LOGICALIS
Architects of Change

CASE STUDY

Logicalis racks up comprehensive and speedy incident response with Cortex XSOAR

XSOAR reduces response time significantly—90-95% incidents resolved through automated playbooks

paloalto NETWORKS

IN BRIEF

Customer

Logicalis Singapore

Product and Services

IT solutions and managed services

Industry

High tech

Organization Size

> 150

Country

Singapore

Website

https://www.ap.logicalis.com/

Challenges

Logicalis wanted to offer threat detection and response capabilities to their customers in Asia. The company also wanted to increase efficiencies in its security operations center (SOC) through automation.

Requirements

+ Provide differentiated services to compete with best-of-breed service providers.
+ Offer threat detection and response capabilities by reducing attack surface.
+ Expand service portfolio as a SOC through automation.
+ Gain the benefits of faster resolution and end-to-end services, fewer incidents and more efficiency within their own SOC.
+ Deploy a vendor-agnostic solution to integrate and pair with existing cybersecurity solutions.

Solution

They chose Palo Alto Networks Cortex XSOAR, the industry's most comprehensive security orchestration, automation, and response (SOAR) platform.

Logicalis is an international solutions provider of digital services currently accelerating the digital transformation of its 10,000 customers around the world. As a global managed security service provider (MSSP), the company has multiple Global Security Operation Centers (GSOC) in Singapore, Jersey Channel Islands, Brazil, and Argentina, each handling its regional customers security operations.

Sai Kumar, Senior Manager, Security Services, oversees GSOC for Asia region with a lean team of five people. Sai and his team wanted to bolster their position across two levels. Firstly, as a regional service provider, they wanted to offer both threat detection and response capabilities to their customers. They also wanted to hasten the implementation of required recommendations and help customers remediate any potential threats in a timely manner. Secondly, they wanted to increase the efficiencies within their own SOC by exploring SOAR technologies.

CHALLENGE

Providing differentiated services to compete with best-of-breed service providers calls for new technologies

Sai and his team set out to streamline their existing services where Logicalis aids in the detection of cyberthreats and provides appropriate recommendations. While the SOC team conducts a thorough analysis of attacks and provides recommendations, the implementation of remediation actions was typically done at the customers' discretion. Given that a significant number of Logicalis customers are from small-to-mid-sized businesses (SMBs)—often with lean security teams that do not necessarily work on a 24/7 model—they had neither the bandwidth nor resources at their disposal to perform recommendations given in a timely manner. From a cybersecurity perspective, fast detection, implementation,

and response are key and something that Sai wanted to change. "Logicalis wanted to provide end-to-end services for our customers, from detection of a cyberattack and to implement changes in (near) real time, through customer-agreed procedures and processes," he says. This strategy would minimize the attack surface for the customer and also help differentiate Logicalis from best-of-breed service providers in the market.

On another level, Sai wanted to increase the efficiency within his own SOC. It was not practical to scale the number of people within the SOC alongside the business expansion. A keen advocate of automation, Sai wanted to automate mundane and repetitive tasks that were time-consuming. He knew that harnessing the power of automation would free up the time of his analysts, enabling them to direct their focus on more complex and skilled tasks that required their expertise.

REQUIREMENTS

SOAR technologies automate instant response and increase SOC efficiency

To achieve the dual goals of helping customers detect cyberattacks and implement recommendations as well as increasing the efficiencies of the SOC, Logicalis began delving into SOAR technologies. The solution that they were looking at needed to meet the following criteria:

- **Provide differentiated services** to compete with best-of-breed service providers in the market.
- **Offer threat detection and response capabilities** to customers by reducing attack surface.
- **Ensure expansion of service portfolio** as a SOC through automation.
- **Increase efficiency within own SOC** through faster resolution, end-to-end services and fewer incidents.
- **Vendor-agnostic solution** that can integrate with and complement other cybersecurity solutions for ease of management.

> "Logicalis wanted to provide end-to-end services for our customers, from detection of a cyberattack and to implement changes in (near) real time, through customer-agreed procedures and processes."
>
> **— Sai Kumar, Senior Manager, Security Services, Logicalis Asia**

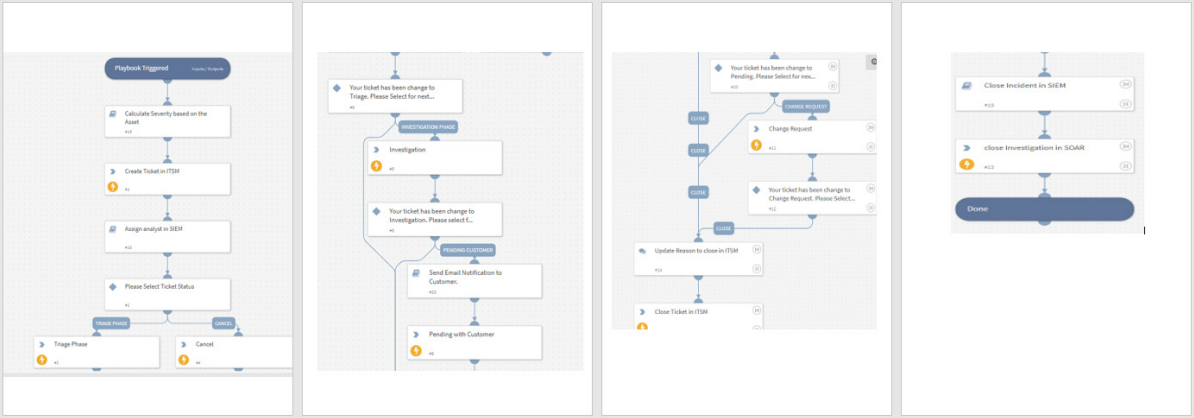
SOLUTION

A customisable solution with built-in threat capabilities leads the way

Logicalis began to scout for SOAR technologies in the second half of 2020. It was imperative that the solution they opted for would integrate seamlessly with existing technologies within the organization. The onset of the pandemic also boosted the need to work remotely and collaboratively; the chosen SOAR solution had to be one that analysts could adapt to easily. The company called for a demo session and conducted a comprehensive proof of concept (PoC).

Besides being vendor-agnostic, Palo Alto Networks Cortex® XSOAR was the most comprehensive SOAR platform as the solution could be integrated with the existing security information and event management (SIEM) tools Logicalis had in place. In addition, Cortex XSOAR did not require any additional skill training for the analysts' team at Logicalis. With 700+ out-of-the-box integrations and the rich library of playbooks that cater to organization-wide use cases, Logicalis was able to easily select and customize the playbooks for suitable business use cases with built-in threat intelligence capabilities.

Sai explains, "Logicalis has established a strong partnership with Palo Alto Networks regionally, and we felt supported throughout our enablement process, especially when we required additional help in creating customized playbooks." Since then, all known issues have been automated, and the team at Logicalis can focus on working on new incidents now.



Example of one of the more than 700 playbooks

> "The fundamental requirement was ease of operations. Palo Alto Networks Cortex XSOAR demonstrated capabilities to customize playbooks during the user acceptance testing (UAT). The success of the playbooks created by the Palo Alto team during the proof of concept (PoC) was unmatched and steered us towards picking their solution ultimately."
>
> **— Sai Kumar, Senior Manager, Security Services, Logicalis Asia**

BENEFITS

Automating 90-95% repetitive SOC incidents

Since having Cortex XSOAR deployed for approximately six months, it has completely taken over the entire security operations tasks that used to be done by L1 analysts. This means that repetitive incidents and the incident triage (e.g., basic sanity check, creating tickets, updating, closing tickets, data enrichment) are all automated. Alerts related to authentication, firewall denials, audit failures, login failures, and such are all automated. Logicalis has even offloaded the task of calling standby engineers for critical incidents to the Cortex XSOAR playbook, reducing the need for overtime by standby engineers. Today, minimal involvement is required from the analysts.

Significant time savings and increased productivity

Prior to deployment of the Palo Alto Networks solution, Logicalis analysts would receive an average of 40-50 alerts per shift, which would take the analyst between 30-45 minutes end to end (including ticket creation, sanity checking, data enrichment, drafting an email, and escalation). With the automation provided by Cortex XSOAR, this takes minutes now. SOC analysts can not only work on incidents but do more high-value work like creating customized reports, building use cases, and spending time with customers to understand their pain points to recommend and deploy suitable solutions. This not only enables better relationship-building practices but allows the analysts to focus on high-value tasks and continuously build their skillset.

Future-ready with Cortex XSOAR

By investing in Palo Alto Networks Cortex XSOAR, Logicalis has now differentiated itself from the competition. Many customers are aware of SOAR technologies and are increasingly looking at partners who can swiftly resolve the issues they are faced with. The company is looking at making Logicalis' SOAR as a service available to existing and prospective customers by providing them with an affordable option instead of making investments to automate and upskill their own SOCs.

> "The level of support provided by the Customer Success team is unrivaled, and the [Cortex XSOAR] playbooks created have brought us immediate and tangible benefits, which we did not think was possible."
>
> **— Sai Kumar, Senior Manager, Security Services, Logicalis Asia**

CONCLUSION

Going forward, Logicalis is considering extending the SOAR capability to its other GSOCs and is looking at replicating similar automation in other regions worldwide. To sum things up, Sai says, "We have been pleasantly surprised by the extensive support that we have received from the customer success team at Palo Alto Networks." The team at Logicalis was unfamiliar with SOAR, but when they embarked on the XSOAR journey with Palo Alto Networks, they were brought up to speed in no time at all. He goes on to say, "The level of support provided by the Customer Success team is unrivaled and the playbooks created have brought us immediate and tangible benefits, which we did not think was possible." Logicalis Singapore has exemplified a high-functioning and effective SOC for the rest of the company's GSOCs and aims to extend the collaboration between the two companies in the years to follow.

paloalto NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com