



Case Study

CASE STUDY | BANK PLUS

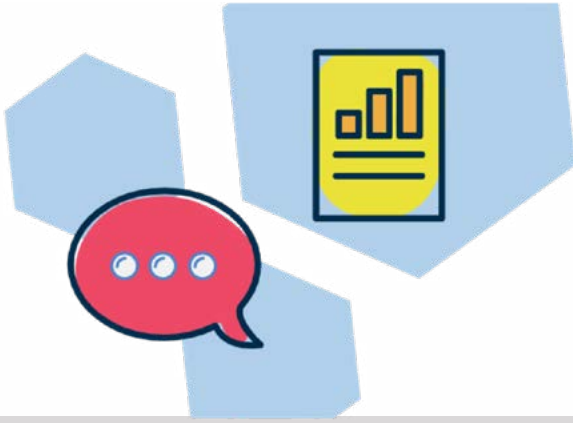
BankPlus has been leveraging Castra's Elite Managed Service and ELK Logger since 2019. The financial institution was utilizing a SIEM but struggled to use the security tool to its full potential. With the retirement of Bank Plus' Chief Technology Officer and their Director of Information Technology within a close time frame, the need for a vendor that had expert level experience in Security Operations, Threat Detection, and SIEM Management all while being affordable and transparent was paramount.



BankPlus initially engaged Castra's services in a consultative capacity after reviewing the Castra Cost-Benefit Analysis. BankPlus had a few needs. First, there was a need for a long term, on-premise logging solution as their SIEM's storage was continually filling with unorganized data. Second, they needed to tune their SIEM to see important security alerts, and third is that they needed the expertise to manage this whole process on a 24x7 basis and respond to threats accordingly.

After their first engagement, BankPlus immediately saw Castra's value and expertise because their SIEM was finally functioning as it should. By leveraging Castra's expertise and Castra's ELK Logger, ElasticSearch, and their SIEM were configured correctly and escalating alarms when was truly appropriate, thus providing accurate security visibility into their environment. This impressive improvement inspired BankPlus to engage Castra's Elite Managed Service to implement this level of ongoing industry knowledge and expertise 24x7 in their Information Technology Department.





BANKPLUS | THE RESULTS



RESULTS

- Saving BankPlus' existing SIEM prevented **“rip and replace” costs**
- True 24x7 security visibility within the BankPlus environment for a fraction of the cost of **1 full-time employee**
- **ELK Logger** allows for easy growth, fast search speeds, and unlimited flexibility
- An outsourced SOC **saved BankPlus significant time and money**, taking the pressure off internal staff



Castra has assisted BankPlus in both building and supporting a scalable big-data platform for our log management and cyber-visualization needs. This has allowed internal technology and risk teams to place time and resources on other critical areas of the organization. Castra has been a true partner, and a real extension to our team. Their SIEM and Security Operations knowledge has been, and continues to be very impressive. They add value to our team and we look forward in continuing to work with them on current and future projects. We would gladly recommend working with Castra.

- Todd Stringer | Vice President & Information Security Officer

Ultimately there are two paths to achieve a strong Information Security posture. Build it in-house, or outsource it. Both options have their pros and cons. On the following page is a SOC Cost-Benefit Analysis to outsource managed security services or build a security team in-house.



Case Study

BANKPLUS | SOC COST ANALYSIS

CASTRA MANAGED SERVICES Average Cost \$48,000/year		VS	ONE FULL-TIME EMPLOYEE Average Cost \$77,665/year	
<i>Pros</i>	<i>Cons</i>		<i>Pros</i>	<i>Cons</i>
Castra Founders have a combined 35+ years of Information Security Experience	OUTSOURCED		IN-HOUSE	Limited Security Operations Experience
US-Based, Diligent SOC Analysts, Mastered Several SIEM Platforms & Information Security Products			EXCLUSIVE TO YOU	Limited SIEM Experience
Leading Partner with Multiple Vendors				Might need SIEM and Incident Response training <i>(more time and money)</i>
SOC2 Type I, Type II Certified				Sick Days
Written Custom Xode, Correlation Rules, & Plugins by the Hundreds				Company Benefits Add More Costs
15,000 SQ FT, 24x7x365 Security Operation Center and team				Limited 40 - 50 Hour Work Week
Currently Managing Several Large & Medium Worldwide Organizations in All Types of Industries				2 Weeks Vacation
Cost is Predictable and Constant				Cost Increases Over Time

