Security, Information, and Event Management (SIEM) Solutions Post-Implementation

****

Western Governors University

Table of Contents

Summary

TransBrasil Logistica was a small shipping company based in São Paulo, Brazil. They received their first major contract from Vicente Industria Sociedade Limitada (LTDA), a large Brazilian parts supplier. At the time, TransBrasil had a small IT department of eight personnel that managed its network infrastructure. For network security, they had a basic setup that saw 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 had 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 used to analyze the log files from its firewalls manually each week to spot anomalies and potential intrusions. They were 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 significantly increased TransBrasil's 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 posed 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 brought up this concern to TransBrasil's executives. The executives, not wanting any major problems to hinder the success of this contract, agreed with the IT department head's concerns and left it up to him to collaborate with the rest of the IT department to come up with a solution they could implement ASAP.

The IT department 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 Artificial Intelligence (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 was 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 gave TransBrasil a foundation for a strong network security posture. Since a SIEM's core function is to collect and analyze security data, it directly solved 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 optimized 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 ensured that TransBrasil was 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 didn'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 allowed it to be a long-term and

cost-effective solution for TransBrasil, as the SIEM could compensate for additional network devices that may be added in the future, and TransBrasil could scale up or down the SIEM and its provisions as needed for their business. Finally, TransBrasil had the option of contracting a third-party MSP to guarantee a smooth and rapid implementation of New-Scale SIEM. Overall, implementing New-Scale SIEM demonstrated 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.

Since TransBrasil's executives wanted a solution implemented as fast as possible, they already decided they were going to use an MSP for the initial setup and continued management and support. This also minimized the amount and severity of problems that came up during the setup process. During this time, the IT department assisted the MSPs in deploying the SIEM and underwent Exabeam official training (Education and Training, 2024) for their eventual takeover of managing the SIEM for TransBrasil. The MSP provided continued maintenance of the SIEM for three months after initial setup. After this time, the IT department and TransBrasil executives decided that the IT department was trained sufficiently to manage the SIEM without the need for an MSP. TransBrasil declined to extend its contract with the MSP, and the IT department took over the monitoring and management of the SIEM.

Each member of the IT department was crucial for the implementation and ongoing support of both the SIEM and TransBrasil's partnership with Vicente Industria. While the SIEM greatly enhanced the IT department's efficiency, its integration also added complexity to the network infrastructure. Combined with the increased business of TransBrasil's new partnership with Vicente Industria, the IT department had to hire more people.

First, the IT department head and TransBrasil's executives established goals for what they wanted the SIEM to accomplish and how it would do so. Then, they met with Exabeam representatives to decide which of their MSP partners would be best for their business (they 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 assessed TransBrasil's current network infrastructure and planned the rollout of New-Scale SIEM in the company.

Second, the IT department and Deloitte used the information gathered from the network infrastructure assessment to design the system architecture and identified log sources to capture data, determined the length of time for data storage, and decided 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 was ample time for them to deploy and evaluate the SIEM's effectiveness. They also developed 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 caused minimal interference to the normal flow of work at TransBrasil. After creating the plans, The IT department and Deloitte got approval from TransBrasil's executives to execute the plan.

Third, Deloitte began the setup of New-Scale SIEM for TransBrasil. They worked with Exabeam to set up the cloud services for the SIEM and log file storage, as well as provisioned user access for the appropriate personnel, such as The IT department and Deloitte service providers. Next, they configured New-Scale SIEM dashboard for local (on-premises) management. Then, they established a high-speed, secure network connection from

TransBrasil's network to the SIEM cloud deployment so that the log files could be captured and sent to New-Scale SIEM for processing and then storage. Finally, Deloitte tested the basic system setup to verify functionality. The IT department head and his second in command oversaw this setup process and took notes while the rest of the department carried out the team's daily tasks.

Fourth, Deloitte did 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 still notified all relevant personnel if any interruptions were going to occur. They used this test to gather feedback on alerts and preliminary SIEM data processing and made adjustments as needed. The IT department head and second in command continued to oversee this process and take notes.

Fifth, after a successful pilot test and configuration, Deloitte proceeded to do a full integration of New-Scale SIEM into TransBrasil's network. This included configuring the SIEM to capture log files fully from both firewalls. Again, the IT department notified all relevant personnel during this time if any interference with normal work was expected to happen. After the full setup, Deloitte monitored the SIEM and log file capturing to fine-tune adjustments. This was to help the AI capture a baseline of what normal traffic in and out of TransBrasil's network looked like and to help reduce false positives in the future. This step took a week to process sufficient logs and evaluate the SIEM's long-term effectiveness. Again, the IT department head and second in command oversaw this process and took notes.

The sixth and final step was ongoing support and training. As stated earlier, Deloitte provided ongoing support for three months after the initial setup of New-Scale SIEM. During this time, they continued to monitor and optimize the SIEM to ensure the best performance for

TransBrasil. While this was ongoing, the IT department went through instructor-led training courses from Exabeam in groups of two so that there were IT personnel left at TransBrasil to handle day-to-day tasks. After training, they worked 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, the IT department took full control of managing the SIEM, and TransBrasil ended its managed service support with Deloitte.

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

Clear and established goals provided a guide for setting up and tailoring the configuration of the SIEM to meet the company's needs. These goals also helped TransBrasil and its IT department to define success criteria and enabled the organization to measure the SIEM's effectiveness. Without clear goals, the SIEM could have been misconfigured and would have failed to address the vulnerabilities that caused TransBrasil to implement the SIEM in the first place. This would have just caused TransBrasil to waste valuable time and resources.

After establishing its goals and doing the preliminary work necessary (selecting a SIEM and MSP), it was important that TransBrasil next developed a plan and implementation process for the SIEM to ensure that it would be configured to satisfy the goals previously

established. This also helped the team to minimize any potential downtime and avoided disruptions to the company, which ensured a smoother rollout.

During the implementation process, it was critical to conduct a test run of the SIEM with a few network resources before doing a full-scale rollout. This allowed 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 was able to identify and address issues early, which reduced the risk of disruptions during the rollout and ensured a smoother implementation of the SIEM.

Review of Other Work

Review of work 1

An article published on TeckPath discusses the impact of AI on SIEM systems. AI has enabled SIEM systems to identify and respond to threats more efficiently by analyzing vast amounts of data in real time. AI has also enhanced event correlation and contextual awareness, which has improved SIEM accuracy and reduced false positives. AI has even allowed SIEM systems to be able to predict potential security incidents by identifying patterns and trends. These improvements by AI have increased SIEM system efficiency so much that they can easily handle larger amounts of data compared to previous-generation SIEMS. Finally, this article also highlights companies that have integrated AI into their SIEM solutions, such as Splunk, IBM Security, Exabeam, Microsoft Sentinel, and many more (Gebremeskel, 2024). This article shows how AI has drastically improved SIEM systems, making them powerful and efficient security tools in today's network infrastructures.

Review of work 2

An article published on Rapid7 outlines three critical steps for a successful SIEM deployment. Before deploying a SIEM, one should gather comprehensive information about their network environment. Second, one should collect and correlate relevant security data to unify it all into one cohesive view. This ensures proper configuration of the SIEM before deployment. Finally, one should leverage the collected data to create dashboards and reports that provide insights into network activity and support compliance requirements. In doing these things, the author states that he was able to deploy a SIEM at his company in days rather than months (Holzer, 2022). This article shows how proper analysis of a network environment, combined with knowing which sources to collect security data from and using the data to create comprehensive dashboards, can significantly shorten the time it takes to deploy a SIEM.

Review of work 3

A blog published on Gurucul discusses the progression of SIEM systems and the emergence of next-generation SIEM systems. The blog starts with the limitations of traditional SIEMs and how the correlation of data was limited to simple grouping by IP address or time. This still caused log file analyses to be time-consuming. As organizations grew and technologies became more sophisticated, traditional SIEMs struggled to handle the vast amounts of data generated in more modern IT environments, showing how those SIEMs struggled with scalability. Traditional SIEMs were also based on static rules-based detection methods, resulting in numerous false positive alerts. This, combined with the complexity of managing traditional SIEMs, showed that traditional SIEMs required significant manual effort to maintain effectiveness. The blog goes on to show that next-generation SIEMs leverage cloud-native architecture and AI to massively improve SIEM performance and reliability and reduce SIEM

complexity (Bhagwat, n.d.). This article shows that while earlier SIEMs had their benefits, they also had drawbacks that would make it understandable for organizations not to be so quick to deploy SIEMs in their IT environments. However, next-generation SIEMs greatly improve on their predecessors, making them a must-have for any IT environment's network security today.

Changes to the Project Environment

At the time of the project proposal, TransBrasil's environment was simple. With the implementation of Exabeam's New-Scale SIEM, TransBrasil's work environment still looks the same on the outside, but it now has a stronger network security posture. Their network infrastructure now has a central security component, placing it in a better position for future expansion. While most TransBrasil employees have not noticed anything different, the IT department has experienced a significant change as they now serve as the trained operators of a new SIEM. This project has helped each member of the IT department improve their IT skills, giving them more confidence in their individual abilities. The entire SIEM implementation process has also boosted the confidence of the team. Following the successful SIEM deployment and the onboarding of Vicente Industria as a partner, the increased workload has necessitated the hiring of two additional IT department employees. The team is confident in its ability to train the new employees to become effective members. The IT department is prepared and excited about future IT projects at TransBrasil. TransBrasil's executives are highly satisfied with the seamless SIEM deployment and confident in their ability to manage the partnership with Vicente Industria, as well as future company collaborations of any size.

Methodology

The Waterfall Method was the best methodology for implementing Exabeam New-Scale SIEM. It is a structured, step-by-step process that follows a linear, sequential approach, which

was crucial for making sure the SIEM was implemented properly and functioned as intended. The rigidity of the Waterfall Method also ensured that each step of the SIEM implementation process stayed 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 were to identify security goals and any compliance requirements. TransBrasil had 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 also identified their data sources for collection, such as firewalls, servers, and applications. After that, they established log retention time periods and reporting

needs. Finally, this phase was completed once final approval from the TransBrasil executives was given for the scope of the SIEM project.

In the design phase, the major milestones were centered around designing the architecture of New-Scale SIEM. Since they already knew what SIEM they would be using and how it would be managed, the IT department worked with Deloitte service providers to carry out this process. Major milestones included 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 contributed to the overall configuration of the SIEM. Finally, this phase was completed once final approval from TransBrasil executives was given for the design plans.

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

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

Finally, in the maintenance phase, the full rollout of New-Scale SIEM was established. Ongoing monitoring and performance of the SIEM began. Deloitte service providers switched from installation tasks to ongoing performance and monitoring tasks and performed configuration changes as necessary to maintain SIEM adherence to established goals and for optimization purposes. The IT department went through Exabeam training and took over New-Scale SIEM monitoring and maintenance after the three-month period ended. Although maintenance is an ongoing process for the entire SIEM lifecycle, this phase was completed once The IT department took full control of the SIEM and the Deloitte service providers were dismissed.

Project Goals and Objectives

The following table breaks down the project goal into objectives and their corresponding deliverables, including whether the deliverables were met or not.

	Goal	Supporting objectives	Deliverables enabling the project objectives	Met/Not Met
1	Improve Network Security	1.a. Implement a SIEM .	1.a.i. Contract with MSP for Exabeam SIEM setup and ongoing support.	Met
			1.a.ii. Draft SIEM design plans	Met
			1.a.iii. Implement the SIEM.	Met
			1.a.iv. Validate SIEM functionality and performance before conducting the full rollout.	Met
		1.b. Train the IT department to manage the SIEM.	1.b.i. MSP shifts from initial setup to SIEM monitoring and ongoing support.	Met
			1.b.ii. Entire IT department completes Exabeam training.	Met

			1.b.iii. IT department takes over SIEM monitoring and maintenance, and MSP is dismissed.	Met

The overall project goal was to improve TransBrasil's network security. Their previous way of manually scanning log files was a network vulnerability that needed to be addressed. The two objectives to accomplish this goal were to implement a SIEM and to train the IT department to manage the SIEM. A SIEM allowed TransBrasil to automate the data collection, analysis, and threat detection processes. This, in turn, made for a stronger, more secure network. The IT department also needed to be trained on how to manage the SIEM. A SIEM is only effective if properly configured and maintained, making it essential that TransBrasil's IT department received the necessary training for its ongoing management and lifecycle support. The goal of improving TransBrasil's network security was achieved because of the two objectives. The SIEM was successfully implemented after the Waterfall Method was used to gather SIEM requirements, design an implementation plan, deploy the SIEM using the plan, verify its functionality, and establish ongoing maintenance and optimization of the SIEM. The IT department received training to manage the SIEM by completing Exabeam training after the MSP shifted from setup duties to monitoring and ongoing support duties. After training, the IT department successfully took over SIEM monitoring and management, and the MSP was dismissed. The simplicity of TransBrasil's network infrastructure and the expertise of Deloitte's MSP team allowed the successful implementation and management of New-Scale SIEM with only a few minor impacts to network performance during the implementation process. There were no major issues or challenges throughout the entire process. With a fully functioning SIEM and a properly trained IT department to manage it, TransBrasil successfully improved its network security.

Project Timeline

Milestone or deliverable	Duration (hours or days)	Projected Start Date	Projected End Date	Actual Start Date	Actual End Date
Contracting with an MSP for SIEM services	7 Days	2/17/2024	2/23/2024	2/17/2024	2/22/2024
Approval of SIEM requirements	7 Days	2/24/2024	3/1/2024	2/24/2024	3/1/2024
Finalized and approved SIEM design plans	7 Days	3/2/2024	3/8/2024	3/2/2024	3/8/2024
Successful completion of SIEM setup and initial configurations	7 Days	3/11/2024	3/17/2024	3/11/2024	3/17/2024
Successful testing followed by full SIEM deployment	14 Days	3/18/2024	3/31/2024	3/18/2024	3/31/2024
Handover of ongoing SIEM monitoring and support to IT department	91 Days	4/1/2024	7/1/2024	4/1/2024	7/1/2024

For the first milestone contracting with an MSP (Deloitte) for SIEM services, the actual completion date was a day earlier than the projected end date due to TransBrasil's small size as a company and the simplicity of its network. However, due to this being a contract, Deloitte service providers could not start work until the first day of the contract. The next four milestones, approval of SIEM requirements, finalizing and approving SIEM design plans, successful completion of SIEM setup and initial configurations, and successful testing followed by full SIEM deployment all took their entire respective times, using all available time to ensure that all goals and plans were thoroughly developed and SIEM setup, configuration, and testing were as thorough as possible. Finally, the handover of ongoing SIEM monitoring and support to the IT department also took all allotted time, as the three months of ongoing support were a contractual obligation with Deloitte.

Unanticipated Scope Creep

TransBrasil's IT environment was already modern. The simplicity of TransBrasil's network, combined with modern computers, operating systems, software, and the fact that no extra SIEM software was necessary for end-user devices, made them the perfect candidate for a seamless SIEM integration. In addition, since New-Scale SIEM and data storage are operated in the cloud, there was no need for extra hardware on the premises for TransBrasil. Exabeam's SIEM software was able to be installed without issue on all IT computers and relevant servers because they were already running the latest software. The use of an MSP for SIEM deployment and continued support meant that TransBrasil had industry professionals for the SIEM deployment serving to mitigate any issues that would have caused any unanticipated scope creep.

Conclusion

In conclusion, this project aimed to enhance network traffic monitoring for intrusion detection, replacing the tedious and inefficient process of manually scanning log files. Manual

analysis is slow and may fail to detect threats in time, leaving organizations vulnerable to cyberattacks and data breaches. A SIEM automates data analysis, enabling real-time threat detection and response. With advancements in cloud technology, modern SIEMs offer faster, more cost-effective security solutions, making them accessible even to small organizations. As a result of this SIEM implementation, TransBrasil's network security posture has increased tremendously. They now have a powerful tool that centralizes their ability to detect and respond to threats, allowing them to be more proactive in threat detection monitoring. Due to the thorough planning and SIEM deployment by trained professionals (Deloitte service providers), the SIEM deployment was successful. This is evidenced by the SIEM's metrics after implementation at TransBrasil. Since New-Scale SIEM's post-implementation and validation, it has been able to consistently and immediately detect potential breaches through simulated attacks, generating alerts while the threats persist. The SIEM has also been able to do this while under a simulated increased network load. Finally, the low number of false positives shows that after months of data collecting and processing, New-Scale SIEM's AI processing has adapted to TransBrasil's network traffic flows enough to have achieved a solid and reliable baseline to distinguish potential threats from normal network traffic.

References

Bhagwat, A. (n.d.). The Evolution From SIEM to Next-Gen SIEM. Gurucul. https://gurucul.com/blog/the-evolution-of-next-gen-siem/

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

Gebremeskel, B. (2024, September 4). How AI is Revolutionizing SIEM in 2024. TECKPATH. https://teckpath.com/how-ai-is-revolutionizing-siem-in-2024/

Holzer, R. (2022, September 27). How to Deploy a SIEM That Actually Works. Rapid7. https://www.rapid7.com/blog/post/2022/09/27/how-to-deploy-a-siem-that-actually-works/

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

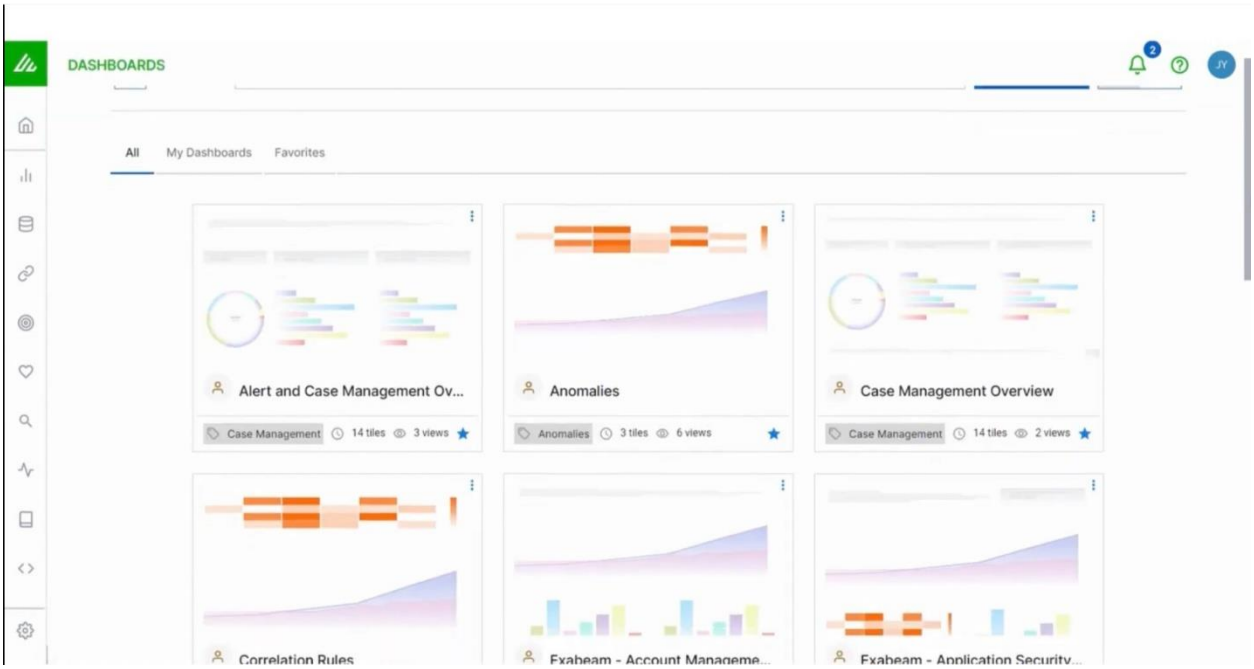
New-Scale SIEM. Exabeam. (2025, January 7). https://www.exabeam.com/platform/new-scale-siem/

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

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

Appendix A

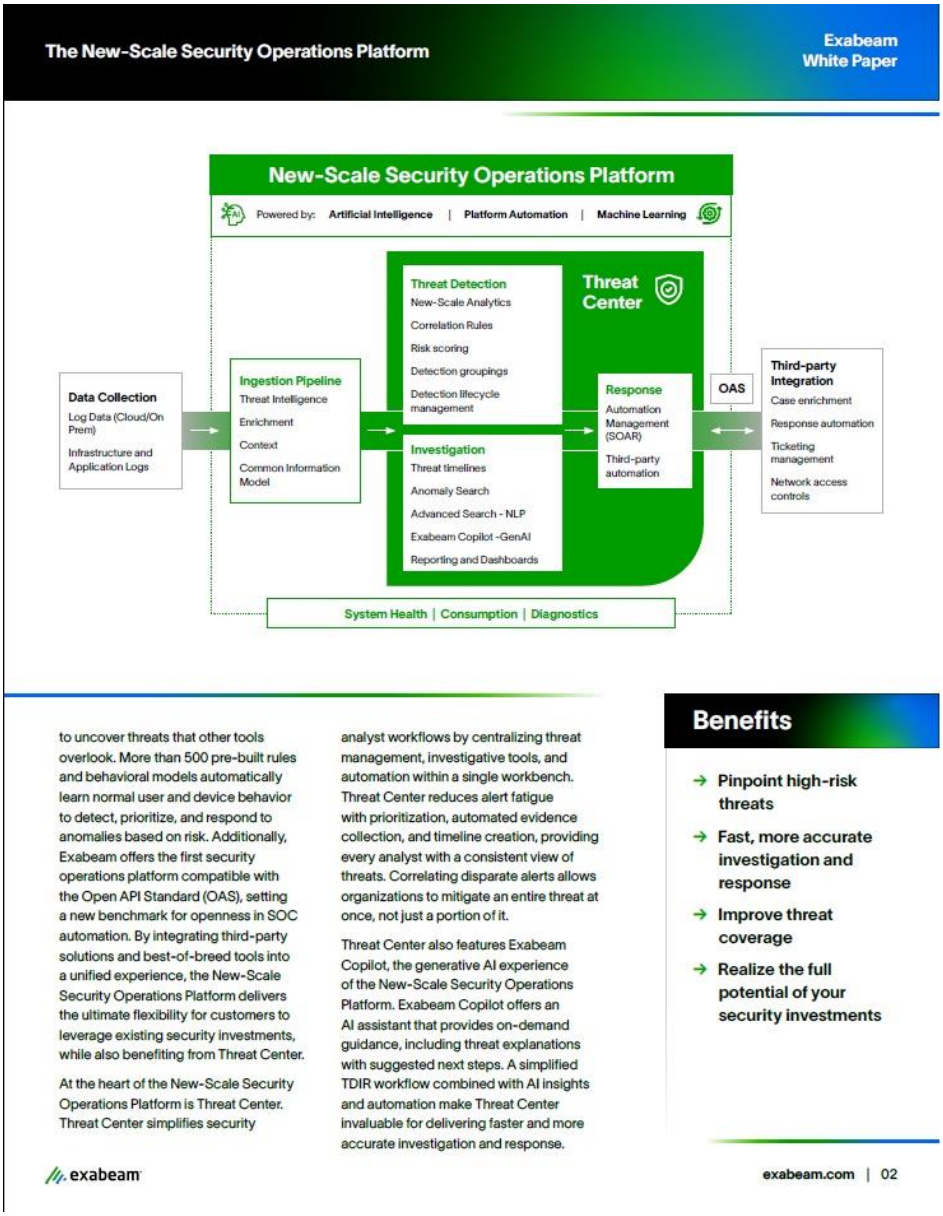
Exabeam Dashboard



Appendix A is an example of Exabeam's Dashboard. This picture shows a dashboard similar to what TransBrasil's IT department would see on their computers when managing New-Scale SIEM.

Appendix B

Exabeam Data Sheet Excerpt



Appendix B is an excerpt from Exabeam's Data Sheet explaining how its New-Scale SIEM operates the New-Scale Security Operations Platform. The graphic shows the process of how New-Scale SIEM collects data and processes it for threat detection, investigation, and response. This is how TransBrasil's data is collected by New-Scale SIEM and processed, providing real-time threat detection capabilities.

Appendix C

Exabeam and Google Cloud Brief Excerpt

Appendix C is an excerpt from a brief by Exabeam and Google Cloud. It shows how the partnership between Exabeam and Google has allowed Exabeam to provide a cloud-based SIEM solution and its advantages. TransBrasil is using these cloud services to provide a centralized security suite for its own network.