RKON | RKON Offering

WHY SO MANY SIEM IMPLEMENTATIONS FAIL—AND HOW TO ENSURE YOUR SUCCESS

By Ronald Palermo
Managing Director and CISO

Unlike more tangible technologies where a failed implementation causes a down network, SIEM (security information and event management) requires a more qualitative approach to determining success or failure. The surprising reality is that most SIEM projects completely fail to deliver any discernable benefits to the organization and are abandoned in frustration. Here are the most common reasons why:

1. Trying to use SIEM to solve all security challenges in an enterprise from day one:

SIEM should be used to alert non-conformity with the security policy. However, the first thing that's often discovered when SIEM is implemented is the complexity of how the network actually operates and how many overlapping systems and conflicts are involved. This typically creates such an abundance of alerts that the projects are either abandoned or the output is ignored. SIEM is a tool to assist organizations in continual process improvement. SIEM implementation is NOT a destination—it's a reasonable starting point and an increasingly complex deployment as an organization's security needs evolve over time. Realistically, you're looking at a 1 to 3-year window, minimum, as your organization moves from a basic "compliance" posture to encompass more-complex "security watchdog" capabilities.

2. Underestimating the technical challenges involved with SIEM technology:

It's essentially an interpreter—taking output from disparate systems and converting it into a common language that can be understood before correlation can take place. There's a significant technical component to these projects that organizations often overlook—they simply assume SIEM will work easily and automatically "right out of the box."

3. Not understanding that maturation of deployment requires cooperation across all areas of the organization:

For SIEM to work correctly and efficiently, everyone needs to work together to accommodate its operation. All of the following factors must be addressed:

a. Application development
b. Patch management and change control in all departments
c. Access control in all departments
d. Server and authentication team
e. Security infrastructure team

f. Network team
g. Storage team
h. Audit and compliance
i. Necessary changes in organizational IT roles and responsibilities

4. Not putting sufficient time commitment into ongoing maintenance of the system:

Every time a system is patched or modified, there's a good chance that the SIEM will either stop working or require "reintegration." The SIEM team must be fully integrated into the organization's operational workflow and change control—and should have influence over the architecture and design. This helps to ensure that the systems are designed and implemented to standard and executed in a way that allows the SIEM solution to measure and report on them.

5. Not having a mature IT operation:

Besides cooperation, just delivering a rudimentary report may require an organization to:

a. Reorganize IT completely.
b. Create a functional CISO role that has independent reporting structure from IT.
c. Change the internal culture so that it can operate less as a hierarchy (vertically) and more from a process standpoint (horizontally). The rubber meets the road the first time a lower-ranking person in one department has to ask a higher-ranking person in another to make a change so that workflow and process can flow across the organization.
d. Eliminate power-hungry leadership—individuals who believe they should have complete say in their department.
e. Develop mature roles and responsibilities (RASCI Model) along with separation of duties.

6. Thinking SIEM is just something you "install" and get working:

Fact is, the biggest benefit of implementing SIEM is that it will show you how to mature your organization and your security across all areas—people, processes and technology. True security can't be achieved until you have a well-run, well-defined organization where the technology works, the processes are well defined and followed, and the personnel put the organization's needs ahead of theirs.

IT'S BEST TO FOLLOW A STEP-BY-STEP PROCESS.

1. Start with a small device sample:

Separate technical challenges from policy and enforcement issues. This means starting with a representative subset of the technical environment.

2. Establish a basic security policy:

How well the security policy can be enforced must be "discovered" first before a comprehensive policy can be enforced. Choosing basic fundamental policies as a starting point is the key to success in the first phase.

3. Focus on operational functionality as the first phase goal:

Resolving inevitable gaps in the security policy and the way the organization is operating often turn out to be bigger tasks than organizations expect. Advanced SIEM functionality such as NABD shouldn't be implemented until base security policy, technical implementation and the supporting incident management procedures are mature. Expect that significant technical, procedural and organizational structural changes will be required just to achieve high

value, low noise and operational efficiency in the base deployment. It's important to keep in mind that one of the key features of a SIEM is the time it saves in reviewing technology logs. If complexity and operational time increases exponentially as a result of the implementation, then the ROI and value to the organization has probably been lost altogether.

THE KEY TO SUCCESS IS A PHASED APPROACH.

It's best to execute a finite subset of SIEM deployment goals where value is delivered back to the organization early in the process—and then add complexity as you go along. The methodology below will ensure early tangible results and a maturity model gridline for long-term success.

Discovery Phase

1. Review the organizational security posture and the initial business case for SIEM. Then prioritize the goals of the SIEM implementation from the most critical to the optional—taking into consideration the tasks that must be performed in order to support the effort.
2. Review in detail the organizational security policy to consider the intent behind it. Separate those policies from a priority standpoint. Determine what's critical, what's necessary for mandatory compliance and which policies are related to best practices for a secure environment.
3. Identify current controls that are auditing those policies to determine compliance level. Ideally, SIEM implementation shouldn't be the first time the organization identifies that its security policy or how it's implemented isn't working according to plan. The reality is that these deployments often expose gaps in security execution that must be remediated before those elements can be integrated into a daily alerting and reporting structure.
4. Identify a smaller representative subset of the current policy and devices where SIEM can be applied and enough data can be gathered to determine what changes need to occur.

Pilot and Controlled Deployment Phase

The primary goal of this phase is to determine which specific SIEM project goals can be implemented in order to establish initial ROI while creating a baseline operational model and run-book.

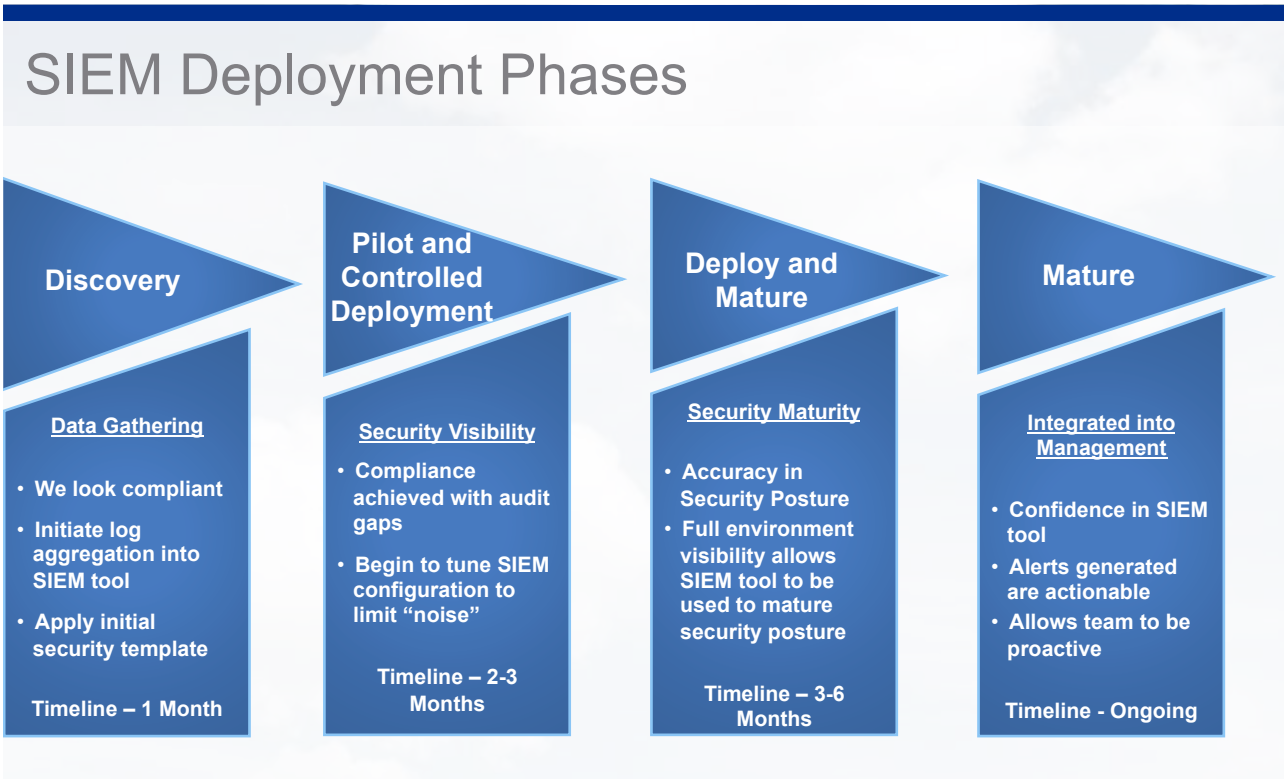
1. The lessons learned from the discovery phase are used to implement a larger subset of technology.
2. The assumptions developed during the discovery phase are tested in real time.
3. The list of devices should be expanded to incorporate a wider set of technologies and numbers.
4. The information developed from this phase is used to determine the final steps of controlled deployment and maturity phase.

Deployment Phase

The primary goal of this phase is to develop a deployment workflow that allows the organization to build capacity as full deployment approaches. This phase also serves as the initial production test run and the completion of operational run-books necessary to manage a full deployment.

Maturity Phase

Based on our experience, significant work must be performed in order to mature the organization's security posture to implement the finer points of the deployment. This phase never has an end point—since SIEM must continually evolve.



PARTNER WITH RKON FOR SIEM DEPLOYMENT.

RKON has developed a successful model for SIEM deployment that's focused on real-world scenarios, based on our firsthand experience with SIEM implementations for a broad range of clients—and our deep understanding of technology as it applies to security.

We have significant experience working with auditors to help them understand that something can issue an alert without being "out of compliance" with the intent of the policy. No organization can eliminate automated tools from delivering false positives. The key is to proactively address how those events are acted upon and interpreted by third parties that do not have the inherent technical knowledge to differentiate between an automated response that a tool delivers and an actual break of a policy.

RKON offers:

Technology Design Knowledge: As a technology integrator, RKON has a deep understanding of the way design and configuration can impact SIEM implementation.

Technology Configuration Knowledge: RKON holds significant certifications across all areas of the network and can help advise clients on solving security challenges and SIEM/tool integration.

Operational Efficiency: Understanding that the ultimate goal of SIEM tools is to create operational efficiency and guides, RKON steers clients through realistic deployments and creates value immediately while maturing the deployment over time with an efficient "low-noise methodology."