How To Use This RFP Template

Step 1: Download The Buyer's Guide to Next-Gen SIEM, and determine your requirements.

Step 2: Use this workbook as a starting point to evaluate SIEM platforms.

Step 3: Score respondent based on answers and description.

Step 4: Total the score and compare vendors.

Category

Vendor Maturity

Question 1

Is the solution SaaS only, or can I deploy it on-prem and self-host?

Answer

Describe how you would demonstrate this to us

Why this matters

Modern security platforms are cloud-native, and only run in the cloud. If there is an on-prem version, it's probably a legacy SIEM posing as a next-gen SIEM.

Score
(0-3, with 3 being the perfect score)

0 1 2 3

Question 2

How long can you keep data hot? How much does it cost to store 1 year of hot, searchable data?

Answer

Describe how you would demonstrate this to us

Why this matters

Being able to search historical data with speed is critical. It should not be cost-prohibitive to search 6 months to a year of historical data.

Score
(0-3, with 3 being the perfect score)

0 1 2 3

Question 3

Do you provide migration services, or is it 3rd party?

Answer

Describe how you would demonstrate this to us

Why this matters

It's not uncommon to use 3rd party partners for services as long as they are qualified. But nothing beats a team of experts who work for the vendor to do professional services.

Score
(0-3, with 3 being the perfect score)

0 1 2 3

Question 4

Please describe your implementation services, including your normalization and tuning processes.

Answer

Describe how you would demonstrate this to us

Why this matters

Many solutions require a certain time before the models used for alerting are "tuned." Be sure to note how long this takes or if it can be reduced for a price.

Score
(0-3, with 3 being the perfect score)

0 1 2 3

Question 5

Do you migrate historical data?

Answer

Describe how you would demonstrate this to us

Why this matters

How will you use AI and anomaly-based detections if you don't have your historical data? The vendor should offer the option of migrating 6 months to 1 year of historical data as part of professional services.

Score
(0-3, with 3 being the perfect score)

0 1 2 3

Question 6

Do you offer technical support? Please describe SLAs and levels of support available.

Answer

Describe how you would demonstrate this to us

Why this matters

You want the vendor to offer their own Tech Support. Using a 3rd party for Tier 1 and 2 is acceptable, but you want to be able escalate quickly to the people who create and maintain the product.

Score
(0-3, with 3 being the perfect score)

0 1 2 3

Question 7

Do you offer training and certification?

Answer

Describe how you would demonstrate this to us

Why this matters

The vendor should be the one who creates and maintains the training material. If they don't offer formal training (and ideally a certification), they may not have the resources to enable your success.

Score
(0-3, with 3 being the perfect score)

0 1 2 3

Question 8

Does your solution use proprietary or standard query language?

Answer

Describe how you would demonstrate this to us

Why this matters

Usually, using a standard query language (like LINQ) is better than a proprietary one (like SPL) since more people will likely to know the open standard.

Score
(0-3, with 3 being the perfect score)

0 1 2 3

Question 9

Were you in the most recent Gartner MQ for SIEM, and what was your ranking?

Answer

Describe how you would demonstrate this to us

Why this matters

Gartner does a good job of assessing the maturity of the SIEM market and highlighting the differences between the different players in the space.

Score
(0-3, with 3 being the perfect score)

0 1 2 3

Category

Data Access, Data Residency, and RBAC

Question 1

Describe the granularity of role-based access controls. Can a user have the ability to query some of the data in a table but not ALL of the data? Can I restrict data to the row or field level?

Answer

Describe how you would demonstrate this to us

Why this matters

Balancing data access controls with the SOC's ability to query data is always tricky. You want a robust role-based access control that allows analysts to see as much as possible while maintaining privacy.

Score
(0-3, with 3 being the perfect score)

0 1 2 3

Question 2

Describe data residence options and how that affects search options. If data is collected in the UK, can you guarantee it stays in the UK? Is it searchable outside the UK?

Answer

Describe how you would demonstrate this to us

Why this matters

If you are a global company, you need a solution that will comply with data residency requirements across the globe. But you may or may not also need global visibility while keeping that data in each country of origin. Be clear on the requirements and if the vendor supports them.

Score
(0-3, with 3 being the perfect score)

0 1 2 3

Question 3

Do you encrypt all data in motion and all data rest? Is there an upcharge for encryption? Describe encryption used

Answer

Describe how you would demonstrate this to us

Why this matters

Your data has to be secure, both in motion and at rest. Some people charge extra for encrypting your historical data. Know your options.

Score
(0-3, with 3 being the perfect score)

0 1 2 3

Category

Data Ingestion

Question 1

Can the solution ingest any type of data, structured and unstructured?

Answer

Describe how you would demonstrate this to us

Why this matters

Lots of solutions import "standard" logs or data types. But many custom apps and APIs use custom or unstructured logs or events. You need a solution that ingests anything.

Score
(0-3, with 3 being the perfect score)

0 1 2 3

Question 2

Does data have to be parsed before it is ingested? Can you create custom parsers? Are custom parsers supported? How do you change a parser?

Answer

Describe how you would demonstrate this to us

Why this matters

If data must be parsed before it is ingested, then problems parsing data can break ingestion and lead to gaps in data and visibility. Custom apps will almost certainly require custom parsers. Since data can change as applications are updated, parsers must be flexible and self-service. You don't want to lose visibility while your vendor takes time to create or update a parser on their end.

Score
(0-3, with 3 being the perfect score)

0 1 2 3

Question 3

Does data have to be indexed before it can be searched? Does data have to be indexed before alerts are generated?

Answer

Describe how you would demonstrate this to us

Why this matters

Indexing data can take time. During peak load, indexing can be delayed as events queue up. This can create large latency gaps between when the event actually occurs and when it is visible to the SOC. You need to be aware of the length of time of that gap since it is effectively "dead time" to the SOC.

Score
(0-3, with 3 being the perfect score)

0 1 2 3

Question 4

At anticipated load, what is the average amount of time from the actual moment an event occurs and when it is searchable in the platform?

Answer

Describe how you would demonstrate this to us

Why this matters

During peak load, indexing can be delayed as events queue up. This can create large latency gaps between when the event occurs, and when it is visible to the SOC. You need to be aware of the length of time of that gap since it is effectively "dead time" to the SOC.

Score
(0-3, with 3 being the perfect score)

0 1 2 3

Question 5

Does the solution preserve the data in its raw state by default, or do I have to pay extra?

Answer

Describe how you would demonstrate this to us

Why this matters

You want a solution that keeps your data raw, in case you want to use it for anything else. If your solution alters the raw data, it is lost forever. Consider if you want to use this data for anything else - like a data lake.

Score
(0-3, with 3 being the perfect score)

0 1 2 3

Question 6

How does your solution support query optimization for large data sets?

Answer

Describe how you would demonstrate this to us

Why this matters

You need to be able to query targeted data and large data sets. Make sure your solution can handle both types of queries with performance expectations.

Score
(0-3, with 3 being the perfect score)

0 1 2 3

Question 7

Please describe the ways you can ingest data (agent, existing log shippers, collector, etc.)

Answer

Describe how you would demonstrate this to us

Why this matters

You want a solution that can ingest your data in the way that best suits your needs. Beware solutions that require a proprietary agent and don't support other open standards.

Score
(0-3, with 3 being the perfect score)

0 1 2 3

Category

Data Visualization, Analytics, and Alerting

Question 1

Do you support both out-of-the box dashboards and custom dashboards?

Answer

Describe how you would demonstrate this to us

Why this matters

You want some great out-of-the box options. But you also want the ability to create custom dashboards as well.

Score
(0-3, with 3 being the perfect score)

0 1 2 3

Question 2

Provide a list of data visualizations available natively inside the solution. Do NOT include any other visualizations.

Answer

Describe how you would demonstrate this to us

Why this matters

You want a solution that provides many different ways to visualize your data natively without exporting the data or querying the data from another separate tool and UI.

Score
(0-3, with 3 being the perfect score)

0 1 2 3

Question 3

Describe the solution's built-in ML or AI capabilities to correlate and identify outliers and advanced potential threats based on multiple log sources.

Answer

Describe how you would demonstrate this to us

Why this matters

You want a solution with native ML and AI abilities to spot anomalies.

Score
(0-3, with 3 being the perfect score)

0 1 2 3

Question 4

What are the limits to the number of logs/devices that can be searched in a single query?

Answer

Describe how you would demonstrate this to us

Why this matters

Understand the restrictions on searches, since these can limit your ability to analyze data to detect threats.

Score
(0-3, with 3 being the perfect score)

0 1 2 3

Question 5

Can the solution support custom rules to perform lookups from the last X amount of time (to compare the triggering alert to events that occurred in the past)?

Answer

Describe how you would demonstrate this to us

Why this matters

Enriching alerts with contextual data is crucial to making decisions and resolving incidents. You want a solution that can dynamically add data to alerts.

Score
(0-3, with 3 being the perfect score)

0 1 2 3

Question 6

Can the solution support customization of the alerts for adding categories, severity, tags, and context (e.g., threat scenario, known false positives that cannot be excluded, possible mitigations, etc.)?

Answer

Describe how you would demonstrate this to us

Why this matters

Customizing alerts using categories, severities, and more can be crucial to the workflow of your SOC today or in the future. So flexibility can be an optional, yet powerful, luxury.

Score
(0-3, with 3 being the perfect score)

0 1 2 3

Question 7

Does the solution support built-in and custom alert suppression to reduce alert fatigue?

Answer

Describe how you would demonstrate this to us

Why this matters

We all have too much alert fatigue - how does this solution mitigate it?

Score
(0-3, with 3 being the perfect score)

0 1 2 3

Question 8

Does the solution allow analysts to implement exclusions into alerts?

Answer

Describe how you would demonstrate this to us

Why this matters

Exclusions can drastically reduce alerts.

Score
(0-3, with 3 being the perfect score)

0 1 2 3

Question 9

Describe how your solution handles alert grouping.

Answer

Describe how you would demonstrate this to us

Why this matters

Grouping alerts can reduce alert fatigue and incidents.

Score
(0-3, with 3 being the perfect score)

0 1 2 3

Question 10

How does the solution map MITRE ATT&CK frameworks to data in visualizations?

Answer

Describe how you would demonstrate this to us

Why this matters

Mapping visualizations to the MITRE ATT&CK framework allows the business and the SOC to speak the same language.

Score
(0-3, with 3 being the perfect score)

0 1 2 3

Question 11

Does the solution natively provide MITRE ATT&CK coverage reporting and make recommendations on improving it?

Answer

Describe how you would demonstrate this to us

Why this matters

MITRE ATT&CK framework coverage reporting allows the business and the SOC to speak the same language.

Score
(0-3, with 3 being the perfect score)

0 1 2 3

Question 12

What formats can the data visualizations, reports, and dashboards be exported to?

Answer

Describe how you would demonstrate this to us

Why this matters

Understand how to get data, reports, and visualizations out of the SIEM so other parts of the business can leverage it.

Score
(0-3, with 3 being the perfect score)

0 1 2 3

Question 13

Does SIEM have native UEBA? How is it licensed and priced?

Answer

Describe how you would demonstrate this to us

Why this matters

UEBA can be a critical method for detecting threats like stolen creds. Understand if it is included and how it is priced.

Score
(0-3, with 3 being the perfect score)

0 1 2 3

Question 14

Is UEBA functionality limited to certain data sources (i.e., Microsoft AD)?

Answer

Describe how you would demonstrate this to us

Why this matters

Not all UEBA is created equal. Some UEBA models rely on a specific data source or format to function. Understand the limitations of the UEBA models.

Score
(0-3, with 3 being the perfect score)

0 1 2 3

Question 15

Please describe the configuration and setup of UEBA for your system. What are your professional services requirements?

Answer

Describe how you would demonstrate this to us

Why this matters

Since UEBA relies on AI and models, you have to understand what it takes to get data into the model, train it, and tune it.

Score
(0-3, with 3 being the perfect score)

0 1 2 3

Question 16

What risk-scoring capabilities does your UEBA provide? Is it adjustable/tunable?

Answer

Describe how you would demonstrate this to us

Why this matters

A risk score can be very useful in understanding the risk a particular event or entity poses to the business.

Score
(0-3, with 3 being the perfect score)

0 1 2 3

Question 17

Does the UEBA solution allow organizations to upload custom machine-learning models?

Answer

Describe how you would demonstrate this to us

Why this matters

Out-of-the-box models are good, but custom models can be even better when detecting sophisticated attacks.

Score
(0-3, with 3 being the perfect score)

0 1 2 3

Question 18

How does your solution support the creation of custom alerts and the configuration of chained alerts?

Answer

Describe how you would demonstrate this to us

Why this matters

Out-of-the-box alerts are good to get started. But complex alerts, particularly chained alerting, can be a powerful tool when triggering automations built to remediate specific attacks or incidents.

Score
(0-3, with 3 being the perfect score)

0 1 2 3

Question 19

Provide information for any built-in memory forensic analysis, including advanced analysis of memory dumps that help detect ephemeral threats stored in RAM.

Answer

Describe how you would demonstrate this to us

Why this matters

Many attack vectors now use ephemeral memory, and are particularly challenging to detect. A solution that includes memory dumps and other lesser-known tactics can be useful for investigating these threats.

Score
(0-3, with 3 being the perfect score)

0 1 2 3

Question 20

Provide any evidence and content repository for external artifacts, such as PCAP (Packet Capture) files and memory dumps for collaboration during investigations.

Answer

Describe how you would demonstrate this to us

Why this matters

When collaborating on incidents and investigations, it is necessary to easily share data and artifacts that allow analysts to make a decision or action. Doing this natively facilitates this collaboration and speeds incident response.

Score
(0-3, with 3 being the perfect score)

0 1 2 3

Category

Security Orchestration, Automation, and Response (SOAR)

Question 1

Describe the decision automation and machine learning capabilities of your SOAR.

Answer

Describe how you would demonstrate this to us

Why this matters

Freeing up resources from your analysts is your SOAR's main job. It should have ML capabilities and at least basic decision-making abilities. Understanding these limits will help you understand the limits of your SOAR's ability to automate tasks.

Score
(0-3, with 3 being the perfect score)

0 1 2 3

Question 2

Describe how your SOAR can reduce false positives.

Answer

Describe how you would demonstrate this to us

Why this matters

Cutting down on false positives and reducing investigations should be the bread and butter of your SOAR. Understand how it does this.

Score
(0-3, with 3 being the perfect score)

0 1 2 3

Question 3

How does your solution support the development of low/no code automation?

Answer

Describe how you would demonstrate this to us

Why this matters

Having a graphical UI that doesn't require advanced programming skills can really eliminate the barrier to entry for a lot of analysts. Having a low code/ no code UI means more analysts can automate more tasks, boosting the efficiency of every analyst.

Score
(0-3, with 3 being the perfect score)

0 1 2 3

Question 4

What is included in your SOAR implementation?

Answer

Describe how you would demonstrate this to us

Why this matters

You need to understand how much things like playbooks and integrations are going to be ready out of the box, and how much is going to need to be built from scratch.

Score
(0-3, with 3 being the perfect score)

0 1 2 3

Question 5

How is the SOAR/automations priced? Per user, per CPU, please provide examples.

Answer

Describe how you would demonstrate this to us

Why this matters

SOAR can be priced several ways, by number of playbooks, number of users, CPU, etc. Pricing should be simple and easy to predict.

Score
(0-3, with 3 being the perfect score)

0 1 2 3

Question 6

What is the pricing schema for the onboarding and setup of new integrations?

Answer

Describe how you would demonstrate this to us

Why this matters

SOAR can be priced several ways, by number of playbooks, number of users, CPU, etc. Pricing should be simple and easy to predict

Score
(0-3, with 3 being the perfect score)

0 1 2 3

Category

Threat Detection & Incident Response

Question 1

How does the solution automatically investigate events?

Answer

Describe how you would demonstrate this to us

Why this matters

A next-gen SIEM should have some automatic investigation capabilities built in. You need to understand the extent of these capabilities, what types of things are investigated automatically, and what triggers it.

Score
(0-3, with 3 being the perfect score)

0 1 2 3

Question 2

How does the solution automatically create a timeline of events?

Answer

Describe how you would demonstrate this to us

Why this matters

A timeline of events is critical when understanding how an attack unfolds over time.

Score
(0-3, with 3 being the perfect score)

0 1 2 3

Question 3

How does the solution automatically investigate event information surrounding an alert?

Answer

Describe how you would demonstrate this to us

Why this matters

The solution should provide context around an alert or event so that the analyst can take appropriate action or at least understand the next step.

Score
(0-3, with 3 being the perfect score)

0 1 2 3

Question 4

How does your solution include hunting for threats (including zero-day threats) within our environment?

Answer

Describe how you would demonstrate this to us

Why this matters

Alerts can only detect known threats. You need a solution that is equally effective at hunting and finding unknown and emerging threats. Understand what the solution brings to the table in this area.

Score
(0-3, with 3 being the perfect score)

0 1 2 3

Question 5

Is there any special software we need to deploy to support this hunting?

Answer

Describe how you would demonstrate this to us

Why this matters

If threat hunting requires 3rd party software or solutions, be aware of everything you need and what the process is for using the entire stack.

Score
(0-3, with 3 being the perfect score)

0 1 2 3

Question 6

Does your hunting methodology map to any security frameworks e.g. MITRE? Please explain.

Answer

Describe how you would demonstrate this to us

Why this matters

Mapping your threat hunting to a framework like MITRE ATT&CK can help you SOC analysts better understand the tactics and techniques of specific types of attacks.

Score
(0-3, with 3 being the perfect score)

0 1 2 3

Total Score _____