance can no longer be used as justification; with awareness, action is necessary.
- As the threats are remediated, the overall risk will begin to decline.

Long-Term Post-SIEM

- Both the risks and costs associated with SIEM will continue to decline, as the SIEM controls and policies are optimized and improved upon.

SIEM's Impact on Risk and Cost Over Time

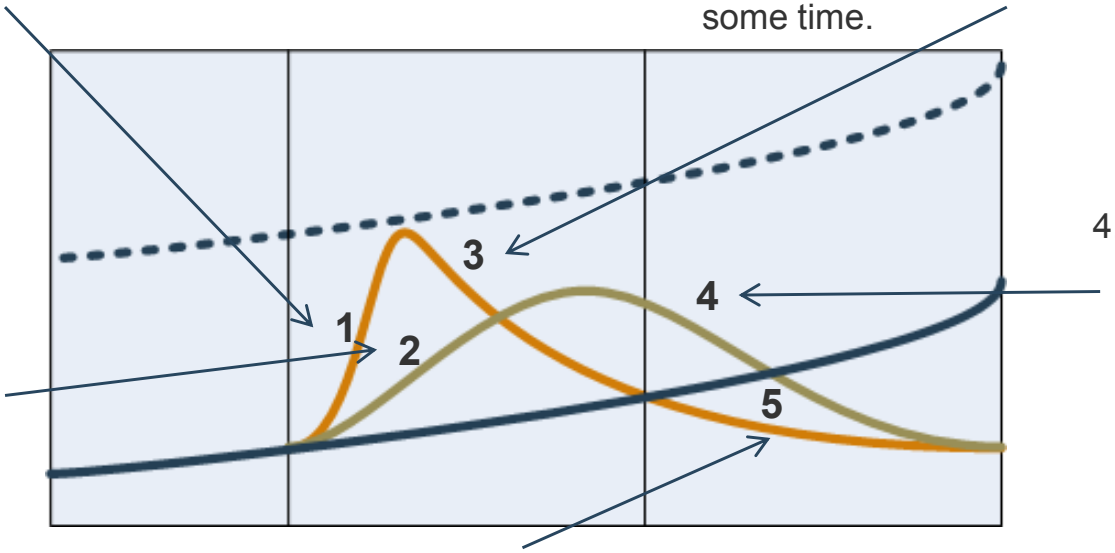


SIEM may make life harder before it makes it easier; if you can't handle the bump, don't invest in SIEM

Improving organizational security stance is not an overnight process; SIEM will help, but things will get worse before they get better.

1. When first deployed, a SIEM solution will expose the enterprise to all the risk it was missing but that existed. In today's regulated world, if you're not prepared to address that increased risk, you'd best just stay unaware.

2. As visibility into risk increases, security spending will, by necessity, increase as new tools and/or time need to be expended to combat identified risks. Most enterprises don't have unlimited security budgets, so spending initially trails behind threat exposure.



3. As the most serious threats are addressed, risk tapers off fairly quickly. At this point perceived risk *and* actual risk are being reduced, though levels are likely to be higher than what was perceived for some time.

4. Spending remains higher for longer as solution deployments must be rationalized and staffing levels finalized. Spending begins to go down when the costs associated with breaches and other threats are eliminated.

5. In time and with concentrated effort, SIEM can enable the enterprise to drive risk and spending to lower levels than were previously experienced. As a side benefit, while risk is being addressed, SIEM is also providing compliance reporting benefits that help in other ways.

Implementation of a SIEM can take time, but will yield great results

Williams Lea
Andrew Allison, Information Security Manager

Company Description: Business process outsourcing company
User Count: 2,500

Source: *ComputerWeekly.com: SIEM Deployment cast study shows patience is required*

Situation

- Allison needed to manage the large number of employees, many of whom worked remotely or were often out of office.
- Further, since there are many contractors, there is a constant turnover for employees.
- One of the biggest duties for Allison was to maintain user privileges and access.
- This was completed by going through manual review of the logs.

Action

- Immediately upon implementation, the log review work became easier.
- It became possible to control admin users and address any generic logins.
- The process of baselining also provided insights into the overall network security.
- However, the full value was not realized just yet as there was still more configuration needed for success.

Future

- Plans were created to implement the IPS logs into the SIEM.
- Further, alerting was considered necessary to provide enhanced capabilities such as sending SMS messages or emails.
- Allison also viewed how the SIEM product could make the management of compliance standards easier.
- While the SIEM involved a great deal of groundwork, the network already became easier to manage and secure.

Determine the broader metrics that you will use to assess the value of your SIEM tool

The ROI and perceived value of the organization's SIEM solution will be a critical indicator of the success of the selection and implementation.

SIEM Solution and Technology Adoption

Solution Performance

- Number of raw and uncorrelated events vs. number of normalized and correlated events
- Number of devices monitored
- Number of critical or severe events detected
- Average time to become aware of a security event
- Decrease in number of false positives from the time that the SIEM is first implemented
- Mean time to detect a real security event, with a decrease after the SIEM is implemented

If your SIEM implementation is successful, it will start to grow on its own

Increase scope and impact of the suite

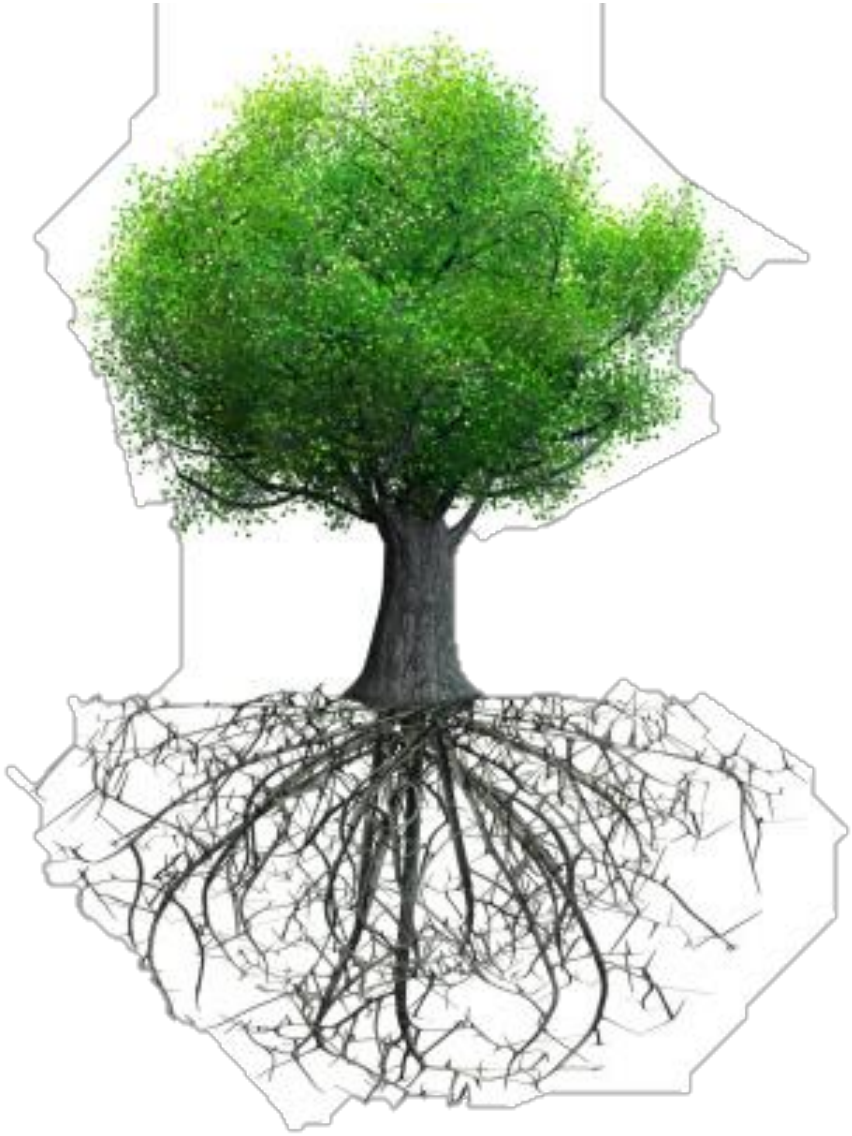
- Number of devices and users will continue to grow.
- More security will be delivered across the organization.
- Additional lines of the business will be protected through your SIEM suite.
- **Grow how you leverage the tool:** Explore and expand how processes and applications can be further supported or created within the suite's environment.

Continuous improvement

- Processes will continue to improve with additional insight during further design iterations.

An evolving landscape

- Vendors will continue to push the functional capabilities of SIEM solutions; update your suite to harvest additional value.

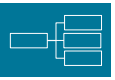


Summary of accomplishment

Knowledge Gained

- The benefits and value of a SIEM solution
- The necessary staff resources and stakeholders
- The metrics to evaluate both the selection process and the tool performance
- The necessary requirements and resource constraints in a SIEM solution
- The vendor and product that provides the best right-sized solution
- Guidelines for implementing the selected SIEM solution

Processes Optimized



- Launch the SIEM selection project.
- Analyze SIEM requirements.
- Shortlist SIEM vendors.
- Select the SIEM solution.
- Plan the SIEM implementation.

Deliverables Completed

- *SIEM Appropriateness Tool*
- *SIEM Procurement Project Charter Template*
- *SIEM Use-Case Fit Assessment Tool*
- *SIEM Vendor Landscape Analysis*
- *SIEM Vendor Shortlist and Detailed Analysis Tool*
- *SIEM RFP Template*
- *SIEM Solution Evaluation and RFP Scoring Tool*
- *SIEM Vendor Demo Script Template*

We'd like to thank the following research contributors and experts for their help in this project

Sofiane Chtioui, CISSP, CISM, IT Architect and Information Security Consultant
Hypratek Solutions Inc.

Sofiane is a seasoned IT professional and InfoSec consultant currently involved in various projects with a focus on aligning Information security and risk management capabilities to the enterprise business model.

He has a strong background in IT/InfoSec with over 22 years of experience in various roles such as management, architecture and design, consulting and pre-sales, solution design, and deployment.

Christopher (Kriss) Warner, President/Chief Security Consultant
Cyberdine

A 20+ year senior sales and technical IT and Security consultant with a documented history of meeting and exceeding client expectations and financial targets. Extensive experience in finding and delivering complex, enterprise solutions to financial, manufacturing, and government organizations within Canada, USA, and Latin America.

His skills include: business development based on consultancy approach; sales management; an extensive technical background in Cybersecurity technologies with focus on SIEM solutions; extensive experience in driving new sales and executing business plans to 100% completion.

Vendor Landscape Methodology: Overview

Info-Tech's Vendor Landscapes are research materials that review a particular IT market space, evaluating the strengths and abilities of both the products available in that space, as well as the vendors of those products. These materials are created by a team of dedicated analysts operating under the direction of a senior subject matter expert over a period of several weeks.

Evaluations weigh selected vendors and their products (collectively "solutions") on the following eight criteria to determine overall standing:

- Features: The presence of advanced and market-differentiating capabilities.
- User Interface: The intuitiveness, power, and integrated nature of administrative consoles and client software components.
- Affordability: The three-year total cost of ownership of the solution; flexibility of the pricing and discounting structure.
- Architecture: The degree of integration with the vendor's other tools, flexibility of deployment, and breadth of platform applicability.
- Viability: The stability of the company as measured by its history in the market, the size of its client base, and its percentage of growth.
- Focus: The commitment to both the market space, as well as to the various sized clients (small, mid-sized, and enterprise clients).
- Reach: The ability of the vendor to support its products on a global scale.
- Sales: The structure of the sales process and the measure of the size of the vendor's channel and industry partners.

Evaluated solutions within scenarios are visually represented by a Pathway to Success, based off a linear graph using above scoring methods:

- Use-case scenarios are decided upon based on analyst expertise and experience with Info-Tech clients.
- Use-case scenarios are defined through feature requirements, predetermined by analyst expertise.
- Placement within scenario rankings consists of features being evaluated against the other scoring criteria.

Info-Tech's Vendor Landscapes are researched and produced according to a strictly adhered to process that includes the following steps:

- Vendor/product selection
- Information gathering
- Vendor/product scoring
- Information presentation
- Fact checking
- Publication

This document outlines how each of these steps is conducted.

Vendor Landscape Methodology: Vendor/Product Selection & Information Gathering

Info-Tech works closely with its client base to solicit guidance in terms of understanding the vendors with whom clients wish to work and the products that they wish evaluated; this demand pool forms the basis of the vendor selection process for Vendor Landscapes. Balancing this demand, Info-Tech also relies upon the deep subject matter expertise and market awareness of its Senior Analysts to ensure that appropriate solutions are included in the evaluation. As an aspect of that expertise and awareness, Info-Tech's analysts may, at their discretion, determine the specific capabilities that are required of the products under evaluation, and include in the Vendor Landscape only those solutions that meet all specified requirements.

Information on vendors and products is gathered in a number of ways via a number of channels.

Initially, a request package is submitted to vendors to solicit information on a broad range of topics. The request package includes:

- A detailed survey.
- A pricing scenario (see Vendor Landscape Methodology: Price Evaluation and Pricing Scenario, below).
- A request for reference clients.
- A request for a briefing and, where applicable, guided product demonstration.

These request packages are distributed approximately eight weeks prior to the initiation of the actual research project to allow vendors ample time to consolidate the required information and schedule appropriate resources.

During the course of the research project, briefings and demonstrations are scheduled (generally for one hour each session, though more time is scheduled as required) to allow the analyst team to discuss the information provided in the survey, validate vendor claims, and gain direct exposure to the evaluated products. Additionally, an end-user survey is circulated to Info-Tech's client base and vendor-supplied reference accounts are interviewed to solicit their feedback on their experiences with the evaluated solutions and with the vendors of those solutions.

These materials are supplemented by a thorough review of all product briefs, technical manuals, and publicly available marketing materials about the product, as well as about the vendor itself.

Refusal by a vendor to supply completed surveys or submit to participation in briefings and demonstrations does not eliminate a vendor from inclusion in the evaluation. Where analyst and client input has determined that a vendor belongs in a particular evaluation, it will be evaluated as best as possible based on publicly available materials only. As these materials are not as comprehensive as a survey, briefing, and demonstration, the possibility exists that the evaluation may not be as thorough or accurate. Since Info-Tech includes vendors regardless of vendor participation, it is always in the vendor's best interest to participate fully.

All information is recorded and catalogued, as required, to facilitate scoring and for future reference.

Vendor Landscape Methodology: Scoring

Once all information has been gathered and evaluated for all vendors and products, the analyst team moves to scoring. All scoring is performed at the same time so as to ensure as much consistency as possible. Each criterion is scored on a ten-point scale, though the manner of scoring for criteria differs slightly:

- Features is scored via **Cumulative Scoring.**
- Affordability is scored via **Scalar Scoring.**
- All other criteria are scored via **Base5 Scoring.**

Cumulative Scoring is on a four-point scale. Zero points are awarded to features that are deemed absent or unsatisfactory, one point is assigned to features that are partially present, two points are assigned to features that require an extra purchase in the vendor's product portfolio or through a third party, three points are assigned to features that are fully present and native to the solution, and four points are assigned to the best-of-breed native feature. The assigned points are summed and normalized to a value out of ten. For example, if a particular Vendor Landscape evaluates eight specific features in the Feature Criteria, the summed score out of eight for each evaluated product would be multiplied by 1.25 to yield a value out of ten to represent in a Harvey Ball format.

In Scalar Scoring, a score of ten is assigned to the lowest cost solution, and a score of one is assigned to the highest cost solution. All other solutions are assigned a mathematically-determined score based on their proximity to / distance from these two endpoints. For example, in an evaluation of three solutions, where the middle cost solution is closer to the low end of the pricing scale it will receive a higher score, and where it is closer to the high end of the pricing scale it will receive a lower score; depending on proximity to the high or low price it is entirely possible that it could receive either ten points (if it is very close to the lowest price) or one point (if it is very close to the highest price). Where pricing cannot be determined (vendor does not supply price and public sources do not exist), a score of 0 is automatically assigned.

In Base5 scoring a number of sub-criteria are specified for each criterion (for example, Longevity, Market Presence, and Financials are sub-criteria of the Viability criterion), and each one is scored on the following scale:

5 - The product/vendor is exemplary in this area (nothing could be done to improve the status).
4 - The product/vendor is good in this area (small changes could be made that would move things to the next level).
3 - The product/vendor is adequate in this area (small changes would make it good, more significant changes required to be exemplary).
2 - The product/vendor is poor in this area (this is a notable weakness and significant work is required).
1 - The product/vendor fails in this area (this is a glaring oversight and a serious impediment to adoption).

The assigned points are summed and normalized to a value out of ten as explained in Cumulative Scoring above.

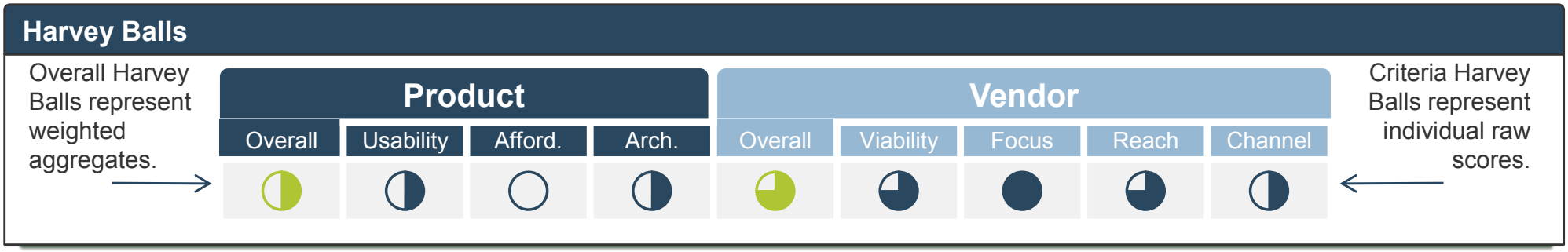
Scores out of ten, known as Raw scores, are transposed as is into Info-Tech's *Vendor Landscape Shortlist Tool,* which automatically determines Vendor Landscape positioning (see Vendor Landscape Methodology: Information Presentation – Vendor Landscape, below), Criteria Score (see Vendor Landscape Methodology: Information Presentation – Criteria Score, below), and Value Index (see Vendor Landscape Methodology: Information Presentation – Value Index, below).

Vendor Landscape Methodology: Information Presentation – Criteria Scores (Harvey Balls)

Info-Tech's criteria scores are visual representations of the absolute score assigned to each individual criterion, as well as of the calculated overall vendor and product scores. The visual representation used is Harvey Balls.

Harvey Balls are calculated as follows:

1. Raw scores are transposed into the Info-Tech *Vendor Landscape Shortlist Tool* (for information on how raw scores are determined, see Vendor Landscape Methodology: Scoring, above).
2. Each individual criterion raw score is multiplied by a pre-assigned weighting factor for the Vendor Landscape in question. Weighting factors are determined prior to the evaluation process, based on the expertise of the Senior or Lead Research Analyst, to eliminate any possibility of bias. Weighting factors are expressed as a percentage, such that the sum of the weighting factors for the vendor criteria (Viability, Strategy, Reach, Channel) is 100%, and the sum of the product criteria (Features, Usability, Affordability, Architecture) is 100%.
3. A sum-product of the weighted vendor criteria scores and of the weighted product criteria scores is calculated to yield an overall vendor score and an overall product score.
4. Both overall vendor score / overall product score, as well as individual criterion raw scores are converted from a scale of one to ten to Harvey Ball scores on a scale of zero to four, where exceptional performance results in a score of four and poor performance results in a score of zero.
5. Harvey Ball scores are converted to Harvey Balls as follows:
   - A score of four becomes a full Harvey Ball.
   - A score of three becomes a three-quarter full Harvey Ball.
   - A score of two becomes a half-full Harvey Ball.
   - A score of one becomes a one-quarter full Harvey Ball.
   - A score of zero becomes an empty Harvey Ball.
6. Harvey Balls are plotted by solution in a chart where rows represent individual solutions and columns represent overall vendor / overall product, as well as individual criteria. Solutions are ordered in the chart alphabetically by vendor name.



Vendor Landscape Methodology: Use-Case Scoring

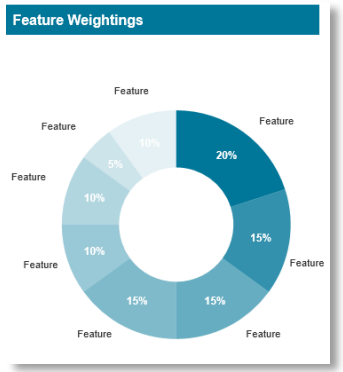
Within each Vendor Landscape a set of use-case scenarios are created by the analysts by considering the different outcomes and purposes related to the technology being evaluated. To generate the custom use-case vendor performances, the feature and Harvey ball scoring performed in the Vendor Landscapes are set with custom weighting configurations.

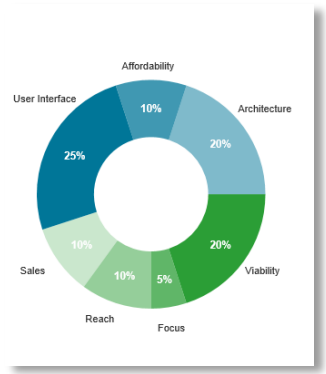
Calculations
Each product has a vendor multiplier calculated based on their weighted performance, considering the different criteria scored in the Harvey Ball evaluations.

To calculate each vendor's performance, the advanced feature scores are multiplied against the weighting for the feature in the use case scenario's configuration.

The weighted advanced feature score is then multiplied against the vendor multiplier.

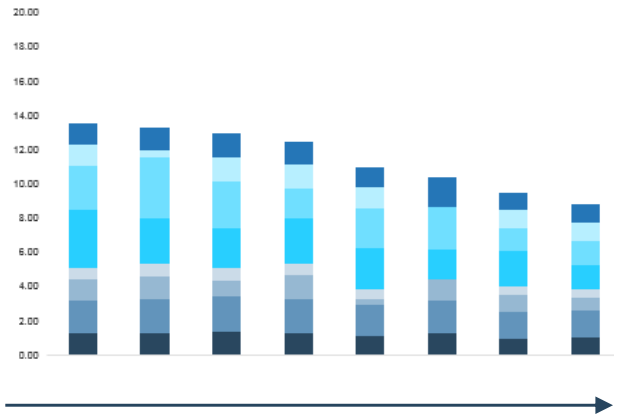
The sum of each vendor's total weighted advanced features is calculated. This sum is used to identify the vendor's qualification and relative rank within the use case.





Each use case's feature weightings and vendor/product weighting configurations are displayed within the body of slide deck.

Use Case Vendor Performance



Vendors who qualified for each use case scenario are ranked from first to last in a weighted bar graph based on the features considered.

Vendor Landscape Methodology: Information Presentation – Value Index

Info-Tech's Value Index is an indexed ranking of solution value per dollar as determined by the raw scores assigned to each criteria (for information on how raw scores are determined, see Vendor Landscape Methodology: Scoring, above).

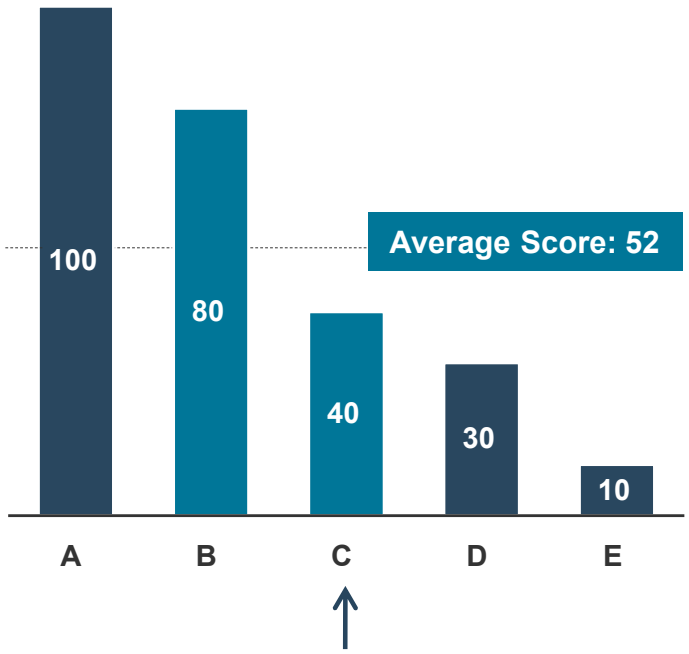
Value scores are calculated as follows:

1. The TCO Affordability criterion is removed from the Affordability score and the remaining product score criteria (Features, Usability, Architecture). Affordability scoring is adjusted with the TCO weighting distributed in proportion to the use case's weighting for Affordability. Weighting is adjusted as to retain the same weightings relative to one another, while still summing to 100%.
2. An adjusted multiplier is determined for each vendor using the recalculated Affordability scoring.
3. The multiplier vendor score and vendor's weighted feature score (based on the use case scenario's weightings), are summed. This sum is multiplied by the TCO raw score to yield an interim Value Score for each solution.
4. All interim Value Scores are then indexed to the highest performing solution by dividing each interim Value Score by the highest interim Value Score. This results in a Value Score of 100 for the top solution and an indexed Value Score relative to the 100 for each alternate solution.
5. Solutions are plotted according to Value Score, with the highest score plotted first, and all remaining scores plotted in descending numerical order.

Where pricing is not provided by the vendor and public sources of information cannot be found, an Affordability raw score of zero is assigned. Since multiplication by zero results in a product of zero, those solutions for which pricing cannot be determined receive a Value Score of zero. Since Info-Tech assigns a score of zero where pricing is not available, it is always in the vendor's best interest to provide accurate and up-to-date pricing. In the event that insufficient pricing is available to accurately calculate a Value Index, Info-Tech will omit it from the Vendor Landscape.

Value Index

Vendors are arranged in order of Value Score. The Value Score each solution achieved is displayed, and so is the average score.

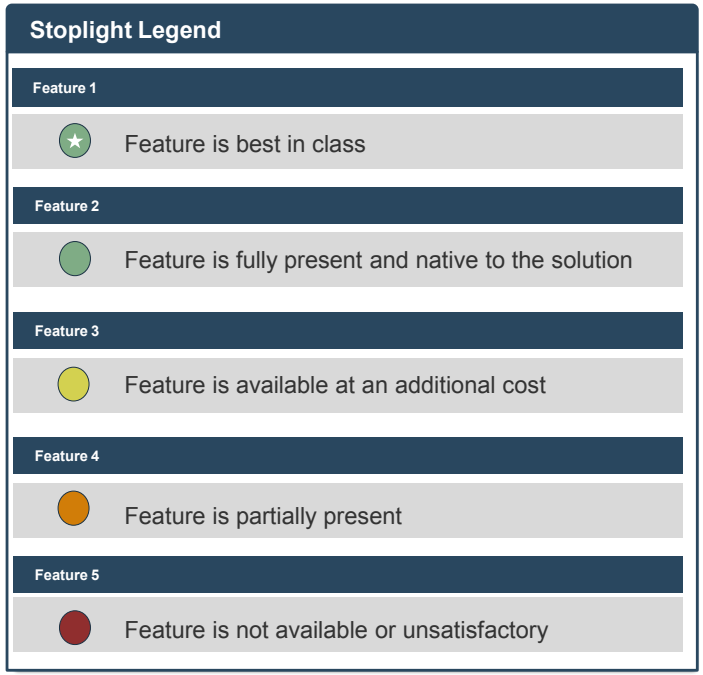


Those solutions that are ranked as Champions are differentiated for point of reference.

Vendor Landscape Methodology: Information Presentation – Feature Ranks (Stoplights)

Advanced features are determined by analyst expertise, leveraging information gained from conversations with clients. Advanced features chosen as part of the evaluation are representative of what Info-Tech clients have indicated are of importance to their vendor solution. Advanced features are evaluated through a series of partial marks, dedicated to whether the solution performs all aspects of the Info-Tech definition of the feature and whether the feature is provided within the solution. Analysts hold the right to determine individual, unique scoring criteria for each evaluation. If a feature does not meet the criteria, Info-Tech holds the right to score the feature accordingly.

Use cases use features as a baseline of the inclusion and scoring criteria.



Vendor Landscape Methodology: Information Presentation – Price Evaluation: Small Enterprise

Info-Tech's Price Evaluation is a tiered representation of the three-year Total Cost of Ownership (TCO) of a proposed solution. Info-Tech uses this method of communicating pricing information to provide high-level budgetary guidance to its end-user clients while respecting the privacy of the vendors with whom it works. The solution TCO is calculated and then represented as belonging to one of ten pricing tiers.

Pricing tiers are as follows:

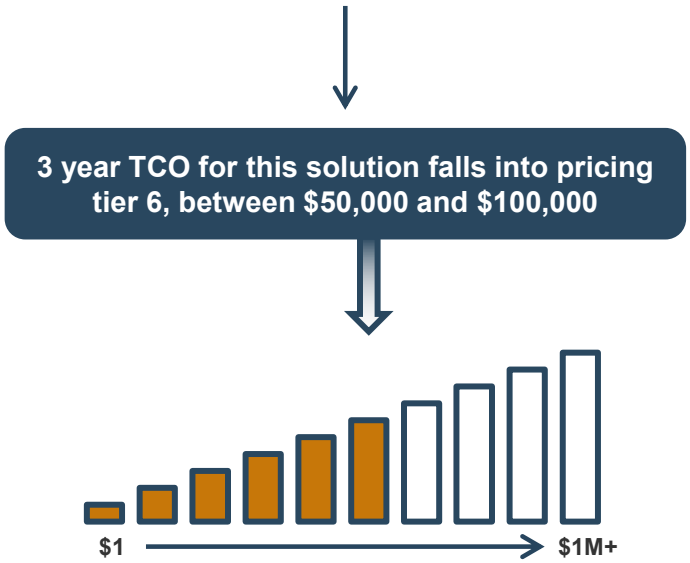
1. Between $1 and $2,500
2. Between $2,500 and $5,000
3. Between $5,000 and $10,000
4. Between $10,000 and $25,000
5. Between $25,000 and $50,000
6. Between $50,000 and $100,000
7. Between $100,000 and $250,000
8. Between $250,000 and $500,000
9. Between $500,000 and $1,000,000
10. Greater than $1,000,000

Where pricing is not provided, Info-Tech makes use of publicly available sources of information to determine a price. As these sources are not official price lists, the possibility exists that they may be inaccurate or outdated, and so the source of the pricing information is provided. Since Info-Tech publishes pricing information regardless of vendor participation, it is always in the vendor's best interest to supply accurate and up to date information.

Info-Tech's Price Evaluations are based on pre-defined pricing scenarios (see Product Pricing Scenario, below) to ensure a comparison that is as close as possible between evaluated solutions. Pricing scenarios describe a sample business and solicit guidance as to the appropriate product/service mix required to deliver the specified functionality, the list price for those tools/services, as well as three full years of maintenance and support.

Price Evaluation

Call-out bubble indicates within which price tier the three-year TCO for the solution falls, provides the brackets of that price tier, and links to the graphical representation.



Scale along the bottom indicates that the graphic as a whole represents a price scale with a range of $1 to $1M+, while the notation indicates whether the pricing was supplied by the vendor or derived from public sources.

Vendor Landscape Methodology: Information Presentation – Vendor Awards

At the conclusion of all analyses, Info-Tech presents awards to exceptional solutions in three distinct categories. Award presentation is discretionary; not all awards are extended subsequent to each Vendor Landscape and it is entirely possible, though unlikely, that no awards may be presented.

Awards categories are as follows:

- **Champion Awards** are presented to the top performing solution in a particular use case scenario. As a result, only one Champion Award is given for each use case, and the entire Vendor Landscape will have the same number of Champion Awards as the number of evaluated use cases.
- **Leader Awards** are presented to top performing solutions for each use-case scenario. Depending on the use-case scenario and the number of solutions being evaluated, a variable number of leader awards will be given. This number is at the discretion of the analysts, but is generally placed at two, and given to the solutions ranking second and third respectively for the use case.
- **Best Overall Value Awards** are presented to the solution for each use-case scenario that ranked the highest in the Info-Tech Value Index for each evaluated scenario (see Vendor Landscape Methodology: Information Presentation – Value Index, above). If insufficient pricing information is made available for the evaluated solutions, such that a Value Index cannot be calculated, no Best Overall Value Award will be presented. Only one Best Overall Value Award is available for each use-case scenario.

Vendor Awards for Use Case Performance

Info-Tech's **Champion Award** is presented to solutions that placed first in an use-case scenario within the Vendor Landscape.

Info-Tech **Leader Award** is given to solutions who placed in the top segment of a use-case scenario.

Info-Tech's **Best Overall Value Award** is presented to the solution within each use-case scenario with the highest Value Index score.

Vendor Landscape Methodology: Fact Check & Publication

Info-Tech takes the factual accuracy of its Vendor Landscapes, and indeed of all of its published content, very seriously. To ensure the utmost accuracy in its Vendor Landscapes, we invite all vendors of evaluated solutions (whether the vendor elected to provide a survey and/or participate in a briefing or not) to participate in a process of fact check.

Once the research project is complete and the materials are deemed to be in a publication ready state, excerpts of the material specific to each vendor's solution are provided to the vendor. Info-Tech only provides material specific to the individual vendor's solution for review encompassing the following:

- All written review materials of the vendor and the vendor's product that comprise the evaluated solution.
- Info-Tech's Criteria Scores / Harvey Balls detailing the individual and overall vendor / product scores assigned.
- Info-Tech's Feature Rank / stoplights detailing the individual feature scores of the evaluated product.
- Info-Tech's Raw Pricing for the vendor either as received from the vendor or as collected from publicly available sources.
- Info-Tech's Scenario ranking for all considered scenarios for the evaluated solution.

Info-Tech does not provide the following:

- Info-Tech's Vendor Landscape placement of the evaluated solution.
- Info-Tech's Value Score for the evaluated solution.
- End-user feedback gathered during the research project.
- Info-Tech's overall recommendation in regard to the evaluated solution.

Info-Tech provides a one-week window for each vendor to provide written feedback. Feedback must be corroborated (be provided with supporting evidence), and where it does, feedback that addresses factual errors or omissions is adopted fully, while feedback that addresses opinions is taken under consideration. The assigned analyst team makes all appropriate edits and supplies an edited copy of the materials to the vendor within one week for final review.

Should a vendor still have concerns or objections at that time, they are invited to a conversation, initially via email, but as required and deemed appropriate by Info-Tech, subsequently via telephone, to ensure common understanding of the concerns. Where concerns relate to ongoing factual errors or omissions, they are corrected under the supervision of Info-Tech's Vendor Relations personnel. Where concerns relate to ongoing differences of opinion, they are again taken under consideration with neither explicit not implicit indication of adoption.

Publication of materials is scheduled to occur within the six weeks following the completion of the research project, but does not occur until the fact check process has come to conclusion, and under no circumstances are "pre-publication" copies of any materials made available to any client.

Pricing Scenario, slide 1 of 2

Info-Tech Research Group is providing each vendor with a common pricing scenario to enable normalized scoring of Affordability, calculation of Value Index rankings, and identification of the appropriate solution pricing tier as displayed on each vendor scorecard.

The pricing scenario functionality applies to at least one of the use cases. Please indicate if your pricing would be significantly different if your products were used for any of the other use cases being considered.

Vendors are asked to provide *list* costs for SIEM software licensing to address the needs of a reference organization described in the pricing scenario. Please price out the **lowest possible** 3-year Total Cost of Ownership (TCO) including list prices for software and licensing fees to meet the requirements of the following scenario.

Three-year total acquisition costs will be normalized to produce the Affordability raw scores and calculate Value Index ratings for each solution.

The pricing scenario:

- A mid-level retailer with corporate offices on the US West Coast, East Coast, and in Ireland is looking to implement a SIEM solution. The company employs 2,200 people. The firm is interested in reducing the effort associated with monitoring, alerting, and responding to security events at the endpoint, network, and data center levels. The firm also has 100 retail outlets scattered throughout the US and Europe, however, *all stores are franchised and, so, out of scope*.
- The corporate office breakdown is as follows:

US West Coast (Head Office)

- Employing 1,600 people (70%), the West Coast office holds Sales, Finance, Strategy, Marketing, Buyers, and the majority of IT. The IT staff here consists of 45 employees, three of which are dedicated security professionals consisting of one security manager and two security analysts.

US East Coast (Satellite)

- Employing 200 people (10%), the East Coast office includes only Sales and Marketing staff.

Ireland (Satellite)

- Employing 400 people (20%), the Ireland office employs buyers and manufacturing, and also a DR facility. Manufacturing consists of 300 employees. The company's remaining five IT staff are located here although none have dedicated security responsibilities.

In terms of the IT infrastructure of the organization, consider the following:

General Infrastructure

- Internal network is gigabit throughout.
  - Redundant core routers at all three facilities
  - Distribution switches: 80 at head office, 10 at East Coast, 20 in Ireland

Pricing Scenario, slide 2 of 2

- Primarily Microsoft – 70% virtualized
  - Four domain servers (two at head office, one at each of the other offices)
  - HA production virtual server cluster at head office, plus separate dev and QA virtual servers in Ireland (also used for DR purposes)
  - Oracle DB on HP-UX dual servers (non-virtual) at the US West Coast office, and a single instance in Ireland.
  - Exchange 2010 (two servers)
  - SharePoint 2010 (one server)
  - 700 laptops running Windows 7; 1,200 desktops also running Windows 7
  - Blackberry is the standard corporate mobile device (with a single BES server), but iOS and Android phones and tablets are allowed to connect via a guest wireless network
  - Running a virtualized VOIP system as opposed to a traditional PBX

Security Infrastructure

- Gateway firewalls at each site
- Endpoint and gateway anti-malware
- Endpoint encryption is implemented on all laptops
- No IDPS or content filtering

Sensors and Event Volumes

- The organization requires licensing/capacity for 150 sensors in the US HQ, 25 sensors in the US remote, and 50 sensors in the Ireland office.
- Peak volume of logged events is 7,500 eps.

Support Services

Gold-level support services should include the following:

- Technical documentation and guides
- 24/7 technical support by phone or online

Other

- Do not include licensing cost for Microsoft host server operating systems.
- If the management suite requires the purchase of an additional host server, do not include the cost of the server, but clearly indicate this requirement.