graylog

From MSSP Reliance to SOC Maturity:
How Circles Secured Its Stack with Graylog

COMPANY SNAPSHOT

Industry:

Telecommunications

Headquarters:

Singapore (global operations)

Company Size:	***Founded:***
1000+ employees	2014

Core Capabilities:

SOC Operations, Cyber Defence, Red Teaming, Threat Intelligence, Digital Forensics, DFIR, SOAR Automation

Products Used:

Graylog Security, Graylog Cloud on AWS, SOAR platform, Generative AI & Illuminate, Custom Integrations

Featured Leaders:

Somanath Varanasi, *Manager II: SOC, Cyber Defence and DFIR*

Elwin Shaji, *Senior Cybersecurity and AI Solutions Engineer*

James Ling Yi, *Staff Cyber Security Engineer*

OVERVIEW

Circles Asia Pte Ltd. is a fast-scaling, global digital telecommunications service provider delivering B2C and B2B services through its proprietary digital-first platform. With millions of subscribers depending on its platform, Circles needed stronger visibility and faster security threat detection capabilities across the Group's instances of its Cloud resources, on-prem systems, and tech stack for Partner deployments.

Until recently, Circles operated its SOC through a managed third-party service. While it helped the Group get started with the basic requirements in the initial years, the arrangement limited visibility, degraded response times, and was inadequate to meet compliance requirements given the group's growth trajectory over the past few years. As part of the roadmap to enhance the capabilities of the internal Cyber Defence team, Somanath, Elwin, and James were tasked with building a modern in-house SOC that could scale quickly and deliver enterprise-grade security outcomes.

Their objectives were:

- **Stronger visibility on the critical Computing resources**, including EC2, S3, Network, and APIs components
- Explore options to **reduce** system and operational **overheads**; and
- Implement an automation-ready SIEM to **minimize alert fatigue** and **accelerate response time**.

After evaluating a few solutions, the team selected **Graylog Security Cloud on AWS** to deliver the necessary outcomes.

> "Before Graylog, security operations at Circles were almost non-existent. Today, Graylog is the centerpiece of our SOC maturity. It gives us visibility across cloud, on-prem, and partner workloads, strengthens our defense against threats, helps us meet compliance demands, and builds confidence with both stakeholders and customers."
>
> — Somanath Varanasi, Manager II: SOC, Cyber Defence and DFIR

THE CHALLENGE

When Circles assumed responsibility for SOC operations, they faced:

- No baseline visibility with alerts handled externally by the MSSP
- Blind spots across the tech stack and deployments
- Manual investigations with no automated orchestration was slowing the response time
- High analyst fatigue from repetitive triage and false positives
- Compliance requirements and enterprise customers demanding proof of controls

They also needed it deployed quickly, without heavy setup or infrastructure management.

> **"Graylog's notification system is central. It triggers the automation, feeds the SOAR with context, and drives necessary triggers downstream."**
>
> **— Elwin Shaji, Senior Cybersecurity and AI Solutions Engineer**

THE SOLUTION

Circles deployed Graylog Security Cloud on AWS as the foundation of their SOC, then layered automation, SOAR, and AI-driven enrichment on top.

GRAYLOG SECURITY ON AWS

- Agentless log collection eliminated system overhead and reduced business pushback on performance impacts
- Unified visibility across Cloud resources, on-prem, and Partner dedicated deployments
- Rapid and seamless threat detection coverage from newly onboarded resources reduced time from weeks to hours

ILLUMINATE & GENERATIVE AI

- Agentless log collection eliminated system overhead and reduced business pushback on performance impacts
- Unified visibility across Cloud resources, on-prem, and Partner dedicated deployments
- Rapid and seamless threat detection coverage from newly onboarded resources reduced time from weeks to hours

SOAR INTEGRATION

- Instant/enhanced automation through Graylog webhooks triggering SOAR workflows
- Reducing IOC isolation and containment to minutes

API-POWERED SOC WORKFLOWS

- By combining Graylog's API with SOAR, Circles was able to bring full auditability across the event lifecycle from signal to enrichment to decision to action flow inside Swimlane
- Curated stream-scoped views by customer deployments and environment gave instant analyst context
- Pipelines and stream routing eliminated noise from benign traffic, such as blocked Cloudflare hits, while surfacing actual malicious behavior
- Built-in normalisation and field extraction powered immediate baselines for outlier detection

> **"Graylog's clean payloads and API-first design enabled us to automate end-to-end playbooks in Swimlane. Analysts can move from raw events to decisions in a single workspace with context scoped by customer deployments. That's top-tier SOC capability without top-tier overhead."**
>
> **— James Ling Yi, Staff Cyber Security Engineer**

Outcomes That Matter

UNIFIED SECURITY VISIBILITY

- Centralized logs across the tech landscape, irrespective of their deployment model
- Fixed API monitoring gaps to strengthen security posture across our tech stack

REAL-TIME AUTOMATED RESPONSE

- Webhook-driven SOAR playbooks accelerated containment
- Automated notification flows bridged Graylog, SOAR, and threat intelligence

SMARTER DETECTION, LESS BURNOUT

- Illuminate and pipelines reduced false positives
- Analysts focused on real threats instead of repetitively mundane triage

SOC MATURITY AND ROADMAP

The Graylog platform is playing a key role in strengthening our logging and monitoring capabilities, which directly supports Circles in achieving its target maturity levels.

A PARTNER FOR SOC MATURITY

Circles views Graylog as the centerpiece of their SOC strategy:

- **Lean-team friendly:** Intuitive dashboards and agentless ingestion keep overhead low
- **Future-proof:** Built-in AI, APIs, and automation scale with business needs;
- **Compliance ready:** Audit evidence delivered instantly for governance, assurance, and customer reviews.

> “If you want something simple to start with and scale along the way, Graylog is the right choice.”
>
> — Elwin Shaji, Senior Cybersecurity and AI Solutions Engineer

TELECOM SECURITY THAT SCALES

Circles’ SOC journey, from zero visibility to automation-driven cyber defence, shows what is possible with the Graylog suite of solutions. Today, Circles can:

- Detect and respond to attacks faster
- Automate investigations with fewer manual steps
- Deliver audit-ready compliance evidence instantly
- Scale SOC maturity to align with business goals

With Graylog, Circles is no longer just chasing alerts. It is proactively protecting what matters at the speed of business.

Explore Graylog Cloud on AWS