Security, Information, and Event Management (SIEM) Solutions

****

Western Governors University

Table of Contents

A. Proposal Overview

A.1 Problem Summary

TransBrasil Logistica is a small shipping company based in São Paulo, Brazil. They have just received their first major contract from Vicente Industria Sociedade Limitada (LTDA), a large Brazilian parts supplier. TransBrasil has a small IT department of eight personnel that manages its network infrastructure. For network security, they have a basic setup that has their network separated into two Virtual Local Area Networks (VLANs): one VLAN for TransBrasil and its partners and another VLAN for TransBrasil's own intranet. The network has one perimeter firewall to monitor traffic between the internet and TransBrasil's network and another to monitor network traffic between the VLANs. The IT department analyzes the log files from its firewalls manually each week to spot anomalies and potential intrusions. They have been able to operate like this as a cost-saving measure since, as a smaller and lesser-known company, they were not receiving much network traffic. However, securing a contract with a large company like Vicente Industria LTDA would significantly increase network traffic, making it impractical for the IT department to manually analyze tens of thousands of logs in a timely manner and effectively detect and respond to potential threats. Ineffective detection and response to potential threats pose a significant security risk, as hackers and other threats could compromise Vicente Industria's, TransBrasil's, and even their other clients' data. The IT department head has brought up this concern to TransBrasil's executives. The executives, not wanting any major problems to hinder the success of this contract, agree with the IT department head's concerns and have left it up to him to collaborate with the rest of the IT department to come up with a solution they can implement ASAP.

A.2 IT Solution

The IT department has decided that TransBrasil should implement a Security, Information, and Event Management system (SIEM). SIEMs are centralized platforms that collect, analyze, and manage security-related data from multiple sources across an organization's IT infrastructure. They can provide real-time insights into patterns and potential security threats (What is SIEM?, n.d.). A SIEM can be implemented as hardware, software, or managed services. Next-generation SIEMs have implemented AI and machine learning into their systems, which enhances the SIEM's ability to detect and respond to threats, as the AI can learn traffic patterns unique to a specific network to better detect any anomalies (What is SIEM?, 2025). A SIEM like Exabeam's New-Scale SIEM is a great solution for TransBrasil, as it is cloud-based, AI-driven, modular, and scalable. It also uses the Google Cloud Platform (GCP) to store log files (New-Scale SIEM, 2025). New-Scale SIEM can be managed in-house by a business' own IT Department or managed through a third-party managed service provider (MSP), IT professionals who can set up and manage the SIEM for an organization (Humphries, 2023).

New-Scale SIEM will give TransBrasil a foundation for a strong network security posture. Since a SIEM's core function is to collect and analyze security data, it directly solves TransBrasil's need to be able to quickly analyze log files for potential threats. Per Exabeam, New-Scale SIEM can sustain a processing speed of over 2 million events per second (New-Scale SIEM, 2025). Implementing this SIEM will optimize resource allocation, enabling the IT department to dedicate more time and effort to other IT-related tasks for Vicente Industria's onboarding. The included AI features ensure that TransBrasil will be implementing a next-generation SIEM, giving their network security the capabilities needed to combat the latest threats in the ever-changing IT landscape. With New-Scale SIEM being cloud-based,

TransBrasil won't have to worry about planning for more hardware onsite for either the SIEM or log file storage. New-Scale SIEM's modularity and scalability allow it to be a long-term and cost-effective solution for TransBrasil, as the SIEM can compensate for additional network devices that may be added in the future, and TransBrasil can scale up or down the SIEM and its provisions as needed for their business. Finally, TransBrasil has the option of contracting a third-party MSP to guarantee a smooth and rapid implementation of New-Scale SIEM. Overall, implementing New-Scale SIEM will demonstrate TransBrasil's commitment to Vicente Industria by showcasing a proactive approach to safeguarding their data and ensuring the highest standards of security for this partnership.

A.3 Implementation Plan

Since TransBrasil's executives want a solution implemented as fast as possible, they have already decided they will use an MSP for the initial setup and continued management and support. This will also minimize the amount and severity of problems that may arise during the setup process. During this time, the IT department will assist the MSPs in deploying the SIEM, as well as undergoing Exabeam official training (Education and Training, 2024) for their eventual takeover of managing the SIEM for TransBrasil. The MSP will provide continued maintenance of the SIEM for at least three months after initial setup. After this time, the IT department and TransBrasil executives will decide if the IT department has been trained sufficiently to manage the SIEM without the need for an MSP. If it is determined that the team isn't ready, they will extend their contract of continued management with the MSP for another three months.

Each member of the IT department will be crucial for the implementation and ongoing support of both the SIEM and TransBrasil's partnership with Vicente Industria. While the SIEM

will greatly enhance the IT department's efficiency, its integration will also add complexity to the network infrastructure. Combined with the increased business of TransBrasil's new partnership with Vicente Industria, the IT department may need to hire more people.

First, the IT department head and TransBrasil's executives will establish goals for what they want the SIEM to accomplish and how it will do so. Then, they will meet with Exabeam representatives to decide which of their MSP partners would be best for their business (they have decided to go with Deloitte Brazil as their MSP, as they have multiple offices throughout Brazil to provide quality support (Offices in Brazil, n.d.)). After selecting an MSP, the IT department head will assess TransBrasil's current network infrastructure to plan the rollout of New-Scale SIEM in the company.

Second, the IT department and Deloitte will use the information gathered from the network infrastructure assessment to design the system architecture, identify log sources to capture data, determine the length of time for data storage, and decide on a deployment timeline. As TransBrasil is a small company with a fairly simple network infrastructure, the IT department and Deloitte decided that two months should be ample time for them to deploy and evaluate the SIEM's effectiveness. They will also develop a plan to inform TransBrasil employees, as well as relevant Vicente Industria and partner personnel, about the upcoming changes, their benefits, and any potential network performance disruptions during the implementation process. The process of implementing the SIEM should only cause, if any, low to moderate interference on the normal flow of work at TransBrasil. After creating the plans, The IT department and Deloitte will get approval from TransBrasil's executives to execute the plan.

Third, Deloitte will begin the setup of New-Scale SIEM for TransBrasil. They will work with Exabeam to set up the cloud services for the SIEM and log file storage, as well as provision user access for the appropriate personnel, such as The IT department and Deloitte service providers. Next, they will configure New-Scale SIEM dashboard for local (on-premises) management. Then, they will establish a high-speed, secure network connection from TransBrasil's network to the SIEM cloud deployment so that the log files can be captured and sent to New-Scale SIEM for processing and then storage. Finally, Deloitte will test the basic system setup to verify functionality. The IT department head and his second in command will oversee this setup process and take notes while the rest of the department carries out the team's daily tasks.

Fourth, Deloitte will do a pilot test on the SIEM by capturing data only from the perimeter firewall and only from outbound log files from the IT department's computers to limit any interruptions to the normal flow of work for TransBrasil and its partners. They will still notify all relevant personnel if any interruptions should occur. They will use this test to gather feedback on alerts and preliminary SIEM data processing and make adjustments as needed. The IT department head and second in command will continue to oversee this process and take notes.

Fifth, after a successful pilot test and configuration, Deloitte will proceed to do a full integration of New-Scale SIEM into TransBrasil's network. This will include configuring the SIEM to capture log files fully from both firewalls. Again, the IT department will notify all relevant personnel during this time if any interference with normal work is expected to happen. After the full setup, Deloitte will monitor the SIEM and log file capturing to fine-tune adjustments. This is to help the AI capture a baseline of what normal traffic in and out of TransBrasil's network looks like and to help reduce false positives in the future. This step may

take several days to a week to process sufficient logs and evaluate the SIEM's long-term effectiveness. Again, the IT department head and second in command will oversee this process and take notes.

The sixth and final step is ongoing support and training. As stated earlier, Deloitte will provide ongoing support for three months after the initial setup of New-Scale SIEM. During this time, they will continue to monitor and optimize the SIEM to ensure the best performance for TransBrasil. While this is ongoing, the IT department will be undergoing instructor-led training courses from Exabeam in groups of two so that there are enough IT personnel left at TransBrasil to handle day-to-day tasks. After training, they will work with the Deloitte service providers to get more hands-on training with the SIEM, as well as draft documentation and standard operating procedures (SOPs) for maintaining the SIEM. After three months or an extended period (if necessary), the IT department will take full control of managing the SIEM, and TransBrasil will end its managed service support with Deloitte.

This implementation plan is appropriate for the SIEM because it provides a structured, step-by-step approach that ensures thorough planning, execution, and evaluation of the SIEM. While all steps in the plan are important, there are some steps that are critical to successfully implement the SIEM. It is crucial that TransBrasil first establishes its goals before they do any work to implement the SIEM. Next, it is also crucial that an implementation plan is designed before the actual rollout. Finally, it is crucial that a test run be conducted before the full rollout of the SIEM.

Clear and established goals provide a guide for setting up and tailoring the configuration of the SIEM to meet the company's needs. These goals also help TransBrasil and its IT department to define success criteria, enabling the organization to measure the SIEM's

effectiveness. Without clear goals, the SIEM may be misconfigured and fail to address the vulnerabilities that caused TransBrasil to implement the SIEM in the first place. This will just cause TransBrasil to waste valuable time and resources.

After establishing its goals and doing the preliminary work necessary (selecting a SIEM and MSP), it is important that TransBrasil next develops a plan and implementation process for the SIEM to ensure that it will be configured to satisfy the goals previously established. This also helps the team to minimize any potential downtime and avoid disruptions to the company, ensuring a smoother rollout.

During the implementation process, it is critical to conduct a test run of the SIEM with a few network resources before doing a full-scale rollout. This allows the team to catch any potential issues with the SIEM before its full rollout, such as integration issues with the existing structure and any configuration issues. By doing a test run, the team can identify and address issues early, reducing the risk of disruptions during the rollout and ensuring a smoother implementation of the SIEM.

Review of Other Works and B .1 Relation of Artifacts to Project Development

Review of work 1

Palo Alto Networks has an article on SIEM implementation best practices. It emphasizes understanding security needs, planning architecture, integrating existing security tools, and thorough testing. It also highlights the need for continuous refinement and training. This article also stresses the importance of defining normal behavior in network traffic to minimize false positives (What are SIEM implementation best practices?, n.d.). This article relates to the methodology used for the IT solution, as it highlights the key aspects used in the implementation plan and their importance. The article also shows it is equally important to plan for the long

term, beyond just planning for the SIEM deployment. A plan for the long term will ensure the success of your SIEM for the long term as well.

Review of work 2

Exabeam has written an article on SIEM compliance and how its products help organizations meet requirements like the European Union General Data Protection Regulation (GDPR) and the Payment Card Industry Data Security Standard (PCI DSS). Exabeam highlights features that their products have to help organizations be in compliance with audits with comprehensive compliance logging, protecting Personally Identifiable Information (PII), mitigating insider threats, and long-term data storage (Compliance, 2024). This is important because some organizations may work with their government and have standards that they need to comply with, or the organizations may have state or federal laws to comply with in how they handle personal data. Exabeam shows how their products, such as New-Scale SIEM, can be configured to meet these governmental or legal requirements. This article relates to the proposed IT solution design process because organizations like TransBrasil need to make sure they are aware of any government or industry standard regulations they may need to comply with so they can make sure their SIEMs are capable of adhering to those standards and configure them accordingly.

Review of work 3

An article published on Exabeam's blog discusses the cost-effectiveness of Exabeam SIEMs. A Ponemon study revealed that 90 percent of surveyed Exabeam SIEM users had reduced costs and increased value when compared to legacy systems. Many surveyed Exabeam SIEM users realized this value within days or a week, up to 92 percent of users. Finally, the article ends by stating that up to 79 percent of surveyed users did not use professional services

for deployment, with 55 percent of those surveyed not needing professional services after deployment (Daughney, 2019). This demonstrates that modern SIEM solutions can be cost-effective for enhancing network security and can be managed efficiently without the need for professional services. These are things organizations like TransBrasil and its IT department can consider when choosing a SIEM and planning its implementation.

Review of work 4

Another article by Exabeam explains how partnering with Google Cloud has enhanced its AI-driven security operations platforms. By integrating Google Cloud's data sources like Google Workspace and Google Cloud Platform services, Exabeams's SIEMs and security suites have improved threat detection, investigation, and response while optimizing data storage and reducing costs. Google Cloud also allows for "petabytes of log ingestion and storage" (Google Cloud, 2024). This article shows how modern SIEMs have moved into the cloud and how cloud technology has greatly enhanced the effectiveness of SIEMs in virtually all aspects.

C. Project Rationale

Integrating a SIEM into a business network infrastructure enables faster and more efficient threat detection and response than manual data analysis, enhancing overall cybersecurity. With AI features for more efficient data processing and threat detection and the capabilities to process vast amounts of data in real-time, next-gen SIEMs are a must-have security solution in today's IT environment. The IT environment is always expanding with new technologies. Unfortunately, with new technologies can also come new vulnerabilities and bad actors who want to capitalize on those vulnerabilities. Hacking has become increasingly sophisticated over the years and has gone from individuals simply stealing PII for identity theft

or data for monetary exploitation to hacking groups causing terror on a national scale, wreaking havoc on large companies and even critical infrastructure and government organizations (Pattison-Gordon, 2021). Organizations that do not keep their network security up to date with the latest standards are leaving themselves vulnerable to a host of bad actors who could infiltrate their networks and steal valuable data. This could cause immense harm to their business and their reputation. For example, in 2013, Target Corporation was the victim of a massive cyber attack. Their slow response to security alerts allowed hackers to breach their systems and go undetected for weeks, allowing the hackers to gain access to the personal and credit card information of over 70 million customers (Brooks, 2024). This cyber attack caused Target massive reputational damage and was an expensive lesson in network security, with Target paying 18.5 million dollars to settle claims (Brooks, 2024). This incident was a pivotal point in IT and cybersecurity, showcasing the need for strong cybersecurity measures to protect from threats. Had Target and its associates implemented SIEMs in their network infrastructure for faster threat detection, the breach would have been caught far sooner, mitigating the damage. Therefore, cybersecurity should always be one of the most important considerations for any organization with a digital presence, and a SIEM should always be the central part of any network security infrastructure.

D. Current Project Environment

Currently, TransBrasil has around 150 employees. However, with this new partnership with Vicente Industria, that number is likely to increase. The success of this partnership with Vicente Industria could very likely launch TransBrasil into being a major shipping company throughout Brazil. The executives know this could be the company's big break and are willing to do everything they can reasonably to make this partnership work. As such, they are currently

more open to change than many of their employees may be, so long as the changes don't significantly interfere with their other contracts.

TransBrasil's software and technology are fairly modern, but its implementation and network are fairly basic. TransBrasil prioritizes simplicity in its technology to streamline employee onboarding and training, making it accessible to workers of all age groups and skill levels while ensuring ease of recruitment and efficient workforce integration. This is also evident in the simplicity of their network infrastructure: two firewalls and one network segmented into two VLANs. The executives believe this simplicity enhances operational efficiency, providing a significant competitive advantage.

The company's current way of manually processing log files has been working so far. Being a lesser-known company, TransBrasil has benefitted from lower network traffic compared to other companies and is less likely to attract the attention of malicious actors due to its relatively low profile. However, this could all change when they partner with such a large company like Vicente Industria. The IT department anticipates a significant increase in network traffic due to the new partnership and heightened attention from individuals and companies curious about Vicente Industria's decision to collaborate with a lesser-known shipping company like TransBrasil. This will bring many more visitors to their website and, unfortunately, potentially bad actors. They may see the small company TransBrasil as a vulnerability, expecting them to have weak cybersecurity to easily breach and get to their data and Vicente Industria's data. A delayed breach detection by the IT department could lead to severe financial, reputational, and legal repercussions for TransBrasil, Vicente Industria, and their other partners. There is no way a team of eight people could possibly manually scan through

thousands or potentially millions of log files fast enough to keep up with the network traffic, let alone do this and keep up with their other duties at the same time.

Implementing a SIEM will enable the IT department to analyze significantly more logs in real-time than is possible manually. This will allow them to detect and respond to threats as soon as they happen. Implementing a SIEM resolves their immediate problem and positions their network infrastructure for future growth, as the SIEM establishes a scalable foundation for enhanced security. Implementing a SIEM will also have minimal impact on end users, as it requires no additional software on their devices. This ensures that older employees and those less comfortable with technology won't need to learn new tools, allowing TransBrasil to remain committed to providing a simple work environment for employee integration.

E. Methodology

The Waterfall Method is the best methodology for implementing Exabeam New-Scale SIEM. It is a structured, step-by-step process that follows a linear, sequential approach, which is crucial for making sure the SIEM will be implemented properly and function as intended. The rigidity of the Waterfall Method also ensures that each step of the SIEM implementation process stays in alignment with the established goals.

The Waterfall Method is broken down into five phases. The first phase is requirements. This is where a project’s goals are established based on an organization’s needs. The second phase is design. After goals are established and requirements are gathered, the solution will be developed to achieve those goals. For example, the design phase of implementing a new technology would be drafting the hardware, software, and integration configurations so that the technology will achieve those goals. The third phase is implementation. This is where the design is taken and put into action. For technology solutions,

this is where the technology or software is installed and configured according to the design plans. The fourth phase is verification. After implementing the solution, it needs to be tested to ensure that it meets established requirements. The final phase is maintenance. Ongoing monitoring of the solution is done to make sure that the solution continues to operate as designed and in accordance with requirements. Optimization also happens here, ensuring that the solution is operating as efficiently as possible.

In the requirements phase for TransBrasil to implement New-Scale SIEM, the major milestones will be to identify security goals and any compliance requirements. TransBrasil has preliminarily identified and acted on one of its goals, selecting Exabeam's New-Scale SIEM and opting for initial management by an MSP, Deloitte, in order to have the SIEM up and operational as fast as possible. They will also identify their data sources for collection, such as firewalls, servers, and applications. After that, they will establish log retention time periods and reporting needs. Finally, this phase will be completed once final approval from the TransBrasil executives is given for the scope of the SIEM project.

In the design phase, the major milestones will be centered around designing the architecture of New-Scale SIEM. Since they already know what SIEM they will be using and how it will be managed, the IT department will work with Deloitte service providers to carry out this process. Major milestones will include designing the data ingestion and storage process, defining correlation rules and alert mechanisms, defining access control roles and users for the SIEM, which devices to install software for the SIEM dashboard and monitoring, and planning the integration of the SIEM with the existing network infrastructure. These milestones contribute to the overall configuration of the SIEM. Finally, this phase will be complete once final approval from TransBrasil executives is given for the design plans.

In the implementation phase, the major milestones will be centered around the successful installation of the SIEM into TransBrasil's network. First, all necessary Exabeam software will be installed on the relevant monitoring stations. Data source integrations will then be configured from the chosen network devices. Finally, New-Scale SIEM dashboard will be configured, consisting of user accounts setup, setting up the rules, and configuring alerts. This phase will be complete upon the successful completion of New-Scale SIEM setup and its initial configurations.

In the verification phase, New-Scale SIEM will be tested to make sure that all parameters of the SIEM are operating as intended. SIEM rules will be validated. SIEM system performance and load tolerance will be tested. Security, monitoring, and alerting features will also be tested. Finally, user accounts will also be validated. This phase will be completed upon successful testing of all components with any identified issues resolved.

Finally, in the maintenance phase, the full rollout of New-Scale SIEM is established. Ongoing monitoring and performance of the SIEM begins. Deloitte service providers switch from installation tasks to ongoing performance and monitoring tasks, performing configuration changes as necessary to maintain SIEM adherence to established goals and for optimization purposes. The IT department will undergo Exabeam training to eventually take over New-Scale SIEM monitoring and maintenance after the three-month period ends. Although maintenance is an ongoing process for the entire SIEM lifecycle, this phase will be completed once The IT department takes full control of the SIEM and the Deloitte service providers are dismissed.

F. Project Goals, Objectives, and Deliverables

F1. Relationship Table

The following table breaks down the project goal into objectives and their corresponding deliverables.

	Goal	Supporting objectives	Deliverables enabling the project objectives
1	Improve Network Security	1.a. Implement a SIEM .	1.a.i. Contract with MSP for Exabeam SIEM setup and ongoing support.
			1.a.ii. Draft SIEM design plans
			1.a.iii. Implement the SIEM.
			1.a.iv. Validate SIEM functionality and performance before conducting the full rollout.
		1.b. Train the IT department to manage the SIEM.	1.b.i. MSP shifts from initial setup to SIEM monitoring and ongoing support.
			1.b.ii. Entire IT department completes Exabeam training.
			1.b.iii. IT department takes over SIEM monitoring and maintenance, and MSP is dismissed.

F.2 Goals, Objectives, and Deliverables Descriptions

The overall project goal is to improve TransBrasil's network security. Their current way of manually scanning log files is a network vulnerability that needs to be addressed. The two objectives to accomplish this goal are to implement a SIEM and train the IT department to manage the SIEM. A SIEM will allow TransBrasil to automate the data collection, analysis, and threat detection processes. This, in turn, makes for a stronger, more secure network. The IT department also needs to be trained on how to manage the SIEM. A SIEM is only effective if properly configured and maintained, making it essential for TransBrasil's IT department to receive the necessary training for its ongoing management and lifecycle support.

In order to complete the objective of implementing a SIEM in accordance with TransBrasil's requests, they need to achieve several deliverables. For 1.a.i., TransBrasil needs to contract an MSP to set up, configure, and provide ongoing support for New-Scale SIEM. To ensure the quickest and smoothest SIEM implementation possible, TransBrasil has opted to contract an MSP to handle setup and configuration and provide ongoing support for a period of time. For 1.a.ii., the IT department and MSP will work together to draft the SIEM design plans. It is crucial for design plans to be drafted to ensure that the SIEM will be configured properly and perform its functions according to TransBrasil's needs. For 1.a.iii., the MSP will implement and configure the New-Scale SIEM in alignment with the design plans. Finally, for 1.a.iv., the MSP will conduct validation and testing of the SIEM functionality and performance, verifying that the SIEM functions as intended before doing the complete rollout on the entire network. These deliverables will ensure that the SIEM will be properly implemented.

There are also several deliverables to complete the objective of getting the IT department trained to manage the SIEM. For 1.b.i., the MSP will shift to ongoing monitoring and support after successfully implementing the SIEM. This will give TransBrasil a team to monitor and maintain New-Scale SIEM while the IT department is in training. For 1.b.ii., TransBrasil's IT department will undergo official Exabeam training to learn how to manage New-Scale SIEM, as they will be the ones to manage the SIEM for its lifecycle. For 1.b.iii., after the IT department has successfully completed their training, monitoring, and maintenance for the SIEM will be handed off to them, and the MSP will be dismissed, ending their contract with TransBrasil. These deliverables will ensure that the IT department is sufficiently trained and that the SIEM will receive the necessary continued support until the IT department is ready to monitor and maintain the SIEM for TransBrasil themselves. With a fully functioning SIEM and

a properly trained IT department to manage it, TransBrasil will have successfully improved its network security.

G. Project Timeline with Milestones

Milestone or deliverable	Duration (hours or days)	Projected start date	Anticipated end date
Contracting with an MSP for SIEM services	7 Days	2/17/2025	2/23/2025
Approval of SIEM requirements	7 Days	2/24/2025	3/2/2025
Finalized and approved SIEM design plans	7 Days	3/3/2025	3/9/2025
Successful completion of SIEM setup and initial configurations	7 Days	3/10/2025	3/16/2025
Successful testing followed by full SIEM deployment	14 Days	3/17/2025	3/30/2025
Handover of ongoing SIEM monitoring and	90 Days	3/31/2025	6/28/2025

support to IT department			

H. Outcome

In conclusion, the purpose of this project was to provide a better solution for monitoring network traffic to detect intrusions instead of manually scanning individual log files. Manually scanning through thousands of log files is a very tedious process that may not be fast enough to detect and respond to potential network breaches. This could leave an organization vulnerable to a host of cyber threats and bad actors looking to breach an organization's network and steal valuable data. A SIEM can automate the data analysis process to monitor network traffic and detect threats in real-time. With the innovations of cloud technology, modern-day SIEMs can be a faster and more cost-effective solution compared to previous-generation SIEMs, making them an attainable network security solution for even the smallest organizations.

For TransBrasil, Exabeam's New-Scale SIEM, which works on the Google Cloud Platform, is a very cost-effective solution. This leaves them with more money to hire a Managed Service Provider to provide the initial setup and ongoing management of the SIEM for a rapid deployment. Since a SIEM works in the background from an end-user perspective, TransBrasil's employees outside of the IT department and its partners will not notice anything different, providing a virtually non-existent impact on their work environment. The result will be a significantly strengthened and better-prepared network security posture for TransBrasil to handle future threats.

This project will be successful based on a few key metrics: the speed at which the SIEM can detect threats and its consistency, the number and accuracy of alerts generated, its

performance under TransBrasil's heaviest network traffic loads, and its effect on the outcome of incidents (LinkedIn, n.d.). A SIEM's real-time detection speed can be easily verified by simulating an unauthorized entry into TransBrasil's network. Intrusions can be simulated periodically to test that the SIEM will broadcast notifications immediately upon detection. The accuracy of these detections can be measured by the amount of false positives generated. Too many false positives can be a distraction and waste too many resources. Network traffic can be artificially increased to test how well the SIEM performs under increased network traffic. Finally, a SIEM's effectiveness in the outcome of incidents, should they arise, can be measured by the quality of information given about potential threats that lead the IT department to quick and effective solutions. The goal for these metrics is to provide a framework for TransBrasil to be able to monitor the SIEM's effectiveness, allowing them to optimize the SIEM as needed or even make configuration changes as the company changes. With these metrics, TransBrasil's new SIEM will always be ready to protect the company from any threats that may arise.

I. References

Brooks, C. (2024, March 12). The Target Breach 10 Years Later. Security Info Watch. https://www.securityinfowatch.com/retail/article/53098895/the-target-breach-10-years-later

Compliance. Exabeam. (2024a, July 8). https://www.exabeam.com/use-cases/compliance/

Daughney, T. (2019, September 17). Ponemon study finds 90% of users get lower costs and more value with Exabeam Siem. Exabeam. https://www.exabeam.com/blog/siem-trends/ponemon-study-finds-90-of-users-get-lower-costs-and-more-value-with-exabeam-siem/

Education and Training. Exabeam. (2024b, November 25). https://www.exabeam.com/support-and-services/education-and-training/

Google Cloud: Powering the AI-driven Exabeam security operations platform. Exabeam. (2024c, November 7). https://www.exabeam.com/partners/google-cloud/

Humphries, S. (2023, December 7). MSSP, MDR, or SAAS SIEM? . Exabeam. https://www.exabeam.com/blog/siem-trends/mssp-mdr-or-saas-siem/

LinkedIn. (n.d.). You've invested in a SIEM deployment. How can you be sure it's paying off? How to Assess and Optimize Your SIEM Deployment.

https://www.linkedin.com/advice/0/youve-invested-siem-deployment-how-can-you-n679f

New-Scale SIEM. Exabeam. (2025, January 7). https://www.exabeam.com/platform/new-scale-siem/

Offices in Brazil. Deloitte. (n.d.). https://www.deloitte.com/br/en/offices/brazil-offices.html

Pattison-Gordon, J. (2021, October). Through the Years: A Broad Look at Two Decades in Cybersecurity. GovTech. https://www.govtech.com/security/through-the-years-a-broad-look-at-two-decades-in-cybersecurity

What are SIEM Implementation Best Practices?. Palo Alto Networks. (n.d.-a). https://www.paloaltonetworks.com/cyberpedia/what-are-SIEM-implementation-best-practices?utm_source=chatgpt.com

What is SIEM?. Palo Alto Networks. (n.d.-b). https://www.paloaltonetworks.com/cyberpedia/what-is-siem#:~:text=SIEM%2C%20which%20stands%20for%20Security,Centralized%20visibility%20into%20network%20security