Implementing a SIEM Solution for Lee Koonce Corral, LCC

Joshua M. Lee

# Western Governors University

Table of Contents

[Western Governors University 1](#_Toc196747671)

[Table of Contents 2](#_Toc196747672)

[A. Proposal Overview 3](#_Toc196747673)

[A.1 Problem Summary 3](#_Toc196747674)

[A.2 IT Solution 3](#_Toc196747675)

[A.3 Implementation Plan 4](#_Toc196747676)

[A.3.a Justification of Plan 6](#_Toc196747677)

[B. Review of Other Work and (B1) Works Informing Design 7](#_Toc196747678)

[C. Project Rationale 10](#_Toc196747679)

[D. Current Project Environment 10](#_Toc196747680)

[E. Methodology 11](#_Toc196747681)

[F. Project Goals, Objectives, and Deliverables 12](#_Toc196747682)

[F1. Goals, Objectives, and Deliverables Table 12](#_Toc196747683)

[F2. Goals, Objectives, and Deliverables Descriptions 14](#_Toc196747684)

[G. Project Timeline with Milestones 17](#_Toc196747685)

[H. Outcome 18](#_Toc196747686)

[References 19](#_Toc196747687)

# A. Proposal Overview

## A.1 Problem Summary

Lee Koonce Corral, LLC is a company in Idaho that provides pet corral services. They provide luxury boarding experiences and along with field trips for pets who need extended boarding while their owners are away. They also have a massive facility for animal rescue that is not limited to just dogs and cats, but all types of pets and injured wildlife. Their culture is never to turn anyone or any animal in need of assistance away and to always be of service. Lee Koonce Corral, LLC recently added all their reservations, pet boarding, rescue databasing, web server, and merchandise portal digitally to their network. These technological additions to their services are relatively new and they are just getting the hang of them. The company recently had a meteoric rise in popularity due to several viral reviews of their services, which has also come with increased exposure. Due to this exposure, the company has seen a steady increase in cyberattacks. Employees are receiving frequent phishing emails, which are leading to unauthorized access attempts and data breaches. Malware has been infiltrating the company through many avenues and infecting systems. These issues are causing lapses in business, which are resulting in backup or turn away of customers or rescues. Currently, Lee Koonce Corral, LLC has two IT Security members on the team who are having difficulty keeping up with these events. They have adapted to the new technological setup, but the various sources they need to look at for data related to these events are scattered across different systems (i.e., firewalls, servers, network devices, etc.), each with its own dashboard. By the time it takes to get the data from these various sources and find the relationships between the data, the events have already created a significant negative impact on the company and create serious risks and disruptions. The amount of data alone is too much for the two-person IT Security team to handle effectively.

## A.2 IT Solution

Since the IT Security team at Koonce Lee Corral, LLC has adjusted well to the new technological setup but are having issues with how long it takes to track down and respond to these security events, we at Default Security want to help introduce a solution called a Security Information and Event Management (SIEM) system into their network. “A SIEM is a security solution that helps organizations recognize and address potential security threats and vulnerabilities before they have a chance to disrupt business operations” (*What Is SIEM?*, 2023).

SIEMs help bring all the security information from different systems into one place, so that the IT Security team does not have to interact with various dashboards or systems whenever there is an issue, losing precious time and having security threats go on longer than necessary. Instead of the previous scenario of sorting through data from the various sources manually, a SIEM can help companies automatically collect, organize, and filter security data related to what is essential for the relevant issues. There can also be rules set up to filter out logs that are not needed to make it easier on the team. This would help the two-person IT Security team identify issues faster and respond to events quicker, saving time and reducing the chances of severe damage to the company.   
 By having all the relevant information on one dashboard instead of many, the two-person IT Security team will be better equipped to handle these security events as they occur. This will reduce the overwhelming instances of manually going through large amounts of data and jumping between different systems. After implementing this solution, the IT Security team can constantly keep turning the SIEM to combat not only the threats they are facing in the present but also ones that can affect Lee Koonce Corral, LLC in the future.

## A.3 Implementation Plan

We are following an Agile methodology, which will break the project up into individual mini projects and will be using ISACA's framework of SIEM implementation for the SIEM implementation into Lee Koonce Corral, LLC. “ISACA is a global professional organization and learning organization with 185,000 members who work in digital trust fields such as information security, governance, assurance, risk, privacy and quality. With presence in 188 countries and with 225 chapters worldwide, ISCA is recognized around the world for its guidance, credentials, education, training and community” (*About ISACA | A Global Business & Technology Community*, n.d.).

First, Lee Koonce Corral, LLC to identify regulatory and business requirements concerning their location in Idaho and the US. They would be able to know their industry, consumers, and regulatory obligations and Default Security will help with consultation on this to assist in this step. This will allow us to see what is available and what solutions the company will be limited to. Also, during this time, we will work with Lee Koonce Corral, LLC, to define the SIEM deployment approach. This would mean conducting a risk analysis of relevant issues to the company, partnered with a cost-benefit analysis to see what systems need to be monitored and what would be financially feasible for them to run.

Next, Lee Koonce Corral, LLC would identify the range of the systems they want to be handled by the SIEM. This will help them understand what needs to be included and what does not need to be included in the data collection. Once they develop the scope, we at Default Security will work with them to help validate and refine it to fit their needs.

We will then work with Lee Koonce Corral, LLC, using the information they have gathered regarding critical operations, business needs, and compliance needs to define use cases, which are scenarios that could apply to SIEM monitoring and detection. This would help map these cases to the SIEM capabilities for threat detection and tracking of these security issues and see if any additional definitions need to be added. Next, Lee Koonce Corral, LLC will provide Default Security with infrastructure details, and we will assist in confirming that they support the defined cases and if more cases need to be added.

After accumulating the information from all the previous steps, Default Security will select recommendations for SIEMs that fit Lee Koonce Corral, LLC’s needs. They will choose which fits their risk profile and cost requirements best, and we will implement the SIEM into their infrastructure.

Lee Koonce Corral, LLC will determine if the SIEM captures the appropriate amount of security data to support the use cases. If not, Default Security will adjust it to the proper level to detect security events. Default Security will also ensure that all the required data and events are sent to the SIEM and correctly analyzed during this time.

After validating the data, Default Security would configure rules and conditions to trigger alerts based on the scenarios provided by Lee Koonce Corral, LLC. This will help them stay on top of things when security events occur. When the alerts are configured, Default Security will configure the dashboards and reports to the specifications provided by Lee Koonce Corral, LLC.

When the full implementation has been completed, the IT Security team will receive training on using the SIEM and will be given documentation to assist with its use. This will also include policies and procedures created by Default Security to guide the IT Security team in properly using the SIEM independently. Lee Koonce Corral, LLC will handle the final part of the implementation, which will happen over the long term. After the handoff, the IT Security team will constantly tune its SIEM to adapt to the evolving security events that are affecting its company. This is the most crucial part, as the continuous effort put into the tuning will assist in protecting them from future security events and threats.

## A.3.a Justification of Plan

The implementation plan is appropriate for Lee Koonce Corral, LLC, as it is in-depth to find the right solution for their company and small IT Security team. The team can adjust to the SIEM implementation process by going through phases without being overwhelmed. It allows Lee Koonce Corral, LLC to identify its current and future risks and work with Default Security to use best practices to find the correct SIEM solution for them. It involves them in the process so they know what is going on every step of the way and can understand why the SIEM solution recommended is an appropriate fit for the company. The implementation plan involves proper training for the IT Security team so they are fully prepared to use the SIEM efficiently after the implementation. In using the SIEM over time, the IT Security team can continuously tune and refine it to meet the needs of Lee Koonce Corral, LLC, as they change, which will keep them protected from future cyber threats.

Adding a SIEM to Lee Koonce Corral, LLC’s infrastructure is justified because it addresses the challenges they are facing: overwhelming setup when gathering data, difficulty in monitoring the multiple systems, and the slow response time to the security events occurring. The SIEM compiles all relevant security data in one dashboard, removing the problem of monitoring multiple systems. It automates the process of relating the various security data sources to help detect suspicious activity faster than was possible when manually performing the process. SIEMs are made to work with existing infrastructures like firewalls, servers, and network devices. Working with us at Default Systems, we will help find the most cost-effective and adaptable SIEM solution to help with the IT Security team's reaction time and visibility during security events. This solution will keep evolving with threats as long as the IT Security team maintains it. This shows immediate and continuous value to Lee Koonce Corral, LLC, as long as it is maintained.

# B. Review of Other Work and (B1) Works Informing Design

**Review of Other Work 1 (*****2023 Volume 3 A Framework for SIEM Implementation*, n.d.)**

This work on ISACA’s website explains why implementing a SIEM is vital to realizing its value to an organization. It elaborates that the cyber threat landscape is an evolving environment, and even if an organization has a plan and the right tools at that moment, something could change, so they need to adapt to get ahead of the curve. Within this work, it states that a SIEM can “provide valuable insights for security teams and enable more efficient and effective incident response activities”, but realizing its potential requires correct implementation and proper logging (*2023 Volume 3 A Framework for SIEM Implementation*, n.d.).

*2023 Volume 3 A Framework for SIEM Implementation* also provides a framework to provide an implementation procedure that will give the most value from using a SIEM. It provides steps for an organization to gather information on its infrastructure and business to determine what is needed in a SIEM and use that information to make the best-informed decision on which SIEM would fit the best. Then, it gives further information on how to implement, configure, and maintain a SIEM to be proper for the security solution now, but one that can be used for the future landscape of security as time passes.

This work relates to this project not only by being the framework on which this SIEM implementation is based, but also as a reason why this phased approach will provide the best value for Lee Koonce Corral, LLC in the long run for their company’s infrastructure. It shows the meaning behind each step in the implementation and why it is essential. This will give Lee Koonce Corral, LLC the confidence in a proper solution and the tools to keep adapting it to their needs for the future of their business.

**Review of Other Work 2 (*SIEM for Small Business*, n.d.)**

The *SIEM for Small Business* article from SentinelOne gives context on how cyberattacks are prevalent amongst large businesses and businesses of all sizes. It explains why small businesses should use a SIEM solution and how it would benefit them in many ways. From improved incident response to making it easier for companies to comply with regulatory and industry standards to an emphasis on removing the burden of manual analysis, this article explains why implementing a SIEM benefits small businesses and how to choose the right one.

This article relates to this project by showing the benefit of implementing a SIEM into smaller businesses like Lee Koonce Corral, LLC. It conveys why the implementation is justified for small companies and reinforces the importance of the features outlined in the framework. *SIEM for Small Business* also supports the proposed process for assessing needs and requirements to determine the best SIEM solution.

**Review of Other Work 3 (“SIEM Implementation: Strategies and Best Practices,” n.d.)**

This work provides strategies and best practices to follow during the whole implementation process of a SIEM. It gives context on what to consider when selecting a SIEM and the best practices to follow during the implementation process. *“SIEM Implementation: Strategies and Best Practices”* also provides strategies on post-implementation and the importance of constant optimization for successful results.

*“SIEM Implementation: Strategies and Best Practices”* relates to this project by reinforcing the same process that the project is being proposed for Lee Koonce Corral, LLC to follow. It validates the importance of the preparation portion of the project to understand the goals and objectives that will drive what benefits are needed in a SIEM. It also reinforces the importance not only of evaluating their current infrastructure concerning implementing a SIEM, but also why it is essential to think of future growth and the evolving cybersecurity landscape.

**Review of Other Work 4 (C, n.d.)**

This work by Bradley C provides information on why continuous improvement and tuning of a SIEM are essential. It also outlines the significant steps in how to optimize a SIEM. The steps provided provide information on how to optimize a SIEM, the logic behind why these steps are essential, and how they benefit a company through continuous improvement.

This work relates to the project by reinforcing the importance of continuous improvement, which Lee Koonce Corral, LLC will field after the handoff. It also shows the importance of previous steps before handoff, like ensuring the alerts are triggered correctly or having the correct rules and conditions to trigger those alerts. This validates why this is the most crucial part of the project and that performing continuous improvement will keep Lee Koonce Corral, LLC ahead of the curve regarding cyber threats.

# C. Project Rationale

This project of implementing a SIEM will benefit Lee Koonce Corral, LLC in many ways. The main reason is that this will allow the client to quickly and accurately adapt to the rise and quantity of new security events with their two-person Security IT team. The IT Security team has been overwhelmed by gathering data from many sources, taking the time to analyze the data, seeing how the data is related, and doing this manually from each source, all within a newly set-up technological infrastructure. The SIEM will allow automation and analysis of the events to enable the two-person IT Security team to handle events that come their way efficiently and accurately. Security events that previously took days or weeks to fix can be managed in hours. The benefit of Lee Koonce Corral, LLC being involved in the implementation project phases will ensure that their input and needs are applied to the SIEM solution, providing maximum benefit for their company and one that aligns with their business culture. Also, with their IT Security team receiving training on how to use and tune the SIEM proficiently, it will ensure that Lee Koonce Corral, LLC protects itself from the current threats plaguing their company and future threats that can occur.

The project can be completed successfully because this type of situation is why SIEMs were created in the first place and why there are so many different SIEM solutions to pick from. The types of SIEMs range from ones that support large organizations to ones that support smaller, evolving companies like Lee Koonce Corral, LLC. SIEMs were also made to be inserted into existing infrastructures, help with overwhelming amounts of data from various sources, and expedite incident response time. With Default Security’s expertise and input from Lee Koonce Corral, LLC about their environment and needs, the project will have enough to be successful and to remedy the current and future issues that Lee Koonce Corral, LLC is facing.

# D. Current Project Environment

Adding the SIEM solution to Lee Koonce Corral, LLC’s infrastructure will positively affect their goals of incident response time, reducing downtime for services, ease of use between multiple systems, and the ability to combat future threats. By adapting this solution, all the necessary data will be stored and analyzed in one place, removing the need for complicated manual collection and analysis. Automating collection and analysis will decrease the response time of combating security events, resolving them faster, and reducing the amount of downtime for issues, if any. Allowing the IT Security team the ability to tune the SIEM constantly will enable them to be one step ahead of the evolving landscape of cyber threats.

This solution aligns with their culture of always being of service and never turning any animal or person down by creating an environment where security events get handled expediently, reducing downtime. By having a solution that can reduce the time an issue gets resolved or even prevented, Lee Koonce Corral, LLC can ensure that any assistance is always available. This will align Lee Koonce Corral, LLC’s values and beliefs in never turning any person or animal away in need of assistance.

# E. Methodology

For this project, we would follow the Agile methodology. This will provide an iterative and collaborative approach to designing and implementing a SIEM. This methodology will help create a strong, efficient system that can evolve to the changing needs of cybersecurity. These are structured into sprints to make the project manageable, allow for adaptation if things change, and provide a high-quality SIEM implementation into Lee Koonce Corral, LLC’s infrastructure.

In the first sprint, we would focus on the initial planning of the SIEM implementation. This would focus on identifying regulatory and business requirements that affect what SIEMs are applicable for use in Idaho and the US. This section will also define the SIEM deployment approach by conducting risk and cost-benefit analyses. The second sprint will determine the scope of what needs to be covered. This will contain the steps of identifying the scope of systems that need to be monitored by the SIEM, allowing us to grasp which SIEMs would support the types of systems in the infrastructure. With the third sprint, we will create scenarios as use cases and confirm that the defined infrastructure will support those use cases. If use cases could be added to increase the effectiveness of what could be detected, those will be added. For the fourth sprint, we provided recommendations to Lee Koonce Corral, LLC for SIEMs. We will commence implementation once they select and approve which SIEM they want added to their infrastructure.

After the implementation, validation will ensure that data capturing is sufficient, excessive, or lacking in the fifth sprint. Adjustments will be made to bring the level of capturing to a desired level. Validations will be made so that all data is sent through the SIEM correctly and analyzed correctly. In the sixth sprint, Default Systems will configure the rules and conditions that will trigger the SIEM alerts and ensure they occur correctly when needed. Also, during this time, Default Systems will configure the SIEM dashboards and their reports to the specifications of Lee Koonce Corral, LLC. The seventh and final sprint will be the training for the IT Security team, which will be conducted to get them proficient with using the SIEM and to provide them with documentation, policies, and procedures provided by Default Security and the SIEM vendor. After this, the SIEM implementation will be completed, and the IT Security team at Lee Koonce Corral, LLC will continuously improve and tune it to keep up with the needs of the company and the evolving cybersecurity landscape.

# F. Project Goals, Objectives, and Deliverables

## F1. Goals, Objectives, and Deliverables Table

|  |  |  |
| --- | --- | --- |
| **Goals** | **Supporting Objectives** | **Deliverables Enabling the Project Objectives** |
| 1. Implementing a SIEM to help monitor and manage security events | 1.a. Identify regulatory and business requirements | 1.a.i. Identify regulatory and business requirements/limitations for the state of Idaho |
| 1.a.ii. Identify regulatory and business requirements/limitations for US |
| 1.b. Define SIEM deployment approach | 1.b.i. Conduct risk analysis |
| 1.b.ii. Conduct a cost-benefit analysis |
| 1.c. Identify the scope of systems SIEM will monitor | 1.c.i. Verify what systems need to be included in SIEM monitoring |
| 1.c.ii Validate the scope of systems to be monitored |
| 1.c.iii. Make suggestions on what needs to be added or removed |
| 1.d. Define use cases | 1.d.i. Gather information on critical operations, business needs, and compliance needs |
| 1.d.ii. Develop specific scenarios for the SIEM to detect, alert, and respond based on those needs |
| 1.e. Confirm infrastructure details support the use cases | 1.e.i. Get information relating to Lee Koonce Corral, LLC’s infrastructure setup |
| 1.e.ii. Confirm if use cases support the infrastructure |
| 1.e.iii. Add use cases that are missing |
| 1.f. Select and implement SIEM solution | 1.f.i. Provide Lee Koonce Corral, LLC SIEM recommendations |
| 1.f.ii. Implement the selected SIEM into the infrastructure |
| 1.g. Validate the capturing of security data | 1.g.i Verify that the amount of data being captured is sufficient, lacking, or excessive |
| 1.g.ii. Adjust the capture level accordingly if changes need to be made |
| 1.g.iii. Ensure all required data and events are being sent to SIEM |
| 1.g.iv. Ensure all data is being correctly analyzed |
| 1.h. Configure rules and conditions | 1.h.i. Configure rules and conditions to trigger alerts based on given scenarios |
| 1.h.ii. Ensure alerts are correctly occurring after being configured |
| 1.i. Configure SIEM dashboard and reports | 1.i.i. Configure the dashboard to Lee Koonce Corral, LLC’s requirements |
| 1.i.ii. Configure reports to Lee Koonce Corral, LLC’s requirements |
| 1.j. Continuous improvement | 1.j.i Lee Koonce Corral, LLC will tune the SIEM consistently to adapt to the security needs of the company |
| 2. Conduct training for the IT Security team on the operation of the SIEM | 2.a. Train IT Security team on how to use the SIEM | 2.a.i. Teach the team how to operate the SIEM |
| 3.b. Provide documentation from SIEM vendor for operation | 2.b.i. Provide documentation from SIEM vendor for assistance in operation |
| 2.b.ii. Create policies and procedures for the IT Security team to follow while using the SIEM |

## F2. Goals, Objectives, and Deliverables Descriptions

1. Default Security will work with Lee Koonce Corral, LLC in implementing a SIEM to help monitor and manage security events concerning the increase in issues occurring due to their rise in popularity.
   1. Lee Koonce Corral, LLC will identify regulatory and business requirements concerning its business location and clientele. This supports the goal by making sure that the proper selection of a SIEM is made.
      1. Lee Koonce Corral, LCC will identify regulatory and business requirements and limitations for Idaho, which will dictate the selection of available SIEM providers. This supports the objective by ensuring what can and cannot be used as a SIEM for the company.
      2. Lee Koonce Corral, LLC will identify regulatory and business requirements and limitations for the US, which will dictate the selection of SIEM providers available. This supports the objective by ensuring what can and cannot be used as a SIEM for the company.
   2. Default Security will work alongside Lee Koonce Corral, LLC to define a SIEM deployment approach that would be appropriate for their infrastructure. This supports the goal by defining which SIEMS will work for Lee Koonce Corral, LLC’s company profile.
      1. Lee Koonce Corral, LLC will conduct a risk analysis and will work with Default Security using that information to decide on their deployment approach. This supports the objective by showing which SIEMs can manage the type of risks inherent to Lee Koonce Corral, LLC’s infrastructure.
      2. Lee Koonce Corral, LLC will conduct a cost-benefit analysis and will work with Default Security using that information to decide on their deployment approach. This supports the objective by establishing how much Lee Koonce Corral, LLC wants to spend while also maximizing the benefits of what the SIEM will do for the company.
   3. Lee Koonce Corral, LLC will identify the scope of systems and their dependencies from which the SIEM will monitor and collect data. This supports the goal by allowing us to see which SIEMs can support the systems that Lee Koonce Corral, LLC would want to be monitored.
      1. Lee Koonce Corral, LLC will verify what systems need to be included in SIEM monitoring and which ones do not need to be added to the SIEM. They will also include any dependent components that are part of each system. This supports the objective by confirming the systems that the SIEM will monitor.
      2. Default Security systems will help validate the scope of systems to be monitored to reinforce the decision. This supports the objective by reinforcing that these systems must be included and will help decide which SIEMs will be appropriate.
      3. Default Security will suggest to Lee Koonce Corral, LLC what systems might need to be added or removed, and the company will either go forward or reject those suggestions. This supports the objective by giving Lee Koonce Corral, LLC another view on what should or should not be part of the scope and affect the decision-making process on which SIEMs will be appropriate.
   4. Default Security will work with Lee Koonce Corral, LLC to help define use cases that assist in mapping them to SIEM capabilities used for threat detection and monitoring security issues. This supports the goal by creating scenarios that will affect which types of SIEM would fit Lee Koonce Corral, LLC’s needs
      1. Lee Koonce Corral, LLC will gather information on critical operations, business needs, and compliance needs to help define use cases using those needs. This supports the objective by giving information to determine what use cases would fit those needs.
      2. Default Security will work with Lee Koonce Corral, LLC to develop specific scenarios for the SIEM to detect, alert, and respond to those needs. This supports the objective by creating the actual use cases to help select the appropriate SIEM.
   5. Default Security will confirm infrastructure details provided by Lee Koonce Corral, LLC that support the use cases needed to be mapped to the SIEM. This supports the goal by applying the layout of systems to the use cases and narrowing down the choices of which SIEM would be appropriate for Lee Koonce Corral, LLC.
      1. Default Security will receive information about Lee Koonce Corral, LLC’s infrastructure setup to assist with what needs to be mapped to the SIEM. This supports the objective by confirming which systems need to be supported by the SIEM and use cases.
      2. Default Security will confirm if use cases support the actual devices that provide logs for each system in the infrastructure. This supports the objective by ensuring that the use cases created within or provided by a SIEM would work for Lee Koonce Corral, LLC’s infrastructure.
      3. Default Security will work with Lee Koonce Corral, LLC, to add additional use cases if they validate that some should be added for more comprehensive information in selecting a SIEM. This supports the objective by being thorough on what scenarios need to be provided by the selected SIEM.
   6. Lee Koonce Corral, LLC will select a SIEM recommendation and Default Security will implement the SIEM into their infrastructure. This supports the goal by choosing the right SIEM solution for Lee Koonce Corral, LLC’s infrastructure.
      1. Default Security will provide Lee Koonce Corral, LLC SIEM recommendations. Lee Koonce Corral, LLC will select one that fits their company and supports their risk and cost-benefit analyses. This supports the objective by using all the information in the previous objectives to help Lee Koonce Corral, LLC to make an informed decision on the SIEM that would be appropriate for their company.
      2. Default Security will implement the selected SIEM into Lee Koonce Corral, LLC’s infrastructure. This supports the objective by providing the solution to monitoring security events for Lee Koonce Corral, LLC’s infrastructure.
   7. Lee Koonce Corral LLC and Default Security will validate capturing security data to ensure the SIEM works to the capacity needed. This supports the goal by confirming that the data is in tune with the security events Lee Koonce Corral, LLC is experiencing and may experience in the future.
      1. The IT Security team from Lee Koonce Corral, LLC will verify that the captured data is sufficient, lacking, or excessive for properly associating data for security events. This supports the objective by collecting the correct data for security event detection and monitoring.
      2. Default Security will adjust to the proper level of capturing data if changes need to be made. This supports the objective by being thorough on what data must be collected to assist with security event detection and monitoring.
      3. Default Security will ensure all required data and events are sent to the SIEM. This supports the objective by confirming that the correct data is used for security event detection and monitoring.
      4. Default Security will ensure all data is being correctly analyzed to ensure it is following the use cases to find security events that will occur. This supports the objective by confirming that the data analysis works for what Lee Koonce Corral, LLC’s security event detection and monitoring needs.
   8. Default Security will configure rules and conditions on the SIEM. This supports the goal by ensuring the SIEM will properly notify Lee Koonce Corral, LLC of any security events occurring.
      1. Default Security will configure rules and conditions to trigger alerts based on scenarios so that Lee Koonce Corral, LLC can be notified and expediently handle security events as they occur. This supports the objective by creating the rules for proper security event detection.
      2. Default Security will ensure alerts are correctly occurring after configuring to ensure that Lee Koonce Corral, LLC will be notified when a security event occurs. This supports the objective by validating that the rules and conditions are working to ensure that the IT Security team can respond to security events promptly.
   9. Default Security will configure SIEM dashboard and reports for Lee Koonce Corral, LLC. This supports the goal by ensuring that Lee Koonce Corral, LLC can properly navigate its SIEM and information in response to security event monitoring, detection, or response.
      1. Default Security will configure the dashboard to Lee Koonce Corral, LLC’s requirements to match what is needed to monitor the SIEM successfully on their own. This supports the objective by adapting the dashboard to Lee Koonce Corral, LLC’s specifications and ensuring the IT Security team can use it properly and effectively.
      2. Default Security will configure reports to Lee Koonce Corral, LLC’s requirements, so that they will have sufficient information to determine whether security events are occurring or not, as well as information for their infrastructure as a whole being portrayed. This supports the objective by ensuring that all the reports needed by Lee Koonce Corral, LLC are available whenever possible and can aid in responding to security event monitoring, detection, or response.
   10. Lee Koonce Corral, LLC will continuously improve the SIEM to ensure that it sufficiently matches the company's needs. This supports the goal by allowing the solution to always be relevant and helpful in security event detection, monitoring, and response.
       1. Lee Koonce Corral, LLC will tune the SIEM constantly to adapt to the company's security needs and the evolving trends of cyberattacks. This supports the objective by keeping the infrastructure safe and meeting the company's needs.
2. Default Security will train the IT Security team at Lee Koonce Corral, LLC on the operation of the SIEM, ensuring they can appropriately manage and interpret the SIEM's information.
   1. Default Security will train the IT Security team at Lee Koonce Corral, LLC on correctly using the SIEM and interpreting its information. This supports the goal by giving the IT Security team the proper tools to manage and maintain the SIEM.
      1. Default Security will teach the team how to operate the SIEM, so that they can use and interpret information from the SIEM correctly. This supports the objective by ensuring that the IT Security team can manage the SIEM independently.
   2. Default Security and the SIEM vendor will provide documentation to assist with SIEM operation. This supports the goal by allowing the IT Security team at Lee Koonce Corral, LLC to have a reference in response to any issues they may have in operating the SIEM.
      1. The SIEM vendor will provide documentation for reference for Lee Koonce Corral, LLC when using the SIEM for assistance on their own. This supports the objective by providing the IT Security team with information if they have any issues or need to learn new procedures concerning the SIEM.
      2. Default Security will create policies and procedures for IT Security team at Lee Koonce Corral, LLC to follow in using the SIEM. These will act as instructions for them on how to use the SIEM effectively and consistently. This supports the objective by keeping the IT Security team on track to operate the SIEM correctly.

# G. Project Timeline with Milestones

|  |  |  |  |
| --- | --- | --- | --- |
| **Milestone** | **Duration**  **(hours or days)** | **Projected Start Date** | **Anticipated End Date** |
| Sprint 1: Planning and  Requirements | 28 days | 6/25/2025 | 7/22/2025 |
| Sprint 2: Scope identification | 14 days | 7/23/2025 | 8/5/2025 |
| Sprint 3: Use Case Design and Application | 21 days | 8/6/2025 | 8/26/2025 |
| Sprint 4: SIEM Selection and Implementation | 21 days | 8/27/2025 | 9/16/2025 |
| Sprint 5: Data Capture Validation | 14 days | 9/17/2025 | 9/30/2025 |
| Spring 6: Configuration of Alerts and the SIEM Dashboard | 14 days | 10/1/2025 | 10/14/2025 |
| Spring 7: Training and Documentation | 14 days | 10/15/2025 | 10/28/2025 |
| Continuous Improvement | Continuous | Continuous | Continuous |

# H. Outcome

This project will be considered successful when, after two months, there has been a 60% reduction in successful adverse security events affecting Lee Koonce Corral, LLC. The data supporting the above will be collected by manually running an initial baseline of successful adverse security events before implementing the SIEM. Then, after two months, the data supporting this after implementation will be collected through the SIEM and confirmed by its reports. We will measure the difference between how many adverse security events occurred before and after implementing the SIEM.

# References

*What is SIEM? | IBM*. (2023, June 23). <https://www.ibm.com/think/topics/siem>

*About ISACA | A Global Business & Technology Community*. (n.d.). ISACA. Retrieved April 23, 2025, from

<https://www.isaca.org/about-us>

*2023 Volume 3 A Framework for SIEM Implementation*. (n.d.). ISACA. Retrieved April 28, 2025, from

<https://www.isaca.org/resources/isaca-journal/issues/2023/volume-3/a-framework-for-siem-implementation>

*SIEM for Small Business: What You Need to Know*. (n.d.). SentinelOne. Retrieved April 28, 2025, from

<https://www.sentinelone.com/cybersecurity-101/data-and-ai/siem-for-small-business/>

SIEM Implementation: Strategies and Best Practices. (n.d.). *Stellar Cyber*. Retrieved April 28, 2025, from

<https://stellarcyber.ai/learn/siem-implementation-best-practices/>

C, B. (n.d.). *Top 8 SIEM Optimizations—How to Get More From Your Existing Tech Stack*. Cribl. Retrieved April 28,

2025, from <https://cribl.io/blog/top-3-siem-optimizations-how-to-get-more-from-your-existing-tech-stack/>