Overseen by the Ministry of Entrepreneur Development and Cooperatives (MEDAC) of Malaysia, the Urban Development Authority (UDA) is a property developer that manages and operates real estate as well as provides services for housing, lifestyle, retail, and hospitality sectors. Renowned as one of the top ten property developers in the market, UDA has played an instrumental role in the development of Selangor, Kuala Lumpur, Penang, Johor, and more. To improve the developer’s overall security posture and gain visibility into its extended IT landscape, UDA has chosen LogRhythm NextGen SIEM Platform.

The Business Challenge

BLIND SPOTS IN CYBERSECURITY

As a company that is responsible for many governmental, commercial, and residential property development projects throughout Malaysia, it is imperative for UDA to ensure that their data, clients’ information, and assets are well protected. However, not only did the cybersecurity team lack the resources, they also lacked the experience and expertise to adequately handle the volume and complexity of both external and internal threats to UDA.
In other words, the team had been unnecessarily spending a substantial amount of time and resources manually detecting threats, which include DDoS, ransomware, brute force, and phishing attacks. Additionally, this manual detection—in the blind—also meant that it was harder to differentiate between real threats and false positives, resulting in a huge impediment to their ability to respond and remediate cyberthreats in the shortest possible time. Eventually, their ability to satisfy compliance regulations was also impacted.

Consequently, the team realized that they needed a security information event management (SIEM) solution that could enhance and centralize visibility, detect advanced threats, and respond to incidents effectively around the clock.

The Solution

FULL VISIBILITY

Following an evaluation of cybersecurity vendors, UDA selected LogRhythm for its ease of deployment and use, user interface, and out-of-the-box content for threat detection and compliance. Recognized for its leader’s position in the Gartner SIEM Magic Quadrant, LogRhythm also surpassed its competitors in terms of scalability, cost-effectiveness, and
customer-focused support system that enabled the UDA team to hit the ground running quickly. In fact, it only took an hour for UDA's IT engineers to understand and familiarise with LogRhythm’s dashboard, which did not require any advanced scripting skills in order to manage it.

Since working with LogRhythm, UDA has gained full visibility into their network and system—of internal and external threats—enabled by threat intelligence. Their efficiency and accuracy have also increased, as they were able to dial back on addressing false positives, and instead focus on real threats that were of high priority.

REDUCED DETECTION AND RESPONSE TIMES

Given the vast landscape of data and information UDA holds, the large organization needs to ensure that they can identify threats attempting to hide within that maze of information swiftly. With LogRhythm's RespondX, UDA was able to streamline the investigation and mitigation of threats by coordinating and automating as many steps in the response workflow as possible. This means greater efficiency and speed in detecting and responding to anomalous activity, thus minimizing damage to the business.

Coupled with having full visibility on the origin of attacks and security environment, the UDA team found additional value in the platform, which served as the central repository for all associated evidence and case management. This immensely helped the UDA team’s time management on tracking and remediating cases, as they were able to view a real-time news feed of all completed actions associated with a timestamp for each case. In fact, by aligning their processes with LogRhythm NextGen SIEM, the team was able to cut down on mean time to detect and response times from between 48 and 72 hours to just under 30 minutes.

ORCHESTRATING WORKFLOWS INTELLIGENTLY AND SWIFTLY

The adoption of LogRhythm’s NextGen SIEM solution has strengthened UDA’s ISO 27001:2013 certification application, which is now in process. It covers various areas in incident response and information integrity through a unified hub orchestrating workflow. The positive results and achievements with LogRhythm have led to UDA placing the platform at the center of its security IT universe, with the IT team looking at closer collaboration efforts for a 24/7 Security Operations Centre (SOC) and the possible inclusion of cloud deployment.

“We’ve adapted extremely well to LogRhythm NextGen SIEM solution and were able to pinpoint specific threat actors. Going on board with the solution was a breeze for our team members, who all had general cybersecurity expertise. Since working with LogRhythm, we have been able to rapidly identify behavioral anomalies and significantly accelerate threat mitigation, thereby reducing mean time to detect (MTTD) and mean time to respond (MTTR). The ease of use with LogRhythm NextGen SIEM Platform has led to our Application Support Team gaining more interest in Security Operations Center (SOC) and proactively honing their skills as part of their career development. Following our success with LogRhythm, we will be looking at securing the cloud and automating processes to raise our security posture to the next level.”

Abdul Yamin Ab Ghani
UDA Holdings Group
Assistant Vice President 3
Head of Information Technology
Infrastructure