Datasheet

Security Operations Centre as a Service

Continuous Protection & Combating Advanced Threats In Your Organisation

Benefits

- Fewer alerts & minimal false positives
- Faster incident response times
- Lower costs and less damage due to fast response time
- Complement existing compliance practices for companies adhering to industry regulations
- Centralised visibility & continuous monitoring services to contain threats as quickly as possible no matter when they strike
- Greater control and transparency surrounding IT security operations and procedures
- Better customer experience as employees and clients can feel more at ease sharing sensitive information with the knowledge that the SOC team is on duty
- Independent, primary or second pair of eyes approach to security professionals
- 24/7/365 monitoring
- Predictable monthly operating expenses

Introduction

SOC-as-a-service offers more than your traditional managed security services provider. Typical MSSPs focus on traditional device management and basic alerting. On the other hand, SOCaaS is a type of security-as-a-service focused on detecting and responding to threats bypassing your preventive controls. When you are looking for security experts who can proactively hunt down threats and give you actionable information to mitigate them, SOCaaS providers are your best choice.

SOCaaS is turnkey solution focused on real-time threat detection and incident response. Typically, these include a cloud-based Security Information and Event Management (SIEM), forensic analysis, vulnerability assessment, and compliance reporting. Such comprehensive, end-to-end security services are ideal for companies with limited budgets and resources.

Clients can rely on LGA's people, processes and technology needed to manage a SOC. All of the necessary components and staff of a SOC (SIEM, security analysts, threat hunters, incident responders, etc) are operated and managed offsite. The complexity associated with managing a SOC on premises is eliminated.

24/7 Monitoring On-Premises and Cloud

LGA provides the necessary 360-degree visibility into your IT environment. This includes a fully integrated monitoring service that protects your infrastructure and resources wherever they reside—on the customer's premises, in a public cloud infrastructure, in SaaS applications, or in hosted security services. Our security experts have visibility across both cloud and on-premises systems, allowing them to detect attacks whenever or wherever they threaten your business. This visibility is achieved in two ways: Sensors on premise and APIs for cloud services.

Scalable and Cloud-based

The service is cloud based, highly scalable, multi-tenant, ingest, parse, and analyse unlimited amounts of raw log and data from customers. The solution combines human and machine intelligence to check millions of events in real time for 24/7 threat detection. The machine learning, threat intelligence feeds, and big data security analytics tools collect and correlate security events from all infrastructure, endpoints, and applications, parsing and aggregating log data into structured observations, analysing data in context using behaviour analytics and external threat intelligence feeds to detect advanced malware, emerging network threats, malicious IP addresses, URLs and prioritising incidents.

Security Operations Centre as a Service

Grow with LGA - The Security Maturity Continuum:

The Security Maturity Continuum describes organisations in various stages of developing their security presence - five stages of security maturity are highlighted. In every stage, a different service level at the SOCaaS is relevant and of worthwhile consideration.

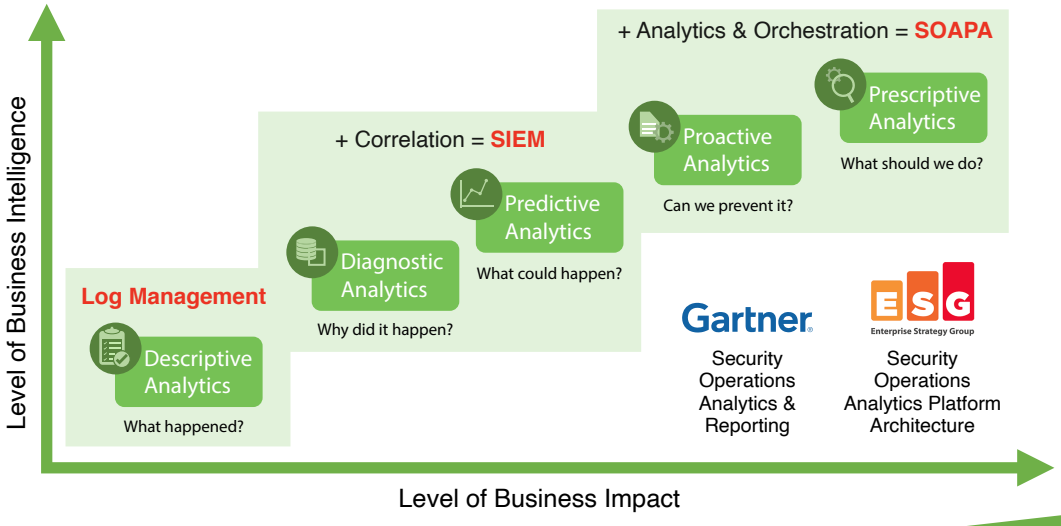
Security Maturity Continuum - Are You Ready for a SOC?

1	2	3	4	5
Minimalists "We got Anti-Virus and Firewall in place. We're good!"	**Reactive** "We haven't explored solutions and don't believe we are at risk. We'll deal with a breach if it happens."	**Concerned** "We're at risk, but budget is a problem. We're overwhelmed by the alerts we are facing. We need help priotising and addressing threats."	**Advanced** "We have budget to invest in security. We have limited personnel and need to maximise them."	**Security Mature** "We're knowledgeable about security. We continuously innovate and improve our program."
• No SIEM or SOC services. • Typically, an IT admin performs compute, network and security functions. • No logging. • Basic firewall at perimeter. • Anti-virus in use.	• No SIEM or SOC services. • Typically, an IT admin performs compute, network and security functions. • Some logging. • Patch management added. • Dedicated firewall & DMZ. • Basic identity and access management added.	• Considering a SIEM or has basic SIEM deployment or SOC services. • Multi-firewall and Network segmentation added. • Data classification added. • Overwhelmed by alerts and logs. • Need to priotise them. • Concerned with optimising budget due to limited resources.	• SIEM or SOC services integrated with most areas. • Considering analytics as a way to cut down on alert fatigue. • Starting to thinking about tools to optimise incident investigation. • Looking to increase operational efficiency and maximise personnel output. • Intrigued by the idea of threat hunting.	• Very mature SIEM or SOC services deployment. • Integrated with virtually all systems. • Performs threat hunting with senior analysts. • Has customised security capabilities that integrate into their workflows. • Capable of building their own data structure algorithms. • Interested in cost efficiency and reduced risk from third party solutions.

Next Generation SOCaaS

Supporting the maturity continuum above, SOCs have evolved from traditional to sophisticated functions. Increasing complexity of IT, evolving threats and the need to coordinate multiple security products require SOCs to respond with advanced analytics and Security Orchestration, Automation and Response (SOAR) integration services.

Evolution of Security Operations (Gartner/ESG)



Security Operations Centre as a Service

Challenges When Building Your Own SOC

Skill shortage: Human analysts are critical to a SOC's ability to quickly identify, prioritise, and respond to security incidents. While numerous tools are available to help organisations gather and analyse massive volumes of security and event data, human experts add the context and situational awareness needed to remediate threats.

Budget: Increased pressure to cut or maintain costs is driving many organisations to outsource key functions to third parties.

Lack of Documented Processes: Many SOCs are running into trouble because they either don't have documented processes or are letting the ones they do have stagnate because of a lack of continuous improvement effort.

Uncertainty about the Mission: Many SOC staffers interviewed for the report appeared to be unsure about their core mission. They either did not have one, or it had not been communicated to staff and other stakeholders. In many cases, SOC managers did not have a clear idea as to which business assets - such as applications and data - were most important to protect. As a result, they had little idea of which threats were most important to focus on.

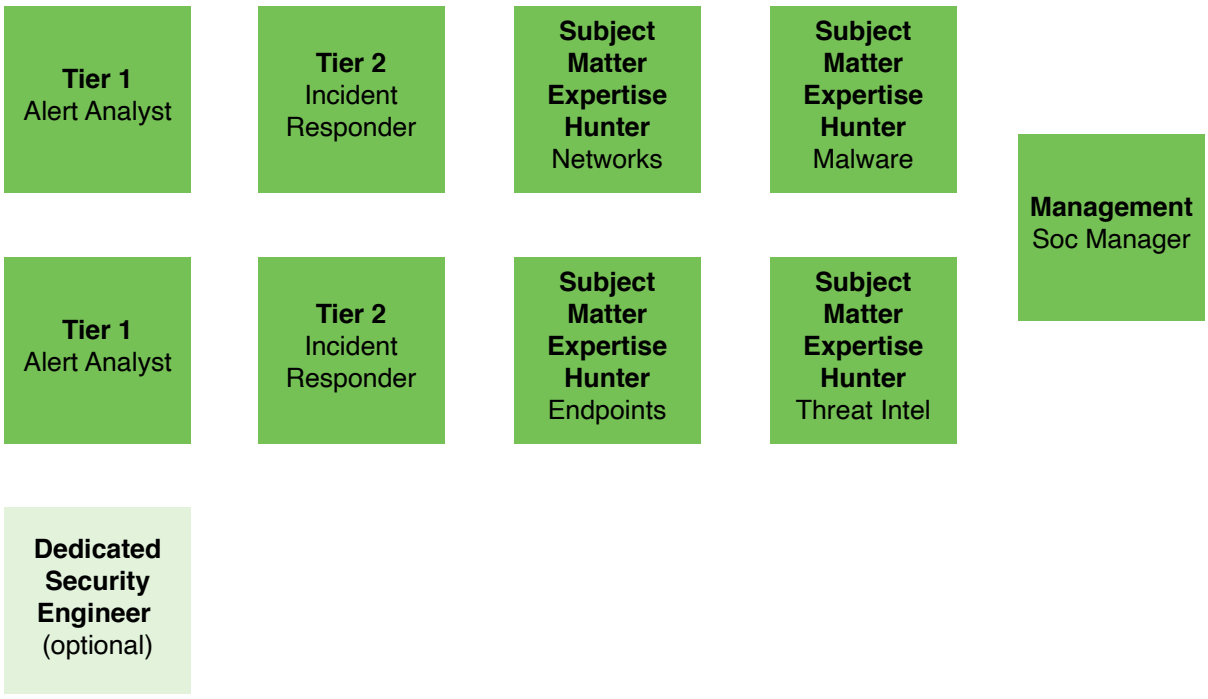
Pinning Hope on Technology: Many SOCs are expecting technologies such as Security Information and Event Management (SIEM), User and Entity Behavioural Analytics (UEBA), Security Orchestration, Automation, and Response (SOAR), and products leveraging on AI and machine learning to alleviate some of the challenges.

For the above reasons, many organisations have chosen to outsource to SOCaaS.

Roles and Responsibilities

LGA's SOC has a hierarchy of roles with a clear escalation path. Day-to-day alerts are received and investigated by the Tier 1 Analyst; a real security incident is stepped up to a Tier 2 Analyst; business-critical incidents pull in the Tier 3 Subject Matter Expertise individuals and, if necessary, the SOC Manager. Named security engineers can be assigned for premium levels.

SecOps Processes / Who Works in a SOC?



Security Operations Centre as a Service

Incident Response Management Processes:

An incident response plan is a documented, written plan with distinct phases that help recognise and deal with a cybersecurity incident like a data breach or cyber attack. We detect, contain, and mitigate cyber attacks against the organisation. The people responsible for incident response are Tier 1, Tier 2 and Tier 3 analysts. The 5 step process upon discovering an event is:

Basic Incident Response Model

1	2	3	4	5
 **Event Classification**	 **Prioritisation and Investigation**	 **Containment and Recovery**	 **Remediation and Mitigation**	 **Assessment**
Tier 1 Analysts monitor user activity, network events, and signals from security tools to identify events that merit attention.	Tier 1 Analysts prioritise, select the most important alerts, and investigate them further. Real security incidents are passed to Tier 2 Analysts.	Once a security incident has been identified, the race is on to gather more data, identify the source of the attack, contain it, recover data and restore system operations.	SOC staff work to identify broad security gaps related to the attack and plan mitigation steps to prevent additional attacks.	SOC staff assess the attack and mitigation steps, gather additional forensic data, draw final conclusions and recommendations, and finalise auditing and documentation.

Platform Integration (Security Eco-system):

When more platform integration and data sources are ingested, the better equipped it is to detect attacks. This also enhances integration to SOAR, allowing a holistic security response.
Inbound data log ingestion includes:

- Firewalls
- Endpoint Security Software
- DDoS Infrastructure
- WAF Infrastructure
- Directory Servers
- DHCP and DNS Servers
- Application Servers / Web Servers
- Cloud Applications
- Operating Systems

In addition, the SOC is able to ingest log sources from database services, mail services, source code controllers, unified communication servers, environmental sensors, load balancers and application firewalls, network intrusion protection systems, routers and switches and wireless LANs, security gateways, threat intelligence feeds, virtualisation, VPN gateways, vulnerability scanners and other forms of logs.

Security Operations Centre as a Service

Threat Hunting with Mitre ATT&CK™ Framework

Effective threat hunting is continual, proactive, and powered by strong intelligence, and to do it right, you need to play offence. LGA uses ATT&CK™ to guide a standardised but flexible framework that will help streamline building, testing and validating customised detection for your organisation. ATT&CK™ contains an ever-evolving taxonomy of the tactics, techniques and procedures (TTPs) adversaries use to compromised networks.

Service Levels and Security Maturity Continum

With LGA, you can consume SOCaaS at any stage of your Security Maturity journey.

SOCaaS: Choose Service Level that Meet your Needs

Service Level	Service Level Functions	Suitability Based On Maturity Continuum
Level 1	• Detection • Event Classification • Alert & Reporting (One Portal) • Optional cyber insurance assistance	• Minimalist • Reactive
Level 2	• Detection • Event Classification • Prioritisation & Investigation (Triage) • Alert & Reporting (One Portal) / Monthly Reporting • Basic Response & Mitigation *limited to security controls managed by LGA • Assessment and Incident Report • Optional cyber insurance assistance	• Reactive • Concerned • Advanced
Level 3	• Detection • Event Classification • Prioritisation & Investigation (Triage) • Alert & Reporting (One Portal) / Monthly Reporting • Threat Hunting (using Mitre ATTACK™ Framework) • Containment, Remediation & Mitigation *limited to security function managed by LGA • Assessment and Incident Report • Named Security Engineer (in-depth knowledge of customer environment and trusted advisor) • Optional cyber security auditing assistance	• Advanced • Security Mature

Contact Us

LGA Telecom Pte Ltd
33 Ubi Avenue 3
#08-53 Vertex (Tower A)
Singapore 408868

Tel (65) 6892 2308
Email: sales@lgatelecom.net
Website: www.lgatelecom.net