SITE
الشركة السعودية لتقنية المعلومات
Saudi Information Technology Company

CASE STUDY

Automation-first managed detection and response centre helps Saudi Information Technology Company provide best-in-class services

Saudi Information Technology Company (SITE) are guiding their country's digital and cybersecurity services to a secure future. Palo Alto Networks Cortex XSOAR is the cornerstone of SITE MDR's innovative, fast-growing managed security service, which supports 150+ clients across Saudi Arabia. By monitoring, detecting, and responding to cybersecurity threats more quickly and effectively, SITE are helping clients enhance their security postures to withstand advanced attacks.

paloalto NETWORKS

IN BRIEF

Customer
Saudi Information Technology Company (SITE)

Services
Comprehensive array of secure digital services and solutions

Country
Riyadh, the Kingdom of Saudi Arabia

Industry
Technology

Organisation Size
150+ clients, 8+ partners, 20+ products

Challenges

SITE required a trusted, mature platform to automate alerts processing for their fast-growing MDR service. Analysts devoted excessive time to data collection and determining false positives. SITE analysts needed more time to focus on decisions, and to devote less time to reactive security responses. SITE MDR needed to save budget and resources while delivering high-quality services to clients.

Requirements

- Automate repetitive tasks.
- Triage security incidents faster with automated investigation and response.
- Increase productivity, efficiency, and accuracy.
- Strengthen defences by connecting workflows across teams and tools.
- Achieve parallelism by carrying out multiple tasks simultaneously while using less resources.
- Standardise investigation approach to reduce human errors.

Solution

Palo Alto Networks Cortex XSOAR

CHALLENGES

Protecting the Kingdom's critical digital assets

Saudi Information Technology Company (SITE) provide secure-by-design digital services and cybersecurity solutions – delivered by Saudi professionals – that protect the Kingdom's critical digital assets. These products and services have made SITE a critical partner for major government organisations, private sector, and national entities.

SITE provide innovative, reliable digital and cybersecurity services and solutions – and develop future technologies – to address needs, aspirations, and threats while fostering an entrepreneurship ecosystem and developing a highly talented pool of Saudi human capital.

Saudi Arabia has a knowledge-hungry economy. Digital transformation is disrupting traditional processes, bringing agility, innovation, and rapid change to commercial and government services. SITE are adapting to this new era, boldly reimagining the way they support central and local entities with modern, trusted cybersecurity solutions.

SITE's Managed Detection and Response (MDR) centre is the heartbeat of this strategy, providing more than 150 clients across the Kingdom with modern, 24x7, remotely delivered security operations centre (SOC) services. MDR is a turnkey, rapidly provisioned, threat-centric SOC that improves the security postures of subscribers from day one. With a diversified technology stack of five main platforms deployed at clients' sites, covering host, network, applications, and analytics, and a cohesive matrix of more than 20 supporting cybersecurity-focused technologies, MDR is supercharged with a rich, well-designed ecosystem focused on sophisticated delivery.

Security orchestration, automation, and response (SOAR) was engraved into the MDR service manifesto right from the start. Until the ideal solution was found, SITE MDR started developing in-house tools and standalone script as short-term fixes to provide the automation necessary to keep up with the MDR service's rapid growth.

> Our mission is to create a secure digital world for our clients. We were receiving up to 1,200 alerts per day, and as demand for SOC services grew, we could no longer rely on manpower. SITE MDR needed a smart, intelligent automation solution to consistently deliver high-quality services.
>
> **–SOC Operations Manager, SITE MDR**

REQUIREMENTS

Triaging security incidents faster

SITE needed a trusted partner to support their best-in-class MDR service. They identified that a solution would be required to:

- Automate repetitive tasks.
- Triage security incidents faster with automated investigation and response.
- Increase productivity, efficiency, and accuracy.
- Strengthen defences by connecting complex workflows across the team and tools.
- Achieve parallelism by carrying out multiple tasks simultaneously with less resources.
- Standardise the investigation approach to reduce human errors.

SOLUTION

"A security design masterstroke"

A Palo Alto Networks Cortex XSOAR trial convinced the Lead Automation Engineer and her team that the platform offered the multitenancy, flexibility, and mature functionality to meet SITE MDR's needs. "XSOAR is a security design masterstroke," she says. "The integrations are fast and simple, and the workflow to build playbooks is incredibly intuitive – not to mention the high flexibility it provides. We simply create an object and link it to a use case. A malware analysis playbook, for example, can be reused for another use case with minimal configuration."

SITE MDR is staffed with highly skilled analysts and engineers, distributed across Tier 1 to Tier 3 in the monitoring team and other dedicated teams – automation, threat hunting, content creation, and administration.

The Lead Automation Engineer is rightly proud of SITE MDR's XSOAR deployment.

> This is much more than straightforward alert hunting. XSOAR supports everything from incident response and alert management through to escalation, facilitating client communication, and reporting – in one unified, best-in-class platform.
>
> **–Lead Automation Engineer, SITE MDR**

On a typical day, SITE MDR will receive up to 1,200 alerts, raised by the SIEM, in any of the 150+ clients' environments or by SITE MDR's internal threat hunting. XSOAR ingests aggregated alerts and indicators of compromise (IoCs) from internal sources, and the technologies deployed client-side provide complete visibility across different log types, network traffic, and endpoints. The majority of SOC alerts are mapped to playbooks based on a sophisticated detection catalogue developed to detect advanced tactics, techniques, and procedures (TTPs). Strategies from the playbooks are then executed in response to these incidents.

> XSOAR has shifted our team away from manual analysis to more strategic tasks. When an alert is fetched, it is mapped to a designated playbook that might simply perform enrichment or manage an end-to-end investigation.
>
> **–Lead Automation Engineer, SITE MDR**

BENEFITS

Investigating alerts 30% faster

SOC security automation is upending operations and service delivery to enable SITE MDR to:

- **Deliver consistently secure, high-quality client experience:** SITE MDR has significantly improved SLA without jeopardising quality by using XSOAR. For example, alerts processed using the playbooks are investigated 30% faster than those processed manually. Their Lead Automation Engineer comments, "For alerts managed entirely by XSOAR, we are meeting 100% of SLAs."

  Moreover, SITE MDR has the flexibility to automate prioritisation of alerts, ensuring nothing is overlooked. XSOAR is also integrated with SITE MDR's custom-built Client Portal, so clients can automatically perform massive security scans, without having to wait for human interaction. This extends the SITE MDR service catalogue and increases client satisfaction.

- **Reduce false positive alerts:** XSOAR automatically closes known false positives without human intervention using playbooks designed to assess alerts for false positive detection. XSOAR also assists the team responsible for building use cases by suggesting tuning cases to reduce the number of false positive alerts a rule may trigger. This has led to a reduction in false positive rates for automated alerts and gave analysts more time for strategic, value-add tasks.
- **Optimise SOC operations:** XSOAR saves time, streamlines operations, and increases SOC productivity. Analysts no longer need to be booked for a day or more to perform exhausting manual tasks – instead, XSOAR automation makes the team highly efficient.
- **Automate across SITE's security stack:** Alerts are ingested across sources and 150+ client environments, executing automated workflows/playbooks to speed up incident response and provide standard investigations.

> We have other use cases that allow us to proactively perform large-scale threat-hunting activities with little or no intervention from the analyst. That would be almost impossible without automation.
>
> **–Lead Automation Engineer, SITE MDR**

> By automating everyday security processes, XSOAR frees our resources to concentrate on strategic client tasks and deliver a great service experience.
>
> **–SOC Operations Manager, SITE MDR**

Learn more about Palo Alto Networks on the website, where you can also read many more customer stories.

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