CASE STUDY

Imagination Technologies transforms SOC operations with Cortex XSIAM

Imagination Technologies have created a highly mature, no-friction security operations centre (SOC) by introducing Palo Alto Networks Cortex XSIAM, the AI-driven security operations platform. Since XSIAM's introduction, Imagination Technologies' incident closure percentage has rocketed from 10% to 100%, even with incidents now coming from more sources. The median time to resolution – "months" before XSIAM – now stands at just five hours, with further reductions anticipated.

IN BRIEF

Customer
Imagination Technologies

Industry
Technology

Services
Processor solutions for graphics, vision, and AI processing

Organisation Size
1,200+ staff worldwide

Country
Kings Langley, UK

Challenges

- Point security platforms obscured visibility.
- Security team was stretched thin dealing with manual, reactive incident response.
- Human interventions led to protracted investigation times and reduced efficiency.

Requirements

- Automate repetitive data analysis tasks and improve productivity.
- Unite endpoint, network, cloud, and identity data to detect advanced threats and simplify investigations.
- Streamline and accelerate onboarding of new data sources.

Solution

Palo Alto Networks Cortex XSIAM

CHALLENGES

The silicon solutions of tomorrow

Imagination Technologies Group have more than 25 years of experience in designing and licensing intellectual property (IP) processor solutions. Headquartered in the UK, the organisation's computing, graphics, and artificial intelligence (AI) IP deliver security, performance, and low power consumption in the smallest area of silicon possible, enabling chip makers to create new, innovative digital products.

Several years ago, Imagination launched a bold and imaginative "Cyber Transformation Programme" to create a no-compromise security posture. A connected portfolio of Palo Alto Networks network, endpoint, and security operations technologies protects Imagination's IP and people from known and unknown cyberthreats – quickly and automatically.

However, some common challenges persisted in the SOC. Business growth and an expanding attack surface generated more security data from more siloed sources. There was significant reliance on reactive manual interventions by the lean security operations (SecOps) team, which in turn led to longer investigation times and reduced efficiency.

"One of the drawbacks to business growth is information overload," says Paul Alexander, Director of IT Operations at Imagination. "Threat actors are highly sophisticated, but we only have the same number of hours each day to tackle those threats. Previously, when we saw suspicious activity, we had to decide where to start the investigation. That required input from the front desk team, application team, server team, and network team. With so many people involved, investigations were slow, complex, and burdened with risk."

According to Paul, the company's existing SIEM was one of the main causes of the problem: "We were collecting vast amounts of data from the network, endpoints, and cloud – but the SIEM was not designed to examine data on that scale or variety. We were only looking at a single data type or a certain type of log. We were never connecting the data or deriving real intelligence from it."

> The SIEM was not designed to examine data on that scale or variety. We were only looking at a single data type or a certain type of log. We were never connecting the data or deriving real intelligence from it.
>
> **–Paul Alexander, Director of IT Operations, Imagination Technologies Group**

REQUIREMENTS

Harnessing the power of AI and machine learning

Working with Palo Alto Networks, Paul and his SecOps team identified that they would require a modern security intelligence and automation management platform to:

- Protect IP and people by using intelligent endpoint protection powered by mature machine learning (ML data models built specifically for security).
- Automate repetitive data analysis tasks to improve productivity, allowing more time for value-add security operations.
- Investigate and close more incidents by leveraging AI to group related alerts into incidents and prioritise incident triage using risk SmartScores.
- Unite endpoint, network, cloud, and identity data to detect advanced threats with precision and simplify investigations.
- Simplify and accelerate onboarding of new data sources.

SOLUTION

Automated end-to-end threat management

Imagination have implemented Palo Alto Networks Cortex extended security intelligence and automation management (XSIAM) in the SOC to deliver automated end-to-end threat management wherever threats originate. This breakthrough automation-first security operations platform turns widespread infrastructure telemetry, threat intelligence, and external attack surface data into an intelligent data foundation to fuel effective automated detection and threat response.

This cutting-edge system supports Imagination across three vectors:

- **Intelligent analytics**: XSIAM creates a complete picture by pulling data from Imagination's endpoints, network, and cloud environments. ML then processes that data with an understanding of how everything connects. In time, Imagination will ingest data from additional sources, including HR systems and authentication events from identity providers.
- **Automation-first security**: Automated analytics and detection take care of low-risk threats to allow analysts to concentrate on a small set of high-risk incidents.
- **Proactive security**: Embedded threat intelligence and attack surface management enables the SecOps team to be proactive – for example, by patching vulnerabilities before an attacker can exploit them.

Unlike a traditional SIEM, new data is automatically integrated into XSIAM for richer analytics.

> We're now getting visibility of what's happening in our offices in real time, mixing up to 15 sources in one go. When users in different geographies set proxies, we're getting alerts on those. We have so much more visibility, and we can be proactive on those alerts.
>
> **–Paul Alexander, Director of IT Operations, Imagination Technologies Group**

BENEFITS

Frictionless security with a breakthrough autonomous security operations platform

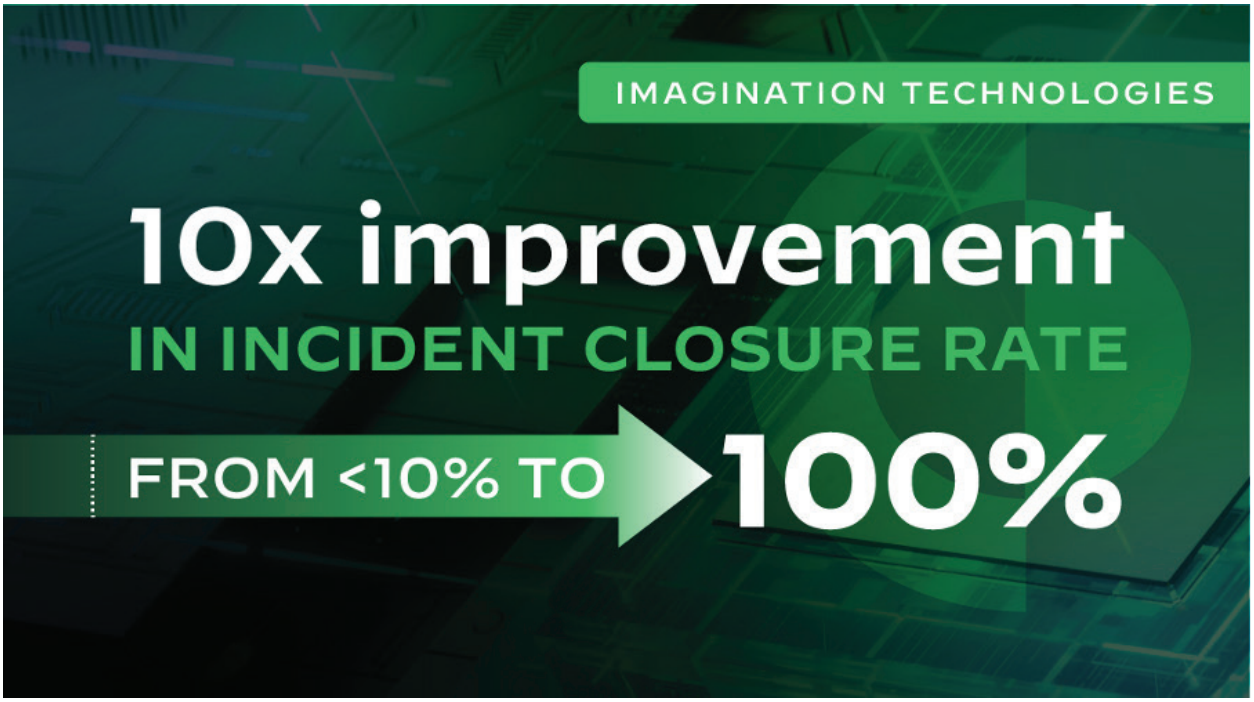
Cortex XSIAM is automating and scaling Imagination's SecOps to protect against advanced threats. The benefits XSIAM delivers include:

- **Increased SOC agility with complete visibility**: Imagination are achieving complete visibility from within the same console with the same workflows, fully integrated data, and ML-Powered automation all contributing to agile, responsive SecOps. Paul comments, "XSIAM really is a single pane of glass. All our SecOps processes happen in one place, which means less context switching. That's a huge saving for a small team like ours."
- **Game-changing security visibility delivered by intelligent data use**: Imagination ingest data from many new sources beyond endpoint and network data. These include HR systems, authentication events from identity providers, security events and raw logs from firewalls, and SaaS events from Microsoft 365. For example, the company ingested only two sources into the previous SIEM, equal to approximately 100GB per day. Now, the team is ingesting 18 sources: 300GB per day. Moreover, XSIAM is analysing 315GB per day of in-line endpoint data.

  "Because XSIAM is cloud-native and because of the integrations it has, we have analytics on the data that's turning that data into rich information for us," outlines Matthew Hunt, Senior Information Security Analyst, Imagination Technologies Group. "We can easily ingest logs and do it from our Office suite, IDP, or from any other SaaS sense we have and quickly deploy."

> XSIAM lets us cut straight to the real incidents we need to focus on. The rest of the noise is handled by automation. XSIAM has made our SOC proactive.
>
> **–Matthew Hunt, Senior Information Security Analyst, Imagination Technologies Group**

- **Comprehensive, unified, future-proof security operations**: Connected SecOps capabilities drive faster median time to resolution, more effective threat response, and lower cost. For example, the median time to resolution is five hours with XSIAM, compared with "months" using the previous SIEM.
- **Proactive security coverage**: ASM coverage provides an outside-in view of publicly exposed assets, potential vulnerabilities, and threats. Tying this to automation has enabled Imagination to plug gaps in security coverage quickly and regularly. Likewise, TIM enables strategic threat intelligence. For example, combining TIM with automation ingests threat intelligence to automatically update dynamic block lists and block potential threats.



- **Simplified operations**: Cortex XSIAM reduces manual effort, cuts delays in onboarding/offboarding employees, lowers the likelihood of misconfigurations, and provides fully audited, repeatable processes. For example, the organisation can close out 100% of the incidents using automation, versus less than 10% with the prior SIEM. "Native automation means accessible automation," Paul explains. "The intuitive ingestion of extra data sources, together with the enrichment and normalisation of that data, gives us great confidence in the data for decision-making."

  Operations are further simplified with modular playbooks. As Matthew explains: "The XSIAM team are developing playbooks all the time, and they are creating those playbooks in a modular fashion. So rather than us editing those playbooks, we just turn features on and off."

- **Improved employee engagement**: Analysts spend less time on low-grade, repetitive tasks and more time on rewarding, value-add processes. Paul comments, "XSIAM improves morale. People have more time to focus on SOC strategy and their personal development. Our SOC is generally a happier place now."

> Cortex XSIAM is a single, tightly integrated suite of tools. It's easy to commission, easy to use, and delivers the trusted answers a modern SecOps team needs. We are now far more mature and efficient, making more intelligent use of the data and getting much more done in the same timeframe.
>
> **–Paul Alexander, Director of IT Operations, Imagination Technologies Group**

Learn more about Palo Alto Networks Cortex XSIAM here. Read the other Imagination case studies to learn how they use Prisma Access and the Palo Alto Networks portfolio.

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