# Security Operations Center as a Service (SOCaaS)

Helping Secure Your Business

**With Security critical** to all organizations,

but the lack of skills and the rapid evolution of threats make it a challenge for them to stay current and provide the highest security efficacy to their organization. Our SOC as a Service Solution allows organizations to leverage our global security expertise with full monitoring, management and optimization of your security information and event management (SIEM) environment.

# Technology overload and ability to **maintain control to ensure compliance**

**Application security fatigue**

**Vulnerability and patch overload**

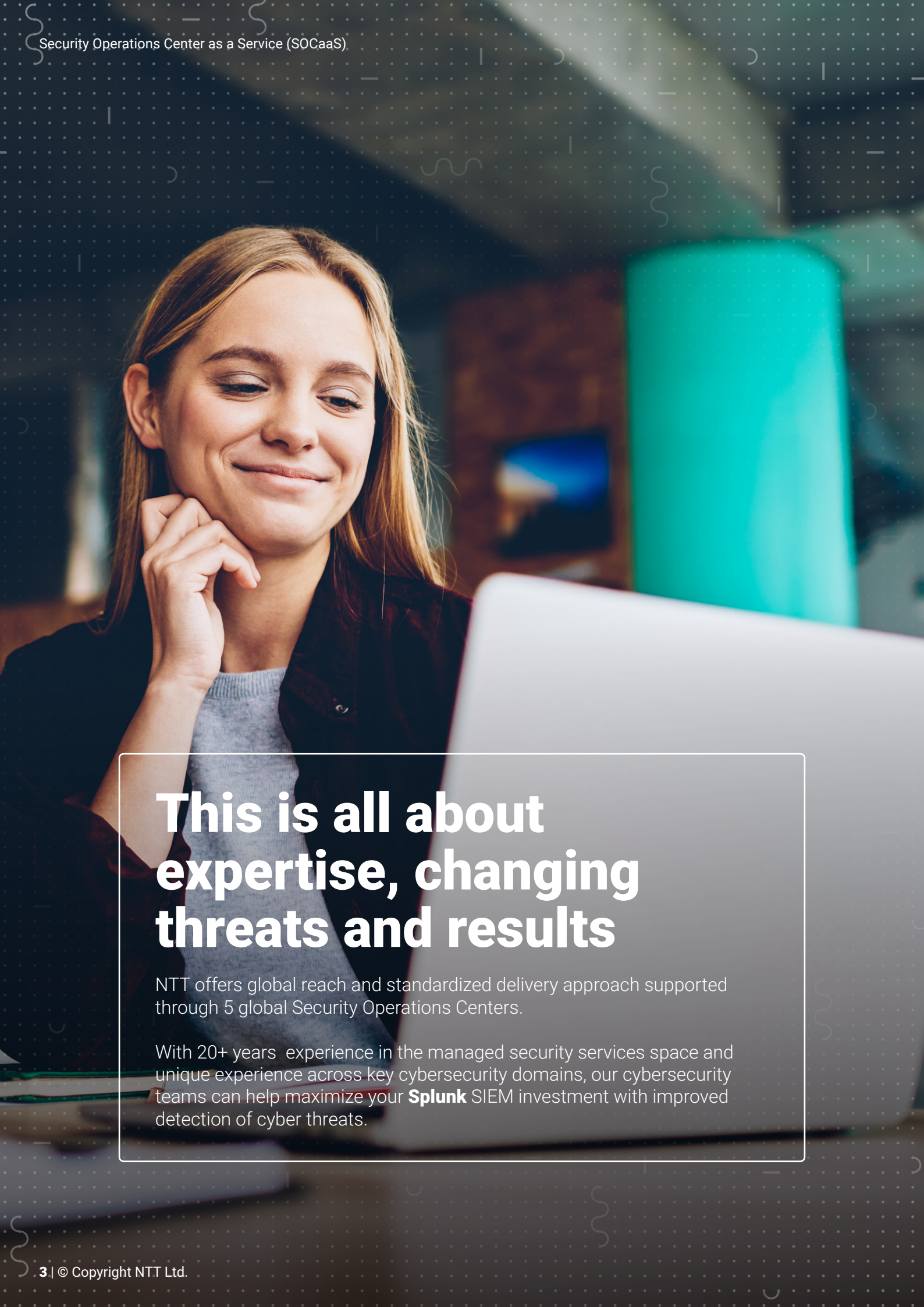
Cybersecurity is a top priority for all organizations with cybercrime a key risk facing the world. The threat landscape continues to evolve as threat actors are constantly on the lookout for weaknesses to exploit. In our 2020 Global Threat Intelligence recorded a 350% increase in ransomware year over year and with greater sophistication in the attacks.

Across all industries balancing governance, risk and compliance with cybersecurity is still a challenge.

Organizations need to establish cyber resilience and agility; however, they are faced with the challenges of a shortage of skilled talent and a continually changing threat landscape. Not only is it difficult to recruit the right skills, but when an attack happens even the best resourced teams find themselves stretched.

It is challenging to stay current and provide the highest security efficacy to their organization. While technology is critical, just investing in more technology may not provide sufficient protection. Each new investment results in additional data to be monitored and analyzed, making it more difficult to identify real threats.
The introduction of new technologies also poses a challenge to security teams who need to keep on top of what is required to keep them compliant.

With the growth in applications, the need to ensure they all remain secure and that any new vulnerabilities are patched can often result in security teams becoming overwhelmed with the requirements for their expertise. The result is this takes resources away from focusing on the events being generated from their security devices.



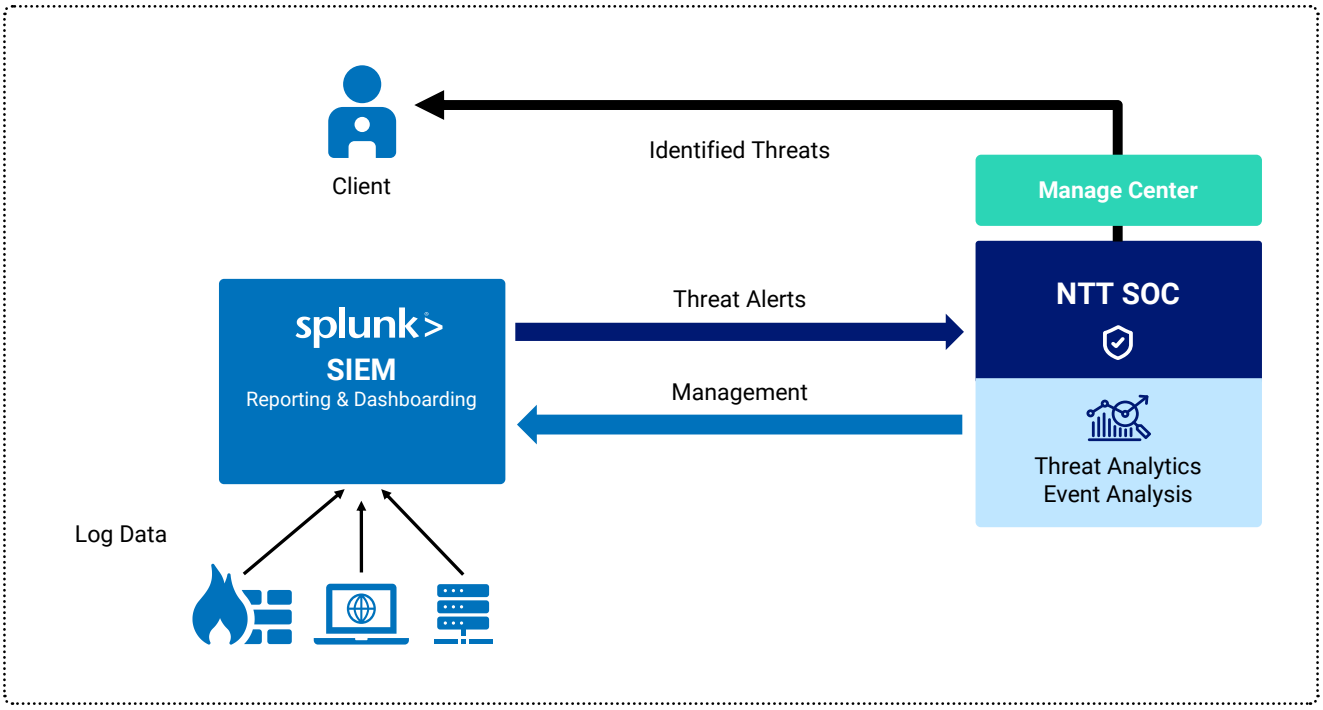
# This is all about expertise, changing threats and results

NTT offers global reach and standardized delivery approach supported through 5 global Security Operations Centers.

With 20+ years  experience in the managed security services space and unique experience across key cybersecurity domains, our cybersecurity teams can help maximize your **Splunk** SIEM investment with improved detection of cyber threats.

# NTT Managed Splunk SIEM **Workflow**




Managed SIEM leverages a client's Splunk SIEM, **whether new or existing, while delivering a broad set of advanced capabilities.**

**Monitor and manage client Splunk SIEM**, including patching and updating

**Identifies, categorizes, and analyzes** incidents and events

**Scalable architecture** that can easily **expand from GB to PB,** with deployments that can **span on-prem and cloud**

**Custom use case development and reporting** (e.g. alerts and rule development)

**Incident analysis and notification**

# Key business **challenges**

Lack of visibility to help **identify genuine risk.**

**Extract value faster** from existing investments **and data.**

Perpetually changing **threat landscape.**

Cybersecurity expertise **is hard to find.**

A need for a wholistic security monitoring, **response and reporting program.**

### 24/7/365 monitoring

Highly trained analysts leveraging client SIEM platforms to perform incident analysis and threat hunting.

### Management

Offload the burden of platform management including updates, patching, and new device enrollment.

### Reporting

Design, build and customize the threat analysis reports.

### Use case development

Develop, test and implement client-specific business and security requirements (including cloud security).

### Tuning

Adjust alerts and rules based on client and SOC feedback, to ensure the lowest possible false positive rate.

### Deep Splunk Expertise

Over 500 trained Splunk experts with deep experience optimizing security operations using Splunk.

# Why choose **NTT?**

**Process Maturity**
**20+ years of Managed Security Expertise**

**Global Coverage and Visibility**

Our worldwide presence ensures that we can deliver wherever you have operations

**Active Threat Hunting**

Through our extensive global network, we have deep insight into emerging threats through our Global Threat Intelligence Centers and Security Operation Centers around the world, analyzing billions of logs each day.

**Secure by Design**

Embed security across your network, data center, applications, and clouds

**Industry Validated: A Leader in IDC MarketScape:** Worldwide Managed Security Services 2020 Vendor Assessment.

# NTT and Splunk Solve Security Challenges with Data

The right expertise paired with the right technology is critical for comprehensive protection against a constantly evolving threat landscape. As part of the SOC as a service solution, NTT Ltd. partners with Splunk, the provider of the Data-to-Everything platform to quickly detect and respond to internal and external attacks, to simplify threat management while minimizing risk, and safeguard organizations' most critical businesses.

The NTT Cybersecurity team uses Splunk to gain organization-wide visibility and security intelligence. This translates into continuous monitoring, incident response and providing executives a window into business risk.

# **Analytics-Driven** Security

**Improve Security Operations –** Identify, prioritize and manage security events with event sequencing, alert management, risk scores, and customizable dashboards and visualizations.

**Investigative Tools for Fast Response –** Gather all the context needed in one view for rapid investigations and response. Take care of existing and newly discovered threats fast with contextual threat detection and incident response.

**Automate and Respond –** Integrations with hundreds of security vendors for context-driven automated response that speeds up manual tasks. Enhance visibility and responsiveness with focused threat detection and accelerated incident investigation.

**Achieve Better Visibility and Insight –** Data is automatically retrieved from network, endpoint, access, malware, UBA anomalies with the ability to ingest any other type or sources of data

**Manage alerts and power dynamic discoveries –** Out-of-the-box capabilities to perform contextual searches enabling the rapid detection and analysis of advanced threats

Thousands of organizations depend on Splunk software for SIEM and advanced security use cases. **Splunk has won numerous industry awards including placement as a leader in the Gartner Security Information and Event Management (SIEM) Magic Quadrant for seven consecutive years.**

The difference between attacks being dealt with swiftly or becoming a catastrophic event can come down to the robustness of an organization's SIEM platform and the expertise of the individuals running an organizations SOC. **With NTT and Splunk organizations enjoy the best of technology and human innovation.**


NTT
splunk>