Post-Implementation of SIEM Solution for Lee Koonce Corral, LCC

Joshua M. Lee

# Western Governors University

Table of Contents

[Western Governors University 1](#_Toc1118392407)

[Table of Contents 2](#_Toc1409628724)

[A. Proposal Overview 3](#_Toc1509656233)

[B. Review of Other Work and (B1) Works Informing Design 6](#_Toc1166389160)

[C. Changes to Project Environment 8](#_Toc1237496051)

[D. Methodology 8](#_Toc721990052)

[E. Project Goals and Objectives 9](#_Toc1453658640)

[F. Project Timeline with Milestones 10](#_Toc1090692197)

[G. Unanticipated Scope Creep 11](#_Toc1562051468)

[H. Conclusion and (H.1) Success of Project 11](#_Toc1398667624)

[References 13](#_Toc1783969392)

[I. Appendices 14](#_Toc1387956633)

[Appendix 1: 14](#_Toc1542808498)

[Appendix 2: 15](#_Toc1748596944)

[Appendix 3: 16](#_Toc1103999821)

# A. 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 were relatively new and they were just now getting the hang of them. The company recently had a meteoric rise in popularity due to several viral reviews of their services, which also came with increased exposure. The problem due to this exposure is that the company was receiving a steady increase in cyberattacks. Employees had received frequent phishing emails, which had led to unauthorized access attempts and data breaches. Malware was infiltrating the company through many avenues and infecting systems. These issues caused lapses in business, which resulted in a backup or turn away of customers or rescues. Lee Koonce Corral, LLC has two IT Security members on the team who were having difficulty keeping up with these events. They have adapted to the new technological setup, but the various sources they needed to look at for data related to these events were scattered across different systems (i.e., firewalls, servers, network devices, etc.), each with its own dashboard. By the time it took to get the data from these various sources and find the relationships between the data, the events had already created a significant negative impact on the company and created serious risks and disruptions. The amount of data alone was too much for the two-person IT Security team to handle effectively.

In the implementation of the SIEM for Lee Koonce Corral, LLC, we followed an Agile methodology, which broke the project into individual mini projects and used the ISACA's framework of SIEM implementation. First, Lee Koonce Corral, LLC identified the regulatory and business requirements concerning their location in Idaho and the US. This helped provide the information on their industry, consumers, and regulatory obligations needed to make a decision and Default Security helped with consultation on this step. This was to make sure that anything selected abided by those requirements and allowed us to see what was available and what solutions the company was limited to. Also, during this time, we worked with Lee Koonce Corral, LLC, to define the SIEM deployment approach. We helped them conduct a risk analysis of relevant issues to the company and a cost-benefit analysis to see what systems needed to be monitored and what would be financially feasible for them to run. Next, Lee Koonce Corral, LLC identified the range of the systems they wanted to be handled by the SIEM. This helped them understand what needed to be included and what did not need to be included in the data collection. After they developed the scope, we at Default Security worked with them to help validate and refine the scope to fit their needs, requirements, and regulations. Default Security then worked with Lee Koonce Corral, LLC, using the information they had gathered regarding critical operations, business needs, and compliance needs to define use cases, the scenarios that would apply to their SIEM monitoring and detection. This helped map these cases to the SIEM capabilities for threat detection and tracking of these security issues. During this, Default Security recommended adding a couple of additional definitions, which Lee Koonce Corral, LLC agreed to. This helped narrow down further which SIEM solutions would provide them support. Next, Lee Koonce Corral, LLC provided Default Security with infrastructure details, and we assisted in confirming that they support the defined cases and that no more needed to be added. Default Security then selected recommendations for SIEMs that fit Lee Koonce Corral, LLC’s needs, defined by the previous steps. Lee Koonce Corral, LLC had chosen SentinelOne because it fit their cost-benefit profile, and AI automation, advanced threat detection, and ease of use were features that aligned with their needs. Default Security confirmed their choice and implemented SentinelOne into their infrastructure once their senior staff approved.

After the implementation, the IT Security team determined that the SIEM captured the appropriate amount of security data to support the use cases that were created. Default Security did not have to make any adjustments. Default Security also ensured that all the required data and events were being properly sent to the SIEM and correctly analyzed. After validating the data, Default Security configured the rules and conditions to trigger alerts based on the use case scenarios provided by Lee Koonce Corral, LLC. After the alerts were configured, Default Security configured the dashboards and reports to the specifications provided by Lee Koonce Corral, LLC. After the full implementation was completed, the IT Security team received training in using the SIEM and was given documentation to assist with its use. This also included policies and procedures created by Default Security to guide the IT Security team in properly using the SIEM independently. After the handoff, the IT Security team at Lee Koonce Corral, LLC confirmed they will constantly tune their SIEM to adapt to the evolving security events affecting their company. This was the most crucial part, as the continuous effort put into the tuning would protect them from future security events and threats.

Since the IT Security team at Koonce Lee Corral, LLC was adjusting well to the new technological setup but were having issues with how long it took to track down and respond to these security events, we at Default Security helped introduce a solution called a Security Information and Event Management (SIEM) system into their network with positive outcomes. Two months after implementation, there was a 74% reduction in successful adverse security events affecting their company. This was measured by the difference between a manual baseline that was conducted of successful adverse security events before the implementation and reports from the SIEM on the number of those same events two months after.

This helped bring all the security information from their different systems into one place, so that the IT Security team did not have to interact with various dashboards or systems whenever there was an issue. This prevented them from losing precious time and having security threats go on longer than necessary. The SIEM successfully collected, organized, filtered, and analyzed the data for the team, instead of the previous scenario of sorting through data from the various sources manually, which allowed them to quickly find security data related to what was essential for the relevant issues. This helped the two-person IT Security team identify issues faster and respond to events quicker, which saved time and reduced 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 was better equipped to handle these security events as they occurred. It removed the overwhelming instances of manually going through large amounts of data and jumping between different systems, allowing them to focus on the actual issues instead of the process of getting to them. After implementing this solution, the IT Security team continued to constantly tune the SIEM to combat the threats they were facing and those they believed would affect Lee Koonce Corral, LLC in the future. Their diligence in this constant improvement is what also contributed to the 74% reduction in adverse security events.

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

**Review of Other Work 1 (Chheda, 2025)**

This work, provided on the site Sprinto by Heer Chheda, gives insight into what a SIEM provides to an organization. It also provides information on how a “SIEM plays a crucial role in providing a real-time view of security incidents by collecting, grouping, and analyzing data from different sources within the company’s IT environment” (Chheda, 2025). The work also provides a list of SIEM use cases that can keep an organization ahead of the evolving cybersecurity landscape

This work relates to the project because it reinforces why a solution of a SIEM was needed for Lee Koonce Corral, LLC. It confirms that since the IT Security team was having issues gathering and analyzing data from multiple sources, the implemented SIEM solution helps with that exact issue by using automation to make the process accurate and efficient. The use cases provided in this work were some of the same cases that were used in the implementation. Attack detection use cases were used primarily due to the initial issues with security events, but even use cases for PCI DSS compliance helped, since they take credit cards for some of their services.

**Review of Other Work 2 (*Top 11 SIEM Use Cases*, n.d.)**

This work on the Coralogix site provides a description of what a SIEM is used for and how it can help an organization. There is also a list of commonly used use cases that are used in tandem with a SIEM provided in this work. These use cases provide a wide range of situations from ensuring compliance to threat hunting.

This work relates to the project as it is another reinforcement of why this solution of a SIEM was needed for Lee Koonce Corral, LLC. Real-time monitoring, event correlation, log management, and incident response were all the needs that the company required addressed to combat the rise in security events they were experiencing. This work also has a well-rounded list of use cases that were used compared to the previous work, which focused more on specific attacks and compliance.

**Review of Other Work 3 (*SIEM Alerts Best Practices*, n.d.)**

This work is provided on the RedLegg site and gives an overview of the importance of SIEM tuning. It gives an explanation to understand why performing SIEM tuning helps to “control the amount of data presented to you, minimizing irrelevant alerts and bringing attention to alerts that are most likely to represent genuine threats in the context of your organization's specific security landscape” (*SIEM Alerts Best Practices*, n.d.). The work provides the benefits of tuning your SIEM and strategies regarding SIEM alert tuning.

The work, *SIEM Alerts Best Practices*, relates to this project because continuous improvement through SIEM tuning was an important focal point explained to the IT Security team at Lee Koonce Corral, LLC. This subject was heavily covered in the training to ensure they understood that not only does tuning help protect the company from present and future threats, but it also allows for a more seamless and effective environment to respond to these events quickly. The IT Security team realized the importance of this subject and made sure to put it into practice, which was one of the major driving factors of achieving the metric of a 74% reduction in successful adverse security events.

# C. Changes to Project Environment

Adding the SIEM solution to Lee Koonce Corral, LLC’s infrastructure positively affected their incident response time goals, reduced service downtime, eased the use between multiple systems, and enabled the ability to combat future threats. This solution aligned with their culture of always being of service and never turning any animal or person down by creating an environment where security events were handled expediently, reducing downtime. By adapting this solution, all the necessary data was stored and analyzed in one place, removing the need for complicated manual collection and analysis and allowing the IT Security team to be ready for issues as they came. The automated collection and analysis decreased the response time of combating security events, resolving them faster, and reduced the amount of downtime for issues, if any. The IT Security team's ability to constantly tune the SIEM enabled them to be one step ahead of the evolving landscape of cyber threats. The above outcomes of the project showed that it aligned with Lee Koonce Corral, LLC’s culture of never turning any person or animal away in need of assistance by keeping issues and downtime to a minimum.

# D. Methodology

For this project, we followed the Agile methodology. This provided an iterative and collaborative approach to designing and implementing the SIEM. This methodology created a strong, efficient system that could evolve to meet Lee Koonce Corral, LLC’s changing cybersecurity needs. These were structured into sprints that made the project manageable, allowed for adaptation if things changed, and provided a high-quality SIEM implementation into Lee Koonce Corral, LLC’s infrastructure.

In the first sprint, we focused on the initial planning of the SIEM implementation. This focused on identifying regulatory and business requirements that affected what SIEMs were applicable for use in Idaho and the US. This sprint also defined the SIEM deployment approach by conducting risk and cost-benefit analyses. The second sprint determined the scope of what needed to be covered. This contained the steps of identifying the scope of systems that needed to be monitored by the SIEM, allowing us to grasp which SIEMs supported the types of systems in the infrastructure. With the third sprint, we created scenarios as use cases and confirmed that the defined infrastructure would support those use cases. A couple of additional use cases were added to increase the effectiveness of what could be detected, with the approval of Lee Koonce Corral, LLC. For the fourth sprint, we provided recommendations to Lee Koonce Corral, LLC for SIEMs that fit their needs and requirements. Lee Koonce Corral, LLC chose SentinelOne as the SIEM solution to be added. Default Security commenced the implementation of the SIEM into their infrastructure once the SentinelOne solution was approved by Lee Koonce Corral, LLC’s senior staff.

After the implementation, the IT Security team validated that the data being captured was sufficient in the fifth sprint. Adjustments did not have to be made by Default Security. Validations were made by Default Security that all data was being sent through the SIEM and analyzed correctly. In the sixth sprint, Default Systems configured the rules and conditions that would trigger the SIEM alerts and ensured they occurred correctly when needed. Also, during this sprint, Default Systems configured the SIEM dashboards and their reports to the specifications required by Lee Koonce Corral, LLC. In the seventh and final sprint, the IT Security team was trained, which was conducted to get them proficient in using the SIEM. Default Security and the SIEM vendor also provided them with documentation, policies, and procedures during this sprint. After the SIEM implementation was completed, the IT Security team at Lee Koonce Corral, LLC continuously improved and tuned it to keep up with the needs of the company and the evolving cybersecurity landscape.

# E. Project Goals and Objectives

The goal of implementing a SIEM to help monitor and manage security events and its objectives were accomplished through the successful and thought-out implementation process. The first three sprints of the implementation were spent defining logistics, environment, needs, and requirements. These sprints were supported by objectives like identifying regulatory and business requirements, creating the scope of systems to be monitored, and defining use cases. This helped accomplish the goal by creating the foundation for what type of SIEM would fit Lee Koonce Corral, LLC’s needs and requirements, ensuring this solution had the correct value for the company.

Sprints four through six handled the actual implementation of the SIEM and the configuration of the data capture and SIEM solution. The implementation objectives in these sprints accomplished the goal by ensuring that the SIEM was properly added to the infrastructure and was working correctly and efficiently before handing the solution over to Lee Koonce Corral, LLC. This assured the company that they had a fully functional solution and that it was set up to their requested specifications. All these implementation steps led up to and supported the final objective of this goal by providing the IT Security team at Lee Koonce Corral, LLC a solution tailored to their needs to allow room for continuous improvement. This would accomplish the overall goal by making sure that the SIEM would always be viable to help monitor and manage security events in their company.

# F. Project Timeline with Milestones

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Milestone** | **Planned Duration** | **Actual Duration** | **Actual Start Date** | **Actual End Date** |
| Sprint 1: Planning and Requirements | 28 days | 28 days | 10/26/2024 | 11/22/2024 |
| Sprint 2: Scope Identification | 14 days | 14 days | 11/23/2024 | 12/6/2024 |
| Sprint 3: Use Case Design and Application | 21 days | 21 days | 12/7/2024 | 12/27/2024 |
| Sprint 4: SIEM Selection and Implementation | 21 days | 21 days | 12/28/2024 | 1/17/2025 |
| Sprint 5: Data Capture Validation | 14 days | 14 days | 1/18/2025 | 1/31/2025 |
| Sprint 6: Configuration of Alerts and the SIEM Dashboard | 14 days | 14 days | 2/1/2025 | 2/14/2025 |
| Sprint 7: Training and Documentation | 14 days | 14 days | 2/15/2025 | 2/28/2025 |
| Continuous Improvement | Continuous | Continuous | Continuous | Continuous |

No variances occurred between the proposed timeline and the actual implementation timeline. Even though the observed holidays of Christmas and Thanksgiving occurred during this timeline, teams put in extra work to ensure that the implementation stayed on schedule. During the Use Case Design and Application sprint, there were a couple of additional use case definitions that Default Security recommended to add to the SIEM. This was approved quickly by Lee Koonce Corral, LLC and added still within the proposed timeframe. The Agile methodology also kept the project on time by giving defined time frames that kept teams on task for each sprint.

# G. Unanticipated Scope Creep

There were no time variances between the proposed timeline and what occurred during implementation. This was due to a couple of factors. First, the Agile methodology helped keep the project on task by breaking it into manageable portions. This allowed teams to focus on the objectives of the current sprint and be cognizant of when each deadline needed to be met. Also, even though the observed holidays of Christmas and Thanksgiving occurred during this timeline, teams put in extra work to ensure that deadlines were met during those respective sprints. The only addition was the recommendation, approval, and implementation of a couple of additional use case definitions during the third sprint. The time needed for this was negligible and it was still completed within the timeframe of that respective sprint.

# H. Conclusion and (H.1) Success of Project

After the implementation, Default Security reconvened with the IT Security team of Lee Koonce Corral, LLC, two months later. We pulled up the manual baseline we conducted together before the implementation process started and compared it to reports produced by the SIEM. After implementing the SIEM, the results showed a 74% reduction in successful adverse security events affecting their company. This was due to the in-depth, mindful implementation process and the SIEM tuning effort provided by the IT Security team. The IT Security team informed us that they were no longer overwhelmed with the amount of data that had to be processed due to the automation of analysis through the SIEM. There were fewer security events to handle, which allowed them to focus on the few that did occur with complete focus and allowed them to field other IT tasks that needed to be completed with the extra time. The culture of Lee Koonce Corral, LLC was preserved as the reduction in downtime allowed them to always be of service and never turn anyone or any animal away from assistance.

Due to the results of the completed project, the future looks bright for Lee Koonce Corral, LLC. With only two months after SIEM implementation providing a 74% reduction in successful adverse security events, constant tuning and improvement should keep the company without significant downtime and always be able to provide assistance to every person and animal. Suppose the IT Security team keeps up to date with current cybersecurity landscapes and is proactive. In that case, there is a high possibility of an increase in the reduction of successful adverse security events.

With a 74% reduction in successful adverse security events, this project is considered successful with the original goal metric being 60%.

# References

Chheda, H. (2025, January 2). Top 12 SIEM Use Cases to Implement in 2025. *Sprinto*.

<https://sprinto.com/blog/siem-use-cases/>

*Top 11 SIEM Use Cases*. (n.d.). Coralogix. Retrieved May 1, 2025, from

<https://coralogix.com/guides/siem/top-11-siem-use-cases/>

*SIEM Alerts Best Practices: Tuning for Fatigue Reduction*. (n.d.). Retrieved May 1, 2025, from

<https://www.redlegg.com/blog/siem-alert>

# I. Appendices

## Appendix 1:

**SentinelOne SIEM Dashboard**

A screenshot of a computer

AI-generated content may be incorrect.

This artifact is a screenshot of the SentinelOne SIEM Dashboard. Lee Koonce Corral, LLC sees this when managing and monitoring their SIEM. It is customizable to allow for adding and removing widgets to give the best single-pane-of-glass experience to what is needed for easy access. This allows the IT Security team access to real-time information and alerts for them to be ready for any security issues that may occur.

## Appendix 2:

**SentinelOne SIEM Training Certificate**

****

This is a copy of a training completion certificate that one of the IT Security members received after training to use the SentinelOne SIEM platform. This certifies that the member has gone through all the proper training and is now proficient in using the SIEM after the handoff occurs. To attain this certificate, the members had to go through a two-week training course and then were given a hands-on test to show that they could display proper use of the platform, proficiency in tuning the SIEM, and competence in interpreting the reports.

## Appendix 3:

**Use Case Mapping Documentation**

**A close-up of several types of data

AI-generated content may be incorrect.**

This is a screenshot of part of the Use Case Mapping Documentation that was used to define the rules the SIEM needed to follow. This was the first draft with the first rules that were immediately added since they were in relation to the issues Lee Koonce Corral, LLC brought to us initially when needing a security solution. More was added from the information provided about their infrastructure, compliance needs, and risk analysis outcomes. This aided in the selection of the SIEM and also what was configured within the solution to protect the company.