UKRSIBBANK

SOC Prime has helped UKRSIBBANK to reduce time for detection and mitigation of threats and increase the productivity of the company’s InfoSec department.

Industry	Region	Company Size	SIEM & XDR in Use
Banking	Eastern Europe	Up to 10,000 employees	Splunk, Elastic Stack, ArcSight

Maxim Yashchenko
Head of Infrastructure Security and Training Control Unit of Information Systems | Security Department at UkrSibbank

> *"Aiming to gain the maximum of the Information Security department, the Bank reached out to SOC Prime for consulting and finally bought a subscription for the Threat Detection Marketplace, platform for sharing analytical content. The subscription enabled us to significantly decrease workload of the department employees for creating the analytical content, and put their efforts into investigation of the detected incidents. New valid use cases and detection queries are continuously added to TDM, which gives us an opportunity to minimize time for detection and mitigation of threats."*

Highlights

- Streamlined delivery of custom use cases tailored to the industry’s needs, including compliance-specific detection content and incident response scenarios
- Reduced SOC team’s workload on threat detection content research and development
- Enabling proactive defense against constantly growing digital threats
- Overcoming the challenges of cross-SIEM content translations with the Uncoder.IO universal Sigma rule converter

Challenges

The dynamic threat landscape requires significant efforts from security practitioners to let them constantly keep up with the rapidly changing attack vectors. Top companies in various industries, including the financial sector, are facing a lack of SOC team resources for the development of threat detection content while the number of attacks is growing at a dynamic pace. A lot of research needs to be done to cover all recent attacks that are getting more sophisticated with the advance of new technologies used by threat actors. All this has shaped the primary concern of UKRSIBBANK related to the substantial workload of the Information Security department and time restrictions on the research and development of high-quality threat detection content.

UKRSIBBANK was looking for ways to streamline the incident response activities and timely react to all external and internal attacks. Proper coverage of these security operations requires hiring a team of SOC specialists with solid expertise in the field that involves significant financial investments. According to the latest reports, a lot of market leaders are lacking in highly experienced staff in cyber security on the global market, and the financial sector is in dire need of such human resources to withstand the attacks.

One more point that required improvements was maintaining cyber security compliance and automating controls across all regulatory standards. UKRSIBBANK as a PCI DSS compliant financial organization wanted to obtain specific detection content that would meet the related security requirements.

Solution

Joining the SOC Prime Threat Detection Marketplace (TDM) has helped UKRSIBBANK to obtain SOC content without the need to hire an in-house team of threat hunters and spend significant financial and time resources on their recruitment and maintenance. Leveraging the Premium TDM subscription, UKRSIBBANK has gained an external team of seasoned security professionals who are constantly researching the situation on the market from the cyber attack perspective. SOC Prime team delivers their clients a great deal of detection rules and threat detection scenarios that allow identifying threats at the earliest stages of the attack lifecycle when the company is still unaware of its vulnerabilities.

The SOC Prime's platform is being constantly enriched with new threat detection content that resonates with the latest attack vectors. The company is enhancing the platform capabilities on an ongoing basis and is flexible when it comes to changing the content priorities to meet the customers' expectations. Security practitioners are welcome to request content that is most relevant to their company's needs, and the members of SOC Prime Team in collaboration with Threat Bounty developers, SOC Prime's crowdsourcing initiative, are delivering new rules, queries, and parsers that fit the company's threat profile and regulations, including compliance-specific detection content for the financial sector.

The development of incident response scenarios is a very tough process that requires a lot of human resources. The SOC Prime Threat Detection Marketplace delivers basic scenarios implementing best security practices that can be applied regardless of the company structure and technologies in use. UKRSIBBANK has mainly used ArcSight, Splunk, and the Elastic Stack analytics-based SIEM solutions, and the cross-platform content from the world's largest Threat Detection Marketplace can be adjusted to various environments based on the company's preferences. With the embedded Uncoder.IO translation tool, detection rules can be easily converted to various SIEM and XDR formats, which solves the problem of migration to another back-end environment.

Achievements

Proactive Approach to Threat Detection

With the SOC Prime Threat Detection Marketplace, UKRSIBBANK has managed to save time, money, and human resources that were required to deliver proactive threat detection. UKRSIBBANK has gained access to the world's largest SOC content repository that is constantly growing and updated, enabling the company to stay informed on the latest threats.

Accelerated Delivery of Custom Use Cases

SOC Prime curates custom detection and response algorithms tailored to the industry-specific threat profile, enabling UKRSIBBANK to obtain the most relevant content faster and more efficiently than before, including compliance-specific use cases and incident response scenarios. Backed by prolific contributions from Threat Bounty Program researchers and content developers, the Threat Detection Marketplace content base continuously provides UKRSIBBANK with the most up-to-date curated content matching the organization's threat profile and compliance needs.

Cross-Platform Content Translation

SOC Prime enables on-the-fly translations to multiple SIEM and XDR language formats and continuously enriches the number of supported platforms. This helps UKRSIBBANK to smoothly convert detection content to the majority of analytics platforms in use, including ArcSight, Splunk, and the Elastic Stack, overcoming the migration challenges to a different environment.

Next-Gen Cyber Defense Capabilities

Being a member of the Microsoft Intelligent Security Association (MISA), SOC Prime is constantly developing new ways to boost cybersecurity tools and operations for security teams that is a driving factor for ongoing partnership. What can be seen as further steps in the company's partnership with SOC Prime is obtaining more compliance-specific content with relevant tagging for a more targeted content search and prioritizing the list of rules according to the company's region and industry.

About UKRSIBBANK

UKRSIBBANK was founded in 1990 and quickly evolved from a regional bank to a national market leader. In 2006, UKRSIBBANK started its strategic partnership with one of the world's industry-leading banking groups, BNP Paribas, that has become the principal shareholder of UKRSIBBANK. BNP Paribas is a global leader of the financial market, one of the world's largest financial groups being present in about 80 countries. The Bank's integration with BNP Paribas Group has opened a set of new prospects, such as association with a global brand, best financial practices, and transition to new management standards. The efficient growth of the Bank is supported by its development in all market segments. UKRSIBBANK currently serves about 2 mln retail clients.