Securelytics

Service Catalogue

Managed Security Service

www.securelytics.my

Securelytics

ABOUT OUR COMPANY

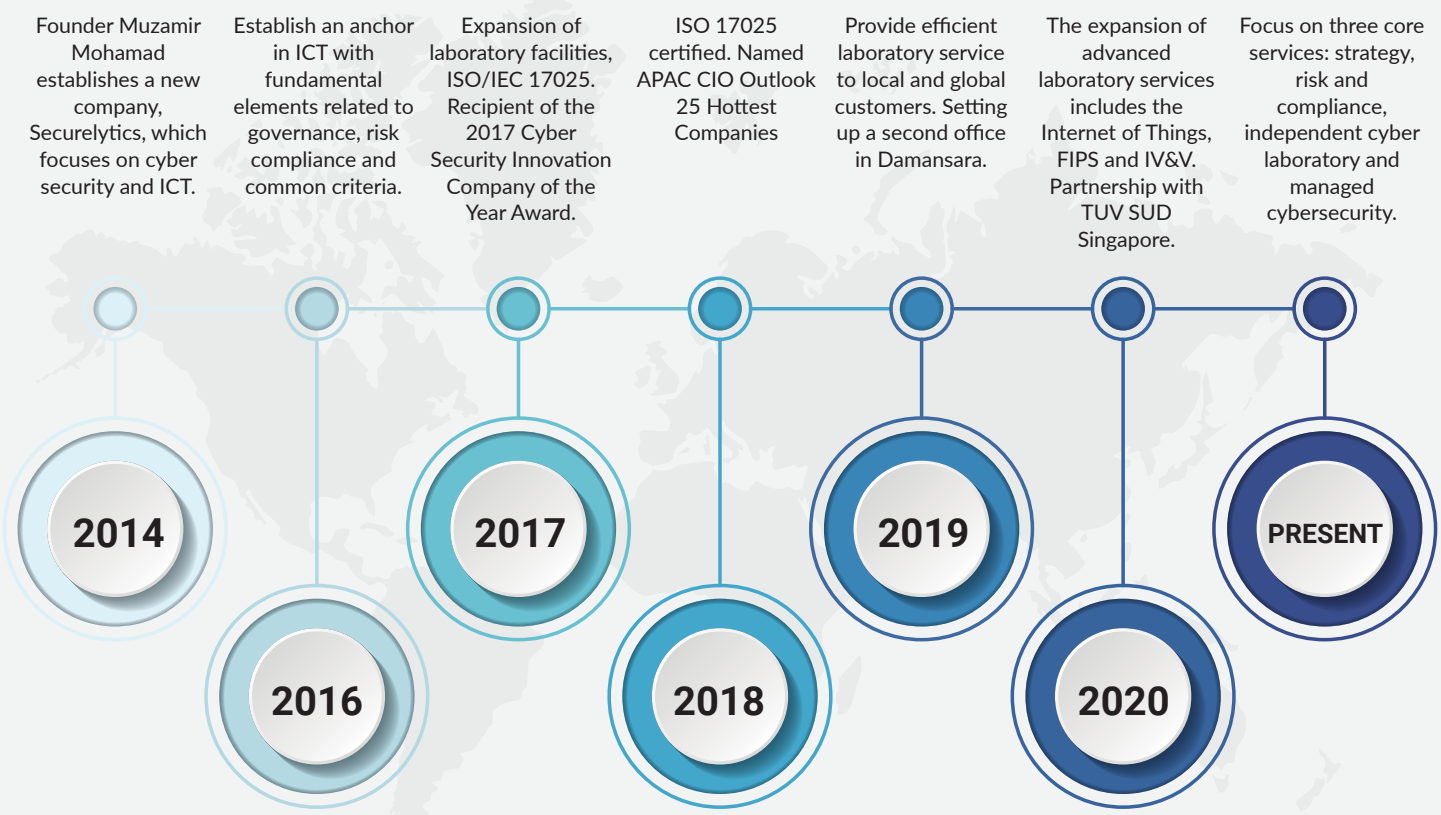
Securelytics is a robust and independent cybersecurity advisory firm with a proven track record in ensuring that we deliver high-quality ICT security advisory and testing services for commercial and government clients.

We deliver a wide range of capabilities – from risk assessments to regulatory and standards compliance. We also provide our clients with comprehensive recommendations to meet regulatory and compliance requirements, helping to make the entire process more efficient.

OUR TEAM

Our consulting and technical team has over 100 years of experience in IT security development, testing and evaluation. We have been on every side of the story, and we know how to tell it.

COMPANY HISTORY



Securelytics

SERVICES

MANAGED SERVICES

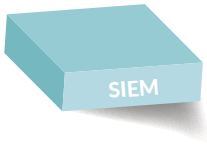
- Managed Detection and Responses (MDR)
- Managed Threat and Vulnerability Management (MTVM)
- Managed Threat Hunting (MTH)
- Managed Device Management (MDM)

PROFESSIONAL SERVICES

- Compromised Assessment (CA)
- SOC Maturity Assessment (SMA)
- Zero Trust Assessment (ZTA)
- Digital Forensic (DF)
- Cyber Security Incident Handling & Response (CSIR)
- Cyber Security Awareness-as-a-Services (CSA-aaS)

Securelytics

OUR SERVICES PILLAR



SECURITY INFORMATION EVENT MGT

Single pane of glass platform to analyze security data in real-time

USER & ENTITY BEHAVIOR ANALYTICS

Solutions that use analytics to build the standard profiles and behavior of users, assets and entities

USER & ENTITY BEHAVIOR ANALYTICS

Solutions that use analytics to build the standard profiles and behavior of users, assets and entities

USE CASES

Specific condition or event (usually related to a specific threat) to be detected or reported by the security tool inline with business requirement

THREAT INTEL

Specific condition or event (usually related to a specific threat) to be detected or reported by the security tool inline with business requirement

EXTENDED DETECTION & RESPONSE

Detection, threat hunting and response platform for Endpoint, Network and Cloud resources

VULNERABILITY MGT PLATFORM

Solution that automatically identify digital asset vulnerability that can be exploited (Attack Surface)

BREACH ATTACK SIMULATION

Automated solution to identify hidden attack paths, test control effectiveness & check configuration gaps

Securelytics

MANAGED SERVICES

Managed Detection and Responses (MDR)

- 24 x 7 remotely delivered focused and rapid monitoring, detection, analysis, response and containment services
- Provide visibility at the endpoint, host, network, application and, increasingly, the cloud services layers
- User behavioural analytics as visibility enrichment
- Improve MTTD & MTTR leveraging automation and Ai driven analytics
- Augmented by full stack of the core SOC technology components
- Combined with the knowledge of threat intelligence, alerts triage, threat hunting, incident response and digital forensics

Managed Threat and Vulnerability Management (MTVM)

- 24 x 7 remotely delivered focused and rapid monitoring, detection, analysis, response and containment services
- Provide visibility at the endpoint and host only (include network with XDR)
- Augmented by the XDR / EDR and Threat Intelligence SOC technology component
- Combined with the knowledge of threat intelligence, threat hunting, incident response and digital forensics

Managed Threat Hunting (MTH)

- Managed Threat Hunting as-a-a service offers round-the-clock monitoring from CSM experts to discover attacks anywhere in client's organization. Our threat hunters work on your behalf to discover advanced threats, such as state-sponsored attackers, cybercriminals, malicious insiders, and malware.

Live Forensic Analysis

Hunt and detect advanced persistent threats and fileless malware with historical and automated live memory forensic analysis.

Continuous Monitoring

Combined with hiostorical data, DivisionIQ continuous monitoring helps incident response teams investigate and remediate advances threats.

Speedily Incident Response

Extensible response options enable security teams to quickly isolate hosts, analyze unknown threats, and respond to security incidents at scale.

Securelytics

PROFESSIONAL SERVICES

Bil	Professional Services	Key Deliverables
1	Compromised Assessment (CA)	Agent-based compromise assessment using Cortex™ XDR for quick and easy analysis of active and on-going attack or unknown breaches. Services is bootstrapped with iQ36™ threat intelligence capability.
2	SOC Maturity Assessment (SMA)	Securelytics will conduct gap analysis on the SOC to assess the maturity level based on international best practices and assist client to develop a roadmap to achieve improved maturity across time. Our maturity assessment model consists of five domains across Business, People, Process, Technology and Services and any other critical aspects.
3	Zero Trust Assessment (ZTA)	Zero Trust Assessment tests your network's adherence to the components of Forrester Zero Trust framework and generates a free status report with actionable recommendations to help you prioritize your Zero Trust decisions. Segmentation and micro-segmentation – Test for cross segment traffic both automatically and per user defined segments
4	Digital Forensic (DF)	Digital investigations may be considered a bespoke service that provides answers to specific customer questions e.g., has the user been accessing inappropriate internet sites? Where and how has a user obtained monies as part of a fraud? Or they may be considered as integral to, or a support function of a Computer Security Incident Response function or eDisclosure (styled eDiscovery in the US) exercise. It involves the deep technical analysis of systems and infrastructures to identify useable evidence in support of the case at hand. It is achieved using a number of Disci-plines including: • Static Computer Forensics • Live Computer Forensics • Network Forensics • Remote Forensics
5	Cyber Security Incident Handling & Response (CSIR)	

Securelytics

TECHNOLOGY PARTNER & ALLIANCE

Securelytics

OUR LAB

A-19-06 Tower A, Atria SOFO Suites,
Jalan SS22/23, Damansara Jaya,
47400 Petaling Jaya,Selangor, Malaysia

CORPORATE OFFICE

A-17-01 Tower A, Atria SOFO Suites,
Jalan SS22/23, Damansara Jaya,
47400 Petaling Jaya,Selangor, Malaysia

E-MAIL

info@securelytics.my

CONTACT NUMBER

+6012366786

WEBSITE

www.securelytics.my