LUMEN

Strategies in addressing cyber risks from an expanding Attack Surface

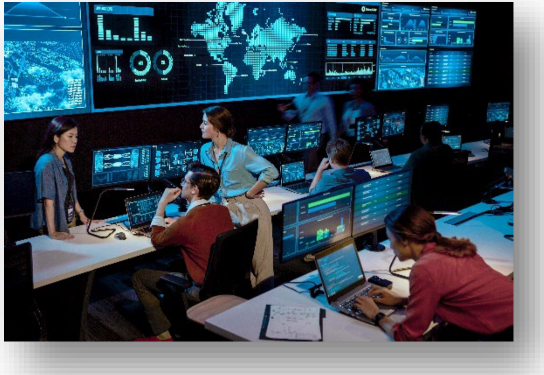
Wai-Kit Cheah

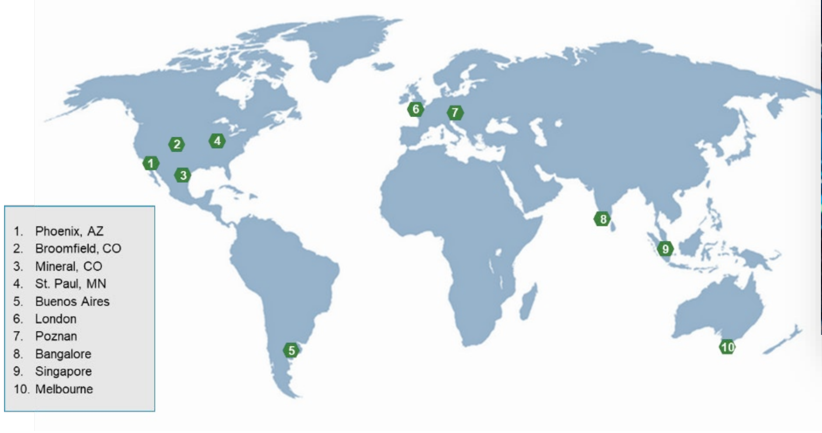
Senior Director, Security Practice
Lumen Technologies Asia Pacific

Empowering Human Progress through technology

Our core purpose is to further human progress through technology. We believe humanity is always at its best when it produces innovative technologies that advance the ways we live and work.

- 40,000 employees globally in 60+ countries
- Operate one of the largest, most connected and most deeply peered networks in the world with ~450K route miles of fibre and ~170K on-net fibre locations. Global Tier-1 ISP with world's highest number of connected AS
- Managed Security Service Provider with Global Security Operation Centres (GSOC), including three GSOCs in APAC (Bangalore, Singapore and Melbourne)





Hackers attack every 39 seconds, on average 2,244 times a day [1]

20% Breaches are caused by compromised credentials [3]

13% Increase in Ransomware breaches, more than in the last 5 years combined [4]

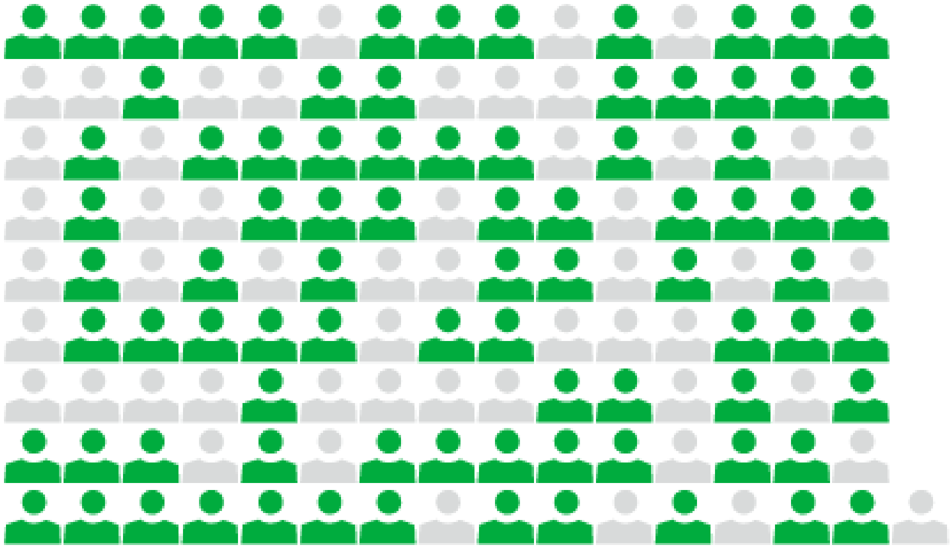
$4.24M Average cost of data breach worldwide increased 9.84% in past 2 years. This is the highest average total cost to-date [3]

280 days Average time to identify a breach in 2020 [5]

*Sources: 1. University of Maryland, 2. Cybint solutions, 3. IBM, 4. Verizon, 5. IBM

LUMEN®

Risks from Supply Chains, Partners and Third Parties



Each glyph represents 25 incidents from a Partner vector in System Intrusion incidents [1]

In 2021, Supply Chain breach was responsible for 62% of System Intrusion incidents.

A force multiplier leading to wide ranging consequences.

In a highly connected world, where businesses rely on partners or third parties, they are vulnerable to backdoors

(1) Verizon Data Breach investigations report, 2022

From Walled Garden to Wild West

Distributed Workforce

Work from Anywhere

775% Microsoft's cloud services adoption growth rate at the heights of covid-19 lockdowns

Today's distributed reality

- Remote workers using unapproved devices and network access that avoids underperforming VPN
- Accelerated adoption of multi-cloud services and SaaS and often shadow IT using unsupported cloud applications
- Haphazard security protocols
- Workforce highly susceptible to malware, phishing, and botnet attack vectors

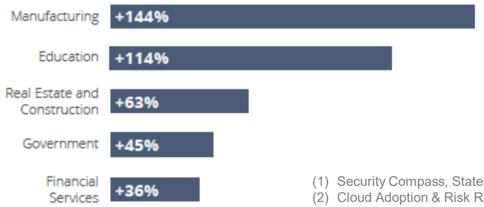
Distributed Assets

Accelerated Cloud Adoption

52% Software applications being developed by enterprises are cloud based [1]

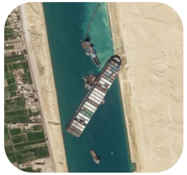
30% On-premise applications are expected to migrate to the cloud within next 2 years [1]

% increase in Enterprise Cloud Service use by vertical [2]



Diverse Inter-connections

Diversifying Supply Chain



- While diversification of your supply chain is in itself a risk management strategy, third-party suppliers introduces risk exposure
- Rise of supply chain attacks
- Risks from supply chain:
  - Poor security practices
  - Secure-by-design practices
  - Vulnerability disclosure & penetration testing
  - Access and privileges
  - Fourth-party risk

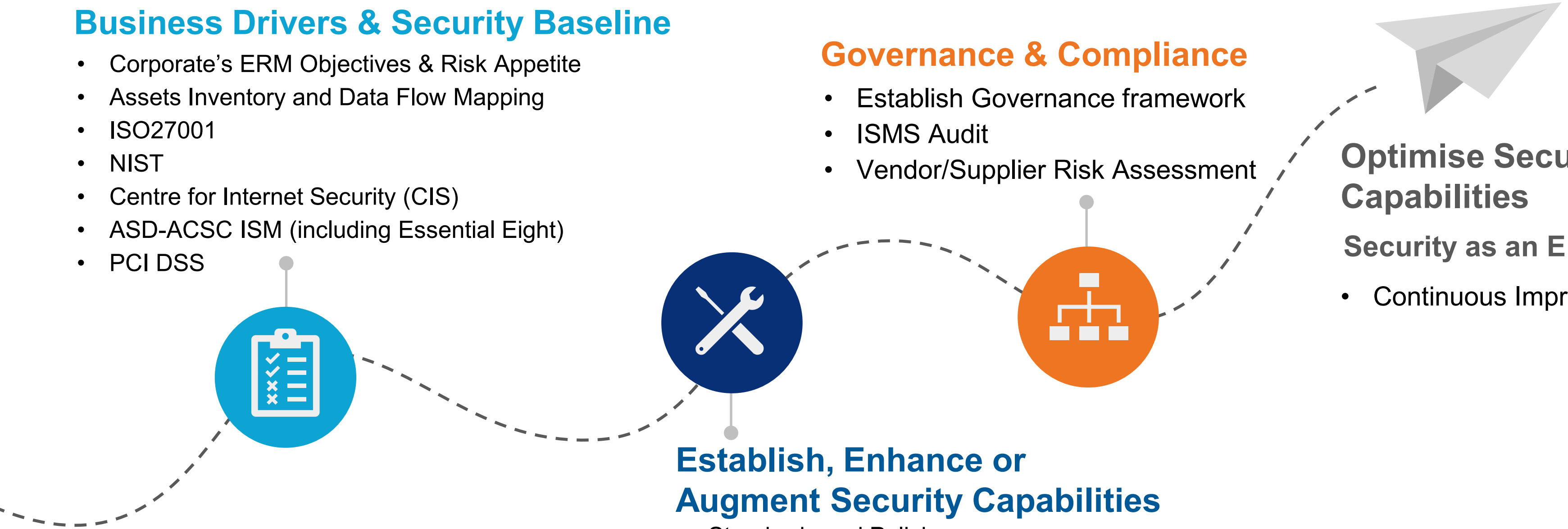
[1] Security Compass, State of Cloud Adoption in 2021

[2] Cloud Adoption & Risk Report: Work from Home Edition, Deloitte,

LUMEN®

Re-assessing your Cybersecurity Strategies

Building a Security Roadmap



Business Drivers & Security Baseline

- Corporate’s ERM Objectives & Risk Appetite
- Assets Inventory and Data Flow Mapping
- ISO27001
- NIST
- Centre for Internet Security (CIS)
- ASD-ACSC ISM (including Essential Eight)
- PCI DSS

Establish, Enhance or Augment Security Capabilities

- Standards and Policies
- Cyber Awareness Training
- Risk Treatments, secure cloud-based applications and Internet access, SASE
- Continuous Security Monitoring (SIEM/Logs, EDR/XDR, UEBA)
- Playbooks to detect faster, respond quicker, automate remediation

Governance & Compliance

- Establish Governance framework
- ISMS Audit
- Vendor/Supplier Risk Assessment

Optimise Security Capabilities

Security as an Enabler

- Continuous Improvement

Lessons from Healthcare

Overview

- Regional Healthcare system
- Two hospital locations
- 20 partner clinics providing lab and radiology
- Medical professional campus with partner services
- Multiple clouds containing shared applications
- One private data centre

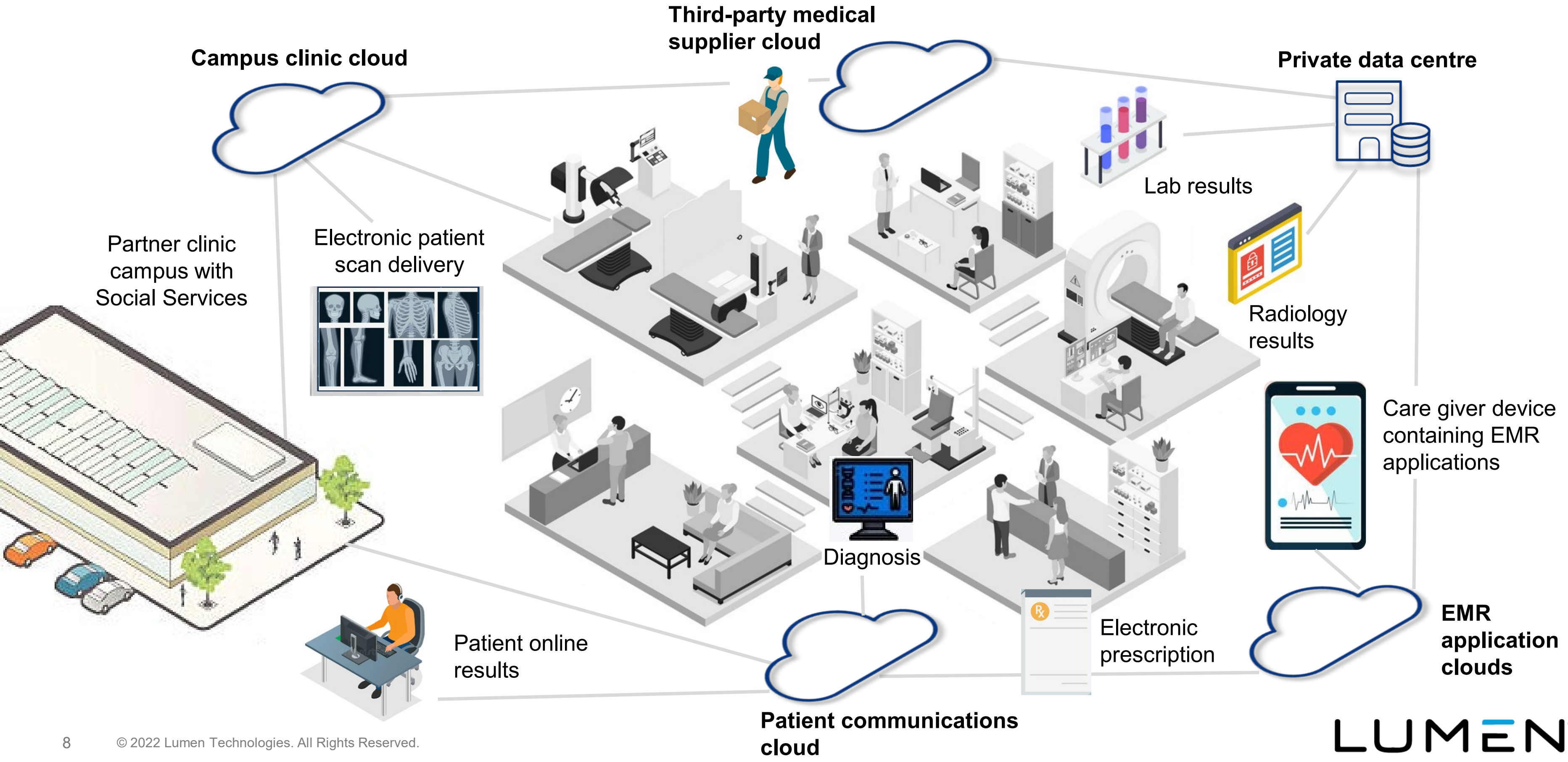
The challenge

Centralised data centre sharing PHI across multiple cloud-based applications. In response to COVID, the provider significantly increased its remote EMR application access to minimise patient impact on hospitals while maintaining optimal patient care.

The network and security approach needed to pivot to improve application performance and securely share compliant patient information while ensuring up-to-date accuracy.

Source: Lumen ITDM SASE Narratives. Quadrant Strategies. October 2021

Healthcare: A day in the life of Electronic Medical Records (EMR)


Third-party medical supplier cloud
Campus clinic cloud
Private data centre
Lab results
Partner clinic campus with Social Services
Electronic patient scan delivery
Radiology results
Care giver device containing EMR applications
Diagnosis
EMR application clouds
Electronic prescription
Patient online results
Patient communications cloud

Healthcare: Best Practices & Solutions

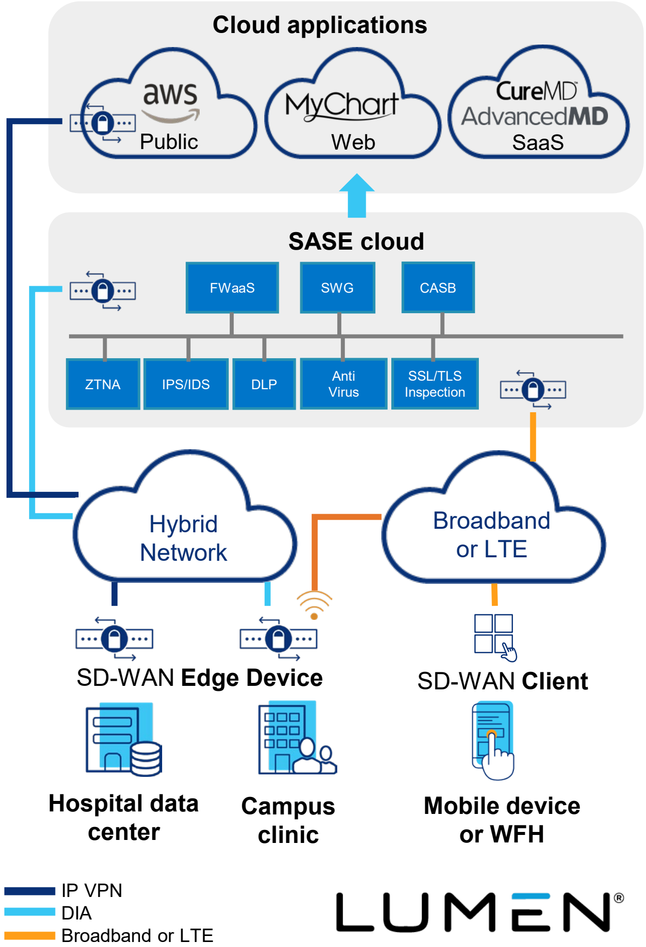
Leveraging on SASE to integrate, simplify and secure, high-performance delivery of EMR applications containing sensitive patient information. The solution combined Lumen private and dedicated internet connections to segment data centre traffic and share uninterrupted transport of critical data between their hospital and campus environments. Patient data collected across devices and diagnostics is privately shared while maintaining uninterrupted delivery.

Broadband and LTE mobile user traffic was secured and prioritised using ZTNA client access to the Lumen SASE secure cloud gateway providing end-to-end visibility and policy control from the device to the cloud application and end user.

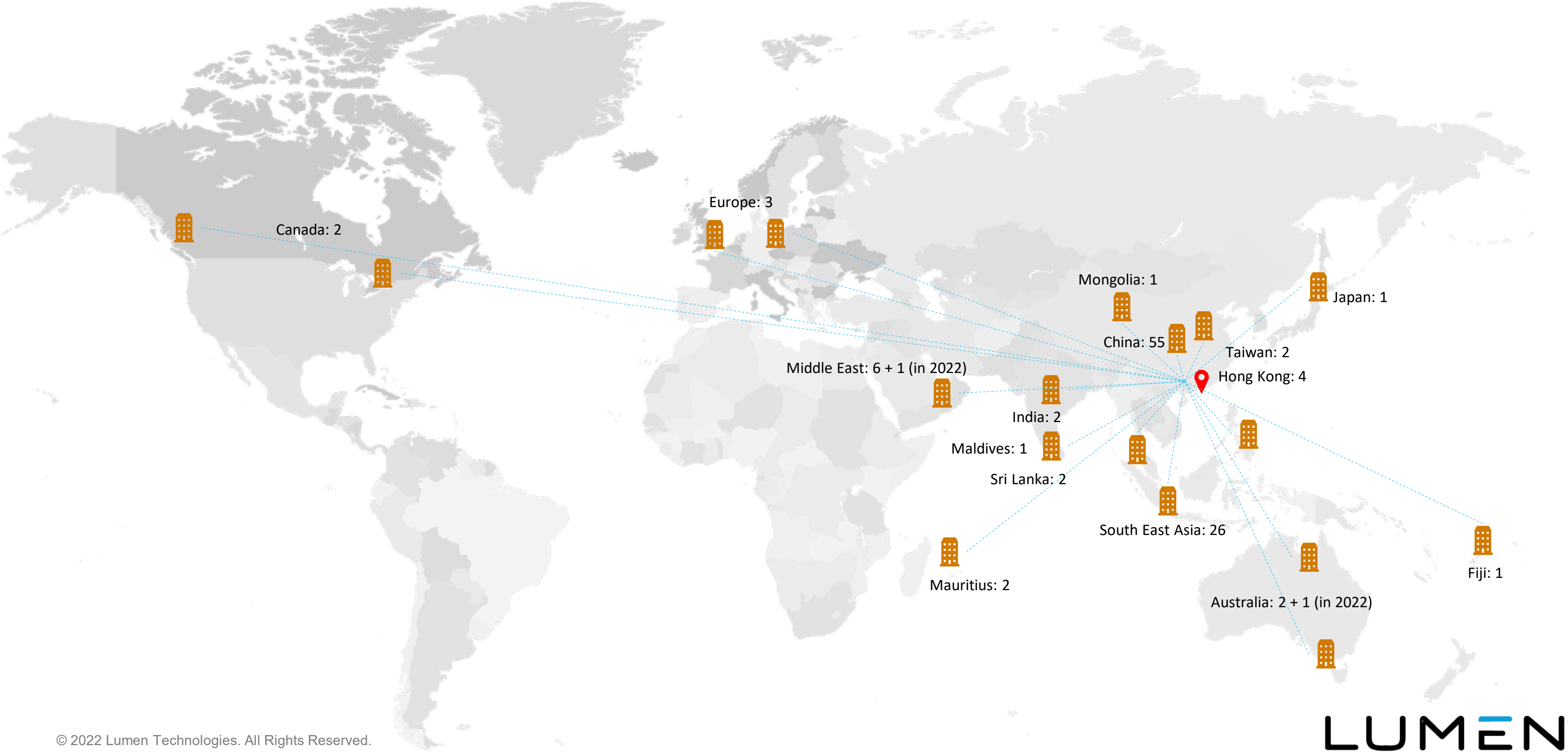
The cloud-native approach centralised policy management. Application performance improved by scrubbing traffic closer to the data source at the service edge and cloud gateways for mobile and remote users.

The outcome

- Lower infrastructure costs with single provider management
- Faster response to patient needs
- Secure sharing of PHI across multiple devices, users, and locations



Lessons from an International Hospitality Provider



Hospitality: Best Practices

Eliminate blind spots through Continuous Security Monitoring, collecting logs & events from their firewalls, network infrastructure, Domain Controllers, EDR, NDR, and other sources.

Ensure use cases coverage of TTPs through threat modelling and mapping to MITRE ATT&CK framework.

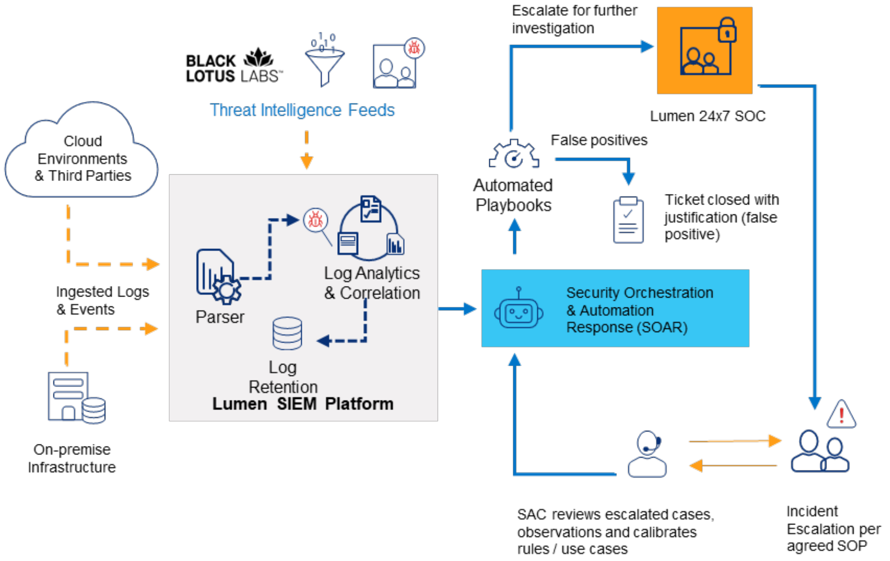
Security Advisory Consultant (SAC) as a trusted advisor to aid and augment internal capabilities and improve security posture.

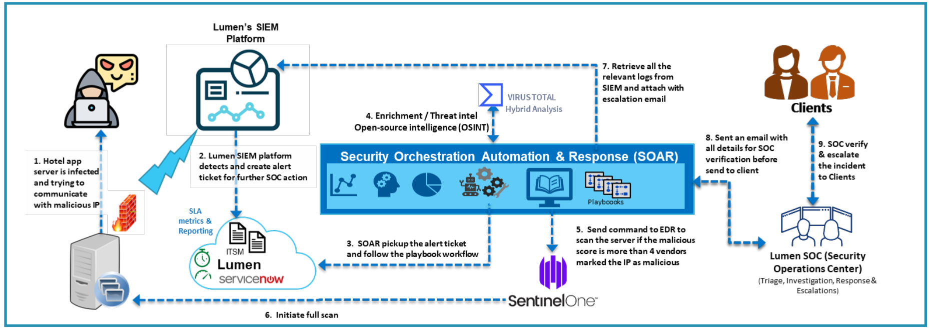
Continuous Improvement:

- Network segregation – guests & corporate networks
- Incident Response Plan review and improvement
- Annual Table-Top Exercise
- 24x7 threat monitoring, response and remediation

The outcome

- Improved Risk Mitigation & Security Posture
- SecOps Automation for rapid playbook orchestration and automation


Escalate for further investigation
Lumen 24x7 SOC
BLACK LOTUS LABS
Threat Intelligence Feeds
Cloud Environments & Third Parties
False positives
Automated Playbooks
Ticket closed with justification (false positive)
Ingested Logs & Events
Parser
Log Analytics & Correlation
Log Retention
Lumen SIEM Platform
Security Orchestration & Automation Response (SOAR)
On-premise Infrastructure
SAC reviews escalated cases, observations and calibrates rules / use cases
Incident Escalation per agreed SOP


Lumen's SIEM Platform
1. Hotel app server is infected and trying to communicate with malicious IP
2. Lumen SIEM platform detects and create alert ticket for further SOC action
SLA metrics & Reporting
ITSM
Lumen
servicenow
3. SOAR pickup the alert ticket and follow the playbook workflow
4. Enrichment / Threat intel Open-source intelligence (OSINT)
VIRUS TOTAL
Hybrid Analysis
Security Orchestration Automation & Response (SOAR)
Playboooks
5. Send command to EDR to scan the server if the malicious score is more than 4 vendors marked the IP as malicious
SentinelOne
6. Initiate full scan
7. Retrieve all the relevant logs from SIEM and attach with escalation email
8. Sent an email with all details for SOC verification before send to client
9. SOC verify & escalate the incident to Clients
Clients
Lumen SOC (Security Operations Center)
(Triage, Investigation, Response & Escalations)

LUMEN CONNECTED SECURITY

See More.

Stop More.

Connected Security.

We’d love to hear from you!

Scan Here

URL

https://www.lumen.com/en-au/security/analytics-and-threat-management.html

Email

apac.mail@lumen.com

Phone

+61 2 9006 1054

LUMEN®

The Platform For Amazing Things

This content is provided for informational purposes only and may require additional research and substantiation by the end user. In addition, the information is provided "as is" without any warranty or condition of any kind, either express or implied. Use of this information is at the end user's own risk. Lumen does not warrant that the information will meet the end user's requirements or that the implementation or usage of this information will result in the desired outcome of the end user. This document represents Lumen's products and offerings as of the date of issue. Services not available everywhere. Business customers only. Lumen may change or cancel products and services or substitute similar products and services at its sole discretion without notice. All third-party company and product or service names referenced in this article are for identification purposes only and do not imply endorsement or affiliation with Lumen.