
CYBER100
National Cybersecurity
Innovation Challenge Program

TABLE OF CONTENTS

Contents		Pages
01	**INTRODUCTION**	**01**
02	**PREFACE**	**02 - 03**
	NACSA	02
	MDEC	03
03	**CYBER100 PRODUCTS AND SERVICES**	**04 - 41**
	MANAGE SECURITY SERVICES PROVIDER	
	Nexagate Sdn. Bhd.	06
	SysArmy Sdn. Bhd.	07
	NetAssist (M) Sdn. Bhd.	08
	Provintell Technologies Sdn. Bhd.	09
	Securelytics Sdn. Bhd.	10
	HeiTech Padu Berhad	11
	THREAT INTELL / DASHBOARD	
	TecForte Sdn. Bhd.	13
	Nexagate Sdn. Bhd.	14
	IDENTITY MANAGEMENT / PRIVILEGED ACCESS MANAGEMENT	
	Securemetric Technology Sdn. Bhd.	16
	SecureKi Sdn. Bhd.	17
	DNS & END POINT PROTECTION	
	CYSECA Sdn. Bhd.	19
	e-Lock Corporation Sdn. Bhd.	20
	DNSVault Sdn. Bhd.	21
	TOOLS DOCUMENT SIGNING / OTP	
	SigningCloud Sdn. Bhd.	23
	SecureKi Sdn. Bhd.	24

Contents Pages

CLOUD SECURITY

Vigilant Asia (M) Sdn Bhd 26
Nexagate Sdn. Bhd. 27
Securemetric Technology Sdn. Bhd. 28
SecureKi Sdn. Bhd. 29
e-Lock Corporation Sdn. Bhd. 30
Netbytesec Sdn. Bhd. 31
DNSVault Sdn. Bhd. 32
EC-Council Cyber Defense Sdn. Bhd. 33
Cydentiq Sdn. Bhd. 34
Advance Product Design Sdn. Bhd. (Biocryptodisk) 35
Infinity Consulting Technology Sdn. Bhd. (Aegis) 36
Firmus Sdn. Bhd. 37
Securelytics Sdn. Bhd. 38
Provintell Technologies Sdn. Bhd. 39
TecForte Sdn. Bhd. 40
SysArmy Sdn. Bhd. 41

04 **SUCCESS CASES** **42 - 49**

Provintell Technologies Sdn. Bhd. 43
Securemetric Technology Sdn. Bhd. 44
HeiTechPadu Berhad 45
DNSVault Sdn. Bhd. 46
TecForte Sdn. Bhd. 47
Nexagate Sdn. Bhd. 48
SigningCloud Sdn. Bhd. 49

05 **SUPPORTED AGENCIES** **50**

01 INTRODUCTION

As the digital economy takes centre-stage around the world, the demand for a safe and secure cyberspace has also grown exponentially.

In order to meet the ever-growing demand of cybersecurity solutions, the Malaysia Digital Economy Corporation (MDEC), in collaboration with the National Cyber Security Agency (NACSA), is initiating the National Cybersecurity Innovation Challenge Program (Cyber100).

The Cyber100 initiative will host numerous cybersecurity challenges on a national scale. Its goal is to seek solutions for industry-specific problems while promoting the creation of local innovative technologies. This will further strengthen Malaysia's information security community and position as a digital hub for this sector.

Significant innovations can be developed when talented people look past the obvious. Think big. Think outside the box.

Solving National Challenges

Validating Challenges from key stakeholders

Top 10 national cybersecurity challenges

Accelerate Cybersecurity Adoption

Develop and pilot adoption programs

Create and curate local supplier scheme listing

Access to Cybersecurity Community

Mentor and subject matter expert to support the innovation

Awareness program for key stakeholders

Convergence of Technologies

Identify and address potential security challenges

02 PREFACE

NATIONAL CYBER SECURITY AGENCY

Cyber security has become an emerging discipline and has driven the focus of many organizations as well as government to invest in advanced security solutions. With the increasing number of cyber security threats, the need for advanced cyber security solutions is crucial. The common cyber security solutions are not enough accomplished of securing the organizations from advanced threats of cloud, network and endpoint security, among others. Besides, high cost associated with cyber security solutions and services limits the adoption among small and medium enterprises.

In order to handle this issue, National Cyber Security Agency, National Security Council (NACSA, NSC) as the national lead agency for cyber security, has planned to spur cyber security innovation and research and development (R&D) by local industry players. A collaboration between NACSA and MDEC will help to create a conducive domestic environment for innovation and R&D.

A program like Cyber100 is a good initiative to encourage innovation, while at the same time promoting a competitive local industry and technology. We hope that this program will be a continuous program and more programs alike will be planned in the near future.

Malaysia Cyber Security Strategy (MCSS) 2020-2024

PILLAR 1
Effective Governance and Management

PILLAR 2
Strengthening Legislative Framework and Enforcement

PILLAR 3
Catalysing World Class Innovation, Technology, R&D and Industry

PILLAR 4
Enhancing Capacity and Capability Building, Awareness and Education

PILLAR 5
Strengthening Global Collaboration

MALAYSIA DIGITAL ECONOMY CORPORATION

Over the past several years, we have witnessed the extraordinary growth of the digital economy. The Internet has rapidly grown into an area where people share ideas, learn new skills, and provide towards and learn from the vault of human knowledge. As is, digitisation is how businesses increase productivity and stimulate innovation.

As MDEC is the lead government agency to drive forward Malaysia's digital economy, it plays a catalytic role in shaping its future. Its role includes empowering local businesses and the Malaysian people with the right tools, proper education and providing all with access to resources needed that can help them reap the endless benefits of digital technologies and services.

Cyber100 is Malaysia's First Cybersecurity Innovation Challenge Program. The initiative includes various awareness and innovation platforms and services that help develop and enhance national cybersecurity capacities and capabilities.

MDEC will keep on doing its utmost to promote the development and deployment of local technologies and establish as well as expand a competitive local cybersecurity industry

Empowering Malaysians with digital skills 01

Enabling digitally-powered businesses 02

Driving digital sector investments 03

CYBERSECURITY COLLABORATION

The Cyber100 Challenge was launched in November 2019 in the hopes of building a better connected and more secure nation. Began with entry submissions from various companies, of which only the companies with the strong solution and meet the requirement were shortlisted.

These companies then participated in an orientation program, whereupon the companies updated committee members of their progress. In return, the committee members guided and advised these participants accordingly. After the orientation period, the companies were required to present and demonstrate their challenges and proposed solutions. The demonstration gave them the opportunity to receive feedback and comments on their respective solutions.

By the end of the Cyber100 Program, there is the golden opportunity for the solutions that the companies presented to undergo pilot testing and be adopted by other agencies with help from the supporting ecosystem partners.

SECUREKI · CYSECA · net NETASSIST · SigningCloud

SysArmy · nexagate · Provintell

Securelytics · HeiTech SECURE-X Powered by HeiTech · eLock

Tecforte SMARTER CYBERSECURITY · DNSVAULT · SECURE METRIC TECHNOLOGY

FIRMUS · VIGILANT ASIA YOUR CYBERSAFETY IS OUR PRIORITY · aegis

NETBYTESEC SECURING YOUR DIGITAL ASSETS · EC-Council Cyber Defense · CYDENTIQ · Biocryptodisk

03 CYBER100 PRODUCT& SERVICES

MANAGE SECURITY SERVICES PROVIDER

- A managed security service provider (MSSP) **provides outsourced monitoring and management of security devices** and **systems**. It maintains organizations' security controls, tools and processes.
- Some of the services that could be obtain via an MSSP include, application management services, which are designed to provide for the day-to-day operations, support, and maintenance of enterprise security applications.
- It's also contain several discrete components; end user support, proactive and reactive application maintenance, proactive application enhancements, and remote onsite application monitoring.

https://www.gartner.com/en/information-technology/glossary/mssp-managed-security-service-provider

nexagate

Nexagate is one of Malaysia's leading cybersecurity service providers. For 13 years, we have delivered trusted security solutions to 400+ organisations across critical sectors within ASEAN. Nexagate offers a complete range of cybersecurity services that has been certified with ISMS ISO/IEC 27001 since 2012. This includes Security Risk & Compliance, Offensive Security, and Managed Security Services which are delivered with seamless digital experience via our own patent-pending and award-winning NSI Unified Security Management Platform.

Challenges VS Services

1. **No cybersecurity expertise in-house** to handle threats effectively.
2. **Lack of visibility and control** leads to delayed threat responses.
3. **Complex evolving cybersecurity threats** with new ones emerging every day.
4. **Strict Compliance Regulations** require security measures for sensitive data protection.
5. **Limited resources (budget or staff)** for robust security measures.

Nexagate Managed Security Services, include:

- Strengthen risk, comply with ISMS ISO/IEC 27001, expert consultants.
- Assess security with CREST-accredited vulnerability testing by the offensive team.
- Defend and protect against data breaches with our 24/7 security operation centre
- Gain visibility on cybersecurity with NSI Unified Security Management Platform.
- Rest assured that all of Nexagate's services comply with ISO 27001 standards.

Solutions

"Nexagate offers Complete, Modular, and On Demand Services via a Platform. Their capable Security Consultants and Analysts deliver solutions that protect your critical information round the clock, leveraging on state of the art technologies."

- SOC as a Service
- Web Security as a Service
- Compliance as a Service
- Brand Monitoring as a Service
- Compromise Assessment as a Service
- Penetration Testing as a Service
- Managed Detection and Response as a Service
- Incident Response as a Service
- Cyber Awareness as a Services

Since 2012
Certified
ISMS ISO/IEC 27001
Global Standard

Since 2019
Certified
CyberSecurity Malaysia
PTSP

Since 2020
Accredited
CREST
200th Member

www.nexagate.com sales@nexagate.com

SysArmy

Cyber 100 03

SysArmy is a key player in the Security Operation Centre (SOC) market. They also provide cybersecurity consulting & professional services to its clients. Their primary goal is to ensure clients are well prepared whenever a cyber security attack or outbreak occurs. This can be achieved through real time security analytics, periodic assessment on critical infrastructures, as well as continuous effort to improve organizational processes.

Challenges VS Services

Challenges

1. **People**: **Lack of Expertise**
   - Less than 5,000 certified professionals for the market
   - Talent development are too focused on technical training
2. **Process**: **Policies & Standard**
   - Lack of policies and standard applicable to local context
   - Policies are created on ad hoc basis often after audit findings to address particular gaps
3. **Technology**: **Considerable Investments**
   - Allocated budget is way beyond technical and functionalities requirement.

Services

1. **Building Best Practice:**
   - Help clients establish their own practices be it as a line of defenses; or as a business unit
2. **Assurance Execution:**
   - Assurance related services such as assessments / reviews on technical domains
3. **Process, Risk & Control:**
   - Conduct audit / training / awareness programs on operational, technological and cybersecurity domains

Solutions

"**SATRIA,** SysArmy Threat Research and Intelligence Alliance"

Strategic
Satria Alliance
- FSISAC
- Brand Monitoring

Tactical
Satria Feed
Satria Exchange

Operational
Satria Standard

2015
ISO27001:2013

2016
Cybersecurity Malaysia Innovation of the Year (NGSOC)

2018
CREST certification

2018
Award winning 2nd NGSOC Malaysia

NETASSIST

NETASSIST (M) SDN BHD

NetAssist is a Managed Security Services Provider. We protects customer from cyber threats in multiple ways depending on the nature of threats either thru our 27x7x365 Security Operation Center (SOC), or Professional security services Team for Penetration Testing, Incidents Response, Security Consultancy Services, Training or with our Security Engineering team to deploy Security Solutions.

Challenges VS Services

1. **Shortage** of cyber security **Talents**
2. **Keep updated** with the various cyber security technologies
3. **Paying higher** than usual **cost** for cyber threats **protections**
4. **Without proper total solutions** that shall encompasses People + Process + Technology

1. **Discoveries, Assessments & Recommendations**: enabling organizations to understand their current level of security resilience
2. **Protect & Detect**: Based on the risk assessments, various strategies encompass People + Process + Technology will be deployed and managed for the organizations
3. **Continuous Monitoring**: NetAssist provide holistic continuous cyber threats monitoring to ensure organizations stay protected continuously without the heavy capex burden

Solutions

> As a Managed Security Services Provider (MSSP), we are brand agnostic and always combine the best-of-breed solutions to more practically address the needs and accurately solve the issues faced by our clients.

- Vulnerabilities Assessment & Penetration test
- Compromise Assessments
- Source Code Security Scanning
- ISMS (ISO27001 Consultancy)
- Consultancy and Security Framework
- 24x7 Security Monitoring via Security Operation Center (SOC)
- Training and Talent Resources
- Managed Security Devices/ Solutions
- Managed Patch Services
- Managed Detections and Response Service

2019
ISO27001:2013

2019
Cybersecurity Malaysia Innovation of the Year (Hybrid Managed Detection & Respond Services)

2019
CREST certification

2020
Frost & Sullivan 2019 Managed Security Service Provider Best Practices Award.

www.securelytics.my info@securelytics.my

Provintell

PROVINTELL is an emerging Managed Security Service Provider (MSSP) and CyberSecurity-as-a-Service Provider (CSaaS) in the region, specializing in Next-Gen Cyber Defense and Response by utilizing the latest Open XDR with Machine Learning / Artificial Intelligence (XDR Kill Chain) technologies to hunt, detect and respond to threats in the most complex environment.

PROVINTELL'S 24x7 Next-Gen CyberSOC is fully managed by our in-house certified cyber security specialists who are highly skilled in threat hunting, incident response, red teaming and penetration testing. We employ 'Threat Intelligence As First Line of Defense' by continuously assessing the attack surface, data breach and exposure risk of our customers, known as the threat and vulnerability intelligence to enhance our CyberSOC capabilities in orchestrating the most effective cyber defense and response strategies against the latest and sophisticated cyber threats.

Challenges VS Services

Cyber defense is getting harder. How does an organization efficiently respond to cyber threats without breaking the bank?

1. **Too Many Tools**
   - Tools are failing
2. **Not Enough People**
   - Skills gap and human error
3. **Too Much Data**
   - Data and alert fatigues

1. Managed Extended Detection and Response (MXDR)
2. External Attack Surface Management (ASM)
3. Vulnerability Management and Security Validation (VM)
4. Adversary Emulation Program (Red Teaming)
5. Penetration Test (VAPT)
6. DevSecOps Managed Application Security Test
7. Compromise Assessment and Incident Response

Solutions

"**Threat Intelligence** As First Line of Defense"

CODEREDASM

Security Intelligence
External
Attack Surface Management (ASM)

PenTestBOX

Exposure Reduction
Vulnerability Management (VM)
and Security Validation

MXDR

Detection & Response
Managed Extended Detection
and Response (MXDR)

2019
ISO/IEC 27001:2013

2018
Technical Codes Drafting Leader
for Malaysian Technical Standards
Forum Berhad (MTSFB)

2020
AT&T
Cyber Security MSSP

2022
Stellar Cyber Government
MSSP Partner of The Year &
Stellar Cyber Fastest
Growing MSSP Award

www.provintell.com info@provintell.com

Securelytics

Securelytics is an independent cyber security and consulting firm. Businesses, critical infrastructure, governments and consumers around the world rely on our cutting-edge threat intelligence to protect them from cyber attacks. They aim to deliver tailor-made services, to solve and support our clients' businesses in creating a secure ICT environment while enabling them to operate smarter.

Challenges VS Services

1. **Recruiting and retaining security personnel:** The market lacks qualified security candidates, making recruitment and retention difficult.
2. **Transforming the way organizations consume IT:** Many firms are shifting to SaaS-based cloud services, which do not interact with traditional security monitoring systems handled by MSSPs. This leaves the managed service provider maintaining numerous security technologies, or gap in coverage and visibility into security risks.
3. **Lack of resources to deliver threat hunting and incident response services:** Many MSSPs just provide security log monitoring, which limits security incident investigations.

Securelytics' Managed Security Services (MSS)

1. Provide intelligence-driven security services that are available 24x7, 365 days to maximise resource efficiency and reduce response time.
2. Uses tried-and-true processes and technologies to reduce false positives and false negatives
3. World-class intelligence laboratories regularly conduct advanced threat and cyber- attack analyses, feeding intelligence into our technologies and services.

Solutions

Advancing The Evolution, A comprehensive end-to-end cyber security solutions provider that move you forward, faster.

Managed Security Services
For today's hybrid multi cloud world

Cybersecurity Lab and Testing
Staying ahead of cyber criminal

Strategy, Risk & Compliance
Meet requirements, comply with standards

Software & Hardware Integration
Extensive software and hardware integration services.

2017
Cyber Security Innovation Company of The Year

2018
25 Hottest Companies APAC CIO Outlook

2020
Partnership with TUV-SUD Singapore

2022
Cyber Security Company of The Year

www.securelytics.my info@securelytics.my

HEITECH PADU & SECURE-X

Secure-X provides leading-edge managed security services solutions with the aim of helping clients achieve their digital transformation goals by unlocking value from the latest cyber security technologies. Our unique Risk-Driven Malaysia Cyber Security Strategy (MCSS) services help businesses turn cyber threats into competitive advantages.

Challenges VS Services

Cyber risk is a systemic challenge and cyber resilience is a public good

1. **Threat Exposure:**
   - Governance
   - Complexity
2. **Visibility:**
   - Risk
   - Vulnerability
3. **Attack Spectrum:**
   - Compliance
   - Skill Sets

Make Habitual Security a Daily Practice Today with Secure-X 'R.A.V.E'

1. **Be (R)eady** - Be prepared for upcoming cyber threats with Strategic Monitoring, Orchestration and Optimization
2. **Be (A)gile** - Predict, prevent, detect and correct potential cyber security issues with Threat Hunting.
3. **Be (V)igilant** - Prevent future attacks by reducing cyber exposure with Forensic Investigation and Threat Intelligence.
4. **Be (E)fficient** - Resolve cyber security issues and recover your lost data with Incident Response.

> "Always be prepared for cyber threats with Habitual Security."

Solutions

prescribePod
Tailored organization's cybersecurity design landscape and deploy according to the best practice and proven technology

practisePod
Manage policies, controls, risks, assessments, and deficiencies across your entire business.

curePod
Intelligence-driven and people-enhanced SOC with Risk-Based Vulnerability Management (RBVM) to increase the protection from cyber security threats

cyberKnowledgePod
Bridge organization's cyber security skills gap with exclusive training courses, certifications and real-world exercises led by top experts in the field

2006
ISO/IEC 27001:2013 Information Security Management Systems

2018
Malaysia Cyber Security Awards Cyber Security Innovation of the Year (Service)

2018 & 2019
Frost & Sullivan Managed IT Infrastructure Service Provider of the Year

2019 & 2020
Frost & Sullivan Malaysia Managed Security Service Provider of the Year

2022
Malaysia Technology Excellence Award – Cybersecurity IT Service

https://www.secure-x.my securex@heitech.com.my

03 CYBER100 PRODUCT& SERVICES

THREAT INTELL / DASHBOARD

Solutions that make threat intelligence actionable in an automated way.

- Security information and event management (SIEM) solution operationalize Threat Intelligence.
- SIEM solution include products designed to aggregate data from multiple sources, which are the used to identify patterns of events that could lead to cyber-attacks, intrusions, misuse, or failure.
- SIEM tools also collect, disseminate, and curate threat intelligence, provide early warning threat services, and can provide information on countermeasures.
- Security dashboard to ensure compliance, gain threat visibility & improve protection

Tecforte is an award-winning company that specialises in Cybersecurity Information and Threats Management. With over 15 years of dedicated focus, our solution has been leveraged to create better and stronger cyber defence and resilience among Governments and all critical Industries.

Challenges VS Solutions

1. **Cybersecurity** Management becoming more and **more challenging**!
2. **Too many new devices** and new cyber threats to manage and monitor.
3. **Lack of resources** and tools, many fail to process security events and attacks in real-time.

As it has become the universal approach for critical security operations worldwide to adopt SIEM and TIP - Security Information and Event Management, and Threat Intelligence Platform - Log Radar makes your cybersecurity operations more secure and sustainable. It provides an All-In-One appliance, combining everything you need to manage cybersecurity effectively.

Solutions

> …our experience and domain expertise have been leveraged to create stronger cyber defense and resilience among Governments alongside key Industries in the region.

- **Proactive Global Threat Intelligence**
  Priorities incident response and patching
- **Full Coverage of Data Collection**
  Leave no blind sports in monitoring scope
- **Easy Compliance to ISO27001**
  Maintain and upkeep organization's compliance level
- **Strong Advance Analytics**
  Better information management and team collaboration
- **Integrated Incident Management**
  Better information management and team collaboration

2013
Common Criteria EAL2 Certification

2015
Malaysia's Cybersecurity Company of the Year 2015

2018
Malaysia's Cybersecurity Product of the Year 2018

2019
Malaysia's Cybersecurity Professional of the Year 2019

www.tecforte.com sales@tecforte.com

nexagate

Cyber 100. Cohort 03

Nexagate is one of Malaysia's leading cybersecurity service providers. For 13 years, we have delivered trusted security solutions to 400+ organisations across critical sectors within ASEAN. Nexagate offers a complete range of cybersecurity services that has been certified with ISMS ISO/IEC 27001 since 2012. This includes Security Risk & Compliance, Offensive Security, and Managed Security Services which are delivered with seamless digital experience via our own patent-pending and award-winning NSI Unified Security Management Platform.

Challenges VS Services

1. Lack of visibility and control leads to delayed threat responses.
2. No cybersecurity expertise in-house to handle threats effectively.
3. Complex evolving cybersecurity threats with new ones emerging every day.
4. Strict Compliance Regulations require security measures for sensitive data protection.
5. Keeping up with a variety of technologies to be adopted to ensure ROI.

NSI Unified Security Management

- Show cybersecurity insights to stakeholders covering major pillars.
- Manage ISMS compliance from documentation to certification audit.
- Implement and track risk management from asset ID to treatment plan.
- Identify gaps in cybersecurity based on ISO 27001 and Bank Negara's RMIT.
- Plan and track security assessment findings remediation.
- Understand deployed security solutions for web apps and endpoints.
- Get daily intelligence on cyber threats and vulnerabilities affecting you.

> Our platform enables organisations to enhance their cybersecurity posture by providing visibility to critical insights, managing compliance activities, tracking risk management, identifying gaps, planning remediation, and delivering daily threat intelligence insights.

Solutions

Compliance Manager
View Risk Compliance Implementation
. Compliance Dashboard (ISMS / RMiT)
. Gap Analysis
. Documentation & Records Management
. Risk Heat Map and Management
. Audit Tracking

Threat Manager
View Actionable Threat Insights
. Threat Dashboard
. Asset Discovery
. On Demand Scanning
. Remediation Planning
. Report Archive

Protection Manager
View Security Solution Insights
. Protection Dashboard
. Incident Management
. Endpoint Protection
. Website Health & Security
. Report Archive

Since 2012
Certified
ISMS ISO/IEC 27001
Global Standard

Since 2020
Conformance
ISO 27017:2018
Cloud Service Provider

Since 2021
Malaysia Technology
Excellence Award
Computer Software

www.nexagate.com sales@nexagate.com

03 CYBER100 PRODUCT& SERVICES

IDENTITY MANAGEMENT / PRIVILEGED ACCESS MANAGEMENT

Products that enable the centralize operations, integration, and management the end user access control

- Identity and digital trust software such as authentication software incorporate public key infrastructure as well as software tokens and software designed to support hardware authentication solutions (tokens, smart cards, and biometrics).
- Single sign-on, multi-factor authentication (MFA) to enhance the risk posture and obtain greater assurance of the user identity.
- Privileged Access Management (PAM) provides restricted password vaults, ephemeral or just-in-time credentials, user session monitoring and recording, and more fine-grained authorizations

Securemetric is the leading cybersecurity company in Southeast Asia and they are listed on the ACE Market of Bursa Malaysia Securities. They are pioneers in setting up Certificate Authorities (CA) across the region with strong in-house R&D capabilities in Digital Signature, Time Stamping and Authentication Solutions utilising PKI (Public Key Infrastructure) technologies.

Securing Digital Identities

Securing Transactions

Securing Applications

Challenges VS Solutions

1. **Concerns on identity theft**, **data security**, login password security and system integrity.
2. Remote working policies and accessing office environments using personal devices (**BYOD**).
3. **Weak VPN authentication** and de-centralised authentication management.
4. Compliance to regulatory requirements.

1. **Made in Malaysia**: TechnoFund from Ministry of Science, Technology and Innovation (MOSTI) of Malaysia in 2015.
2. **First in Malaysia**: Common Criteria EAL4+ Certification. First in Southeast Asia: FIDO2 certified in JAPAN.
3. Adaptive Intelligence (AI) with Risk Scoring: Prevention of unauthorized access through behaviour study.
4. **Strong password-less authentication** with FIDO2 and PKI.

Solutions

CENTAGATE, Multi Factor Authentication Solution (MFA) and Single Sign On (SSO).

Security
Eliminate phishing, fraud and password theft.

Efficiency
Control, protect and secure all your applications through one login credential.

Compliance
Comply to PDPA and GDPR through MFA.

2017
Common Criteria EAL4+ Certification

2019
FIDO2® Certification

www.securemetric.com sales@securemetric.com

SECUREKI

SecureKi specialises in securing and managing credentials which helps many customers to stop targeted attacks, mitigate insider threats, achieve compliance, improve operations and secure the hybrid enterprise.

SecureKi solutions are designed and developed with futuristic and innovative security technologies designed to help organizations to secure and manage their enterprise passwords in an effective and automated way.

Challenges VS Product

As the integration of core infrastructure and business systems expand in the age of digital connectedness, safeguarding privileged access is imperative to avert data breach successfully and is a core requirement of multiple compliance regimes.

SecureKi Advanced Credential Management helps drive IT security and compliance risk reduction and improves operational efficiency by enabling privileged access defence.

SecureKi Advanced Credential Management (ACM) is the next generation automated privileged password management solution with visual recording, fine-grained access control, multi-factor authentication, and Infrastructure Single-Sign-On capabilities

> SecureKi solutions are designed and developed with futuristic and innovative security technologies designed to **help organizations** to **secure** and **manage** their **enterprise passwords** in an effective and automated way

Solutions

Privileged Password Management
Enforcing and maintaining password policy

Advanced Credential Management
Provides identity infrastructure Single-Sign On with OTP verification without exposing credential

Smart Analytic
Provides a Session Monitoring feature that covers both CLI and GUI modes.

2016
APICTA Awards Malaysia:
Best of Security

2017
Common Criteria EAL2 Certification

03 CYBER100 PRODUCT& SERVICES

DNS & END POINT PROTECTION

Solutions that automate data management, protection, optimization, movement, and governance

- Data classification and data loss prevention suites (software and hardware) can detect sensitive data in motion (transiting a network), in use (being viewed or accessed via an end-user device), and at rest (e.g., files and data stored on endpoints, servers, and removable media).
- DLP suites may also include native functionality or APIs that provide encryption, file blocking, or other techniques to prevent data from exiting an environment or unintended access.
- DNS-based malware protection – block the communication between infected client to the command center

CYSECA endpoint application control is an endpoint application whitelist solution. It allows uses of selected application based on certain criteria set as policy.
Designed to lockdown endpoint including I/O interface, prevent execution of unauthorized application, unknown application, malware, ransomware, zero-day malware, non-malware attacks and various scripting such as VBScript and PowerShell.
Designed with granular policy, extensive application catalogue as well as, real-time monitoring and defences, CYSECA reduces the risk of threat exposures on client.

Challenges VS Product

1. **Anti malware technology** had relied on signature-based detection and has become ineffective.
2. **The next generation Endpoint Protection** includes Behavioral Detection, Artificial Intelligence (AI) and Machine Learning (ML), **require heavy processing**.
3. **Downside** – Anti malware false positive when doing basic function (i.e. win updates) and signature-based fails when it comes to malware mutate, polymorphic code.
4. **Critical system increasingly targeted**, resulting in data leakage, locked folders with ransom note, loss of valuable data, compromised endpoints used as launching pad.

CYSECA Endpoint Application Control

1. **Zero False Detection:**
   - Ability to detect all attempts of unauthorized application installation.
2. **Lightweight on Endpoint:**
   - Extremely light agent and designed for efficiency
3. **Low Maintenance:**
   - On whitelist updates.
4. **Lock down Systems:**
   - To stop malware, Ransomware, zero-day, cryptomining, advanced complex files like DLL, JAR, VBScript and PowerShell.
5. **Administration Agility:**
   - Allow policy user grouping, on-demand whitelist update and multi-tenancy

Solutions

"Endpoint Application Control"

IDENTIFY [Audit Mode]
Identify and discover all software and applications installed in the client's machine

DETECT [Protection Mode]
Detect running application or attempt to execute application

RESPOND
Qurarantine unknown, unwanted, unapproved applications including malware.

PROTECT
Block and lockdown Endpoint from executing any unknown, unwanted, unapproved applications including malware. Set AWL policy.

2020
Malaysian Common Criteria Evaluation & Certification (MyCC EAL 2)

www.cyseca.com.my marketing@cyseca.com.my

e-Lock Corporation Sdn. Bhd. is a premier IT security company that provides enterprises with solutions against identity thefts, advanced cyber-attacks and threats to corporate data integrity for more than 25 years.
Their multi-layered protection products and services cover all key aspects within an organization's security lifecycle from monitoring to protection which keeps your data safe from threats, including ransomware. Their award-winning solutions are designed to ensure that all organizations are well protected.

Challenges VS Solutions

The threat from ransomware has become one of the top concerns to businesses and organizations.

Large organizations including government agencies and critical infrastructure services with have also fallen victim to these attacks

ARWare puts up a blanket protection on over a hundred popular file types instantly, locking down your endpoints by allowing only registered business software to write/modify protected file types. Everything else is denied, including ransomware, and other unknown malware

Solutions

"Policy-based Against Zero-Day Attacks"

Protect
Protection against modern malware

Whitelist
List of all known, good programs

Block
Block programs not on the whitelist from entering your system and making changes to protected files

2017
Recipient of SME100 Malaysia Fast Moving Company

2022
Listed in Good Firms; Top IT Services Firm

DNSVAULT is a comprehensive internet control and filtering solution based on DNS technology. It is hosted and managed by DNSVault in a secure cloud environment and provides complete protection from online threats such as malware, ransomware, and phishing. Our content filtering solution is very effective, and the best part is that it requires zero maintenance and can be set up in just a minute.

Challenges VS Solutions

Cyberattacks against big companies are well-publicised by the news media, while attacks against small firms generate little attention. This can give small businesses a false sense of security. Yet, small firms are generally more vulnerable than large ones because they have fewer resources to devote to security.

DNSVault ITP (Intelligence Threat Protection)

1. Restrict access to adult content and other categories including Malicious, Gambling, Fake News, Adult etc.
2. Gain control and visibility to what's happening on your network
3. Provide clean and safe internet browsing experiences
4. Effective and easy to deploy from small up to enterprise level

Solutions

> We believe that everyone should have the right to live in a safe and protected online society without the fear of potential intrusion by cyber criminals.

• Detect
Real time and historical analysis of global DNS data to detect security threats

• Feed
Policy enabled recursive DNS servers are updated with real-time threat feed

• Enforce
Servers examine DNS transactions and block domain and IP security threats and filtered sites and categories

Mitigate •
Locate and quarantine infected devices

• Report
Malicious activity is identified and reported

2017
Cyber Security Innovation Gold Medalist - ITEX 2017

2017
Cyber Security Company Of The Year - Cybersecurity Malaysia

2018
EAL2 - Common Criteria Certificate

2019
Cyber Security Innovation Of The Year - Cybersecurity Malaysia

2019
Excellence in IT Security - International Islamic Leadership Award

2019
Excellence In Cyber Security - Malaysia Excellence Business Awards

2020
Top 3 Winner CYBER100 – MDEC-NACSA

www.dnsvault.net hello@dnsvault.net

03 CYBER100 PRODUCT& SERVICES

TOOLS DOCUMENT SIGNING / OTP

Solutions that allow the agile sharing of sensitive data; Tools that prevent online and offline scam

- Data security (in storage, in-transit, and in-use) is critical.
- A digital signature is a mathematical scheme for verifying the authenticity of digital messages or documents. A valid digital signature, where the prerequisites are satisfied, gives a recipient very high confidence that the message was created by a known sender (authenticity), and that the message was not altered in transit (integrity).
- A one-time password (OTP), also known as a one-time PIN, one-time authorization code (OTAC) or dynamic password, is a password that is valid for only one login session or transaction, on a computer system or other digital device.

SigningCloud strives to be a universal e-signing platform that supports multiple eKYC (electronic Know Your Customer) and Certificate Authority (CA) providers, giving signers the option to choose their providers free from vendor lock-in.
In the near and far future, SigningCloud will continue to enhance the platform by adding more trusted eKYC and CA providers (both local and global) to the list, enabling it to become a cross-border, universal e-signing platform.

Challenges VS Product

1. **Businesses:** face high costs of business digitalization in daily workflow processes, and system integrations to existing legacy systems, especially the PKI knowledge required to integrate to the License Certificate Authority (CA) in Malaysia.
2. **Customers:** Concerns arise when it comes to confidentiality, document integrity, security and data privacy when choosing the right Electronic Signature or Digital Signature.
3. **Regulators:** The existing regulatory and legal framework of Digital Signature Act 1997 and Electronic Commerce Act 2006, etc.

1. **Integrity**: Tamper-proof features ensure the integrity of the documents. It guarantees the integrity of the content, signature, and identity of the signed document.
2. **Authenticity:** Secure validation of the machine and identity's users; identity authentication is conducted through eKYC which are accepted by a local and trusted CAs, step-up authentication is used to prove the act of willful signing.
3. **Non-repudiation:** Ensures that communication, data exchanges and transactions are legal and irrevocable. Private key is protected by PKI technology and no one else is able to duplicate or generate the signature.

Solutions

> SigningCloud provides both Electronic Signature and Digital Signature

- **Universal Signing Platform**
- **PKI Technology**
- **Time Stamping Authority (TSA)**
- **Plug-ins Ready**
- **MFA Authentication Security Log in**
- **Mobile & Web Present**
- **Full Security Audit Trail**
- **Tamper proof to CAdES and PAdES Standard**

2022
ISO 27001

SECUREKI

SecureKi specialises in securing and managing credentials which helps many customers to stop targeted attacks, mitigate insider threats, achieve compliance, improve operations and secure the hybrid enterprise.

SecureKi solutions are designed and developed with futuristic and innovative security technologies designed to help organizations to secure and manage their enterprise passwords in an effective and automated way.

Challenges VS Product

1. Users may find MFA to be inconvenient or difficult to use, which can lead to low adoption rates and increased security risks.
2. Implementing MFA can be complex, especially for organizations with many users and a wide variety of authentication methods.
3. Implementing MFA can be expensive.

1. SecureKi MFA solution is **easy** to use with **great flexibility**, allowing organizations to use a variety of authentication methods such as OTP, biometrics, and Web SSO.
2. SecureKi MFA solution integrate with existing systems, such as Active Directory and SSO solutions, to **provide a seamless user experience** with the ability to scale to meet the needs of organizations with large number of users.
3. SecureKi MFA solution is **cost-effective**, with pricing that is affordable for organizations of all sizes.

> SecureKi solutions are designed and developed with futuristic and innovative security technologies designed to help organizations to secure and manage their enterprise passwords in an effective and automated way"

Solutions

Zero-Trust Privileged Access Management

SecureKi MFA

Endpoint Privileged Management

Identity Security Workforce

2016
Best of Security Award Winner APICTA Malaysia

2019-2022
Technologies Security Assurance

2022
FIDO® Certification

2017
Common Criteria EAL2 Certification

www.secureki.com info@secureki.com

CYBER100 PRODUCT& SERVICES

CLOUD SECURITY

VIGILANT ASIA

YOUR CYBERSAFETY IS OUR PRIORITY

Vigilant Asia is an award-winning Managed Security Service Provider (MSSP) operating regionally since 2017.
Following industry best standards and practices, they are ISO 27001:2013 certified as well as CREST accredited for Penetration Testing and their Security Operations Centre (SOC). With a team of over 50+ certified cybersecurity professionals, their clientele consists of some of Asia's leading organizations hailing from industries such as FSIs, Manufacturing, Education, MNCs, GLCs & Govts.

Challenges VS Services

1. **Shortage Of Security Staff:** Security analysts are a scarce and expensive resource that is difficult to hire and train.
2. **Protection Against Advanced Attacks:** Advanced attacks are difficult to protect against because they use tactics, techniques and procedures (TTPs) that can bypass baseline security measures..
3. **Slow Detection, Investigation And Response:** IT teams don't have time to validate and assess every alert and set priorities for further investigation. The Mean Time to Respond (MTTR) for most organizations is measured in months, while attackers compromise and exfiltrate data in days.
4. **Too Many Tools:** Organizations need to manage multiple consoles across different technologies to maintain a robust cybersecurity posture.

1. **Assess Current & Continuous Security State:** Compromised Assessment, Cybersecurity Audits, Breach and Attack Simulation, Intelligence-Led Pen Testing, Red Teaming.
2. **Derive The Cyber Security Strategy:** Roadmap to elevate from current state to targeted Cyber Resilient state.
3. **MSSP Services & Solutions:** Managed Detection and Response, Security Monitoring, Incident Analysis, Threat Hunting, Incident Response.

Solutions

"Managed Security Service Provider (MSSP)"

- Managed SIEM
- End Point Protection Solutions
- Vulnerability Management
- Mobile Application Security
- Security Intelligence
- Deception
- Brand protection
- IOT / OT
- Automated Awareness and Phishing Simulation

2019
ISO 27001:2013 Certified, CSM - Cybersecurity Company of the Year

2020
CREST Accredited for Penetration Testing

2021
CREST Accredited for SOC and CSM - Cybersecurity Innovation of the Year

2022
SOC Team of the Year Asia and CSM - Cybersecurity Professional of the Year

2023
Cybersecurity Service Provider of the Year Asia

nexagate

Cyber 100. Cohort 3

Nexagate is one of Malaysia's leading cybersecurity service providers. For 12 years, we have delivered trusted security solutions to more than 400 organisations across critical verticals within the ASEAN region. Nexagate offers a complete range of cybersecurity services that has been certified with ISMS ISO 27001 (since 2012). This includes Risk Compliance, Offensive Security, and Managed Security Services which are delivered with seamless digital experience via our patent-pending and award-winning NSI Unified Security Management Platform.

Cloud
Risk & Compliance

Cloud
Offensive Security

Cloud
Managed Security

Challenges VS Product

1. Complexity of Cloud Provider Native Security offerings
2. Vulnerability of system due to Cloud Misconfigurations
3. Not understanding Share Responsibility Model
4. Increasing Compliance Requirements (GDPR, PCI-DSS, SOC2, ISMS 27017 and 27018)
5. Lack of in-house Expertise

Nexagate Cloud Security Services comprises Complete, Modular, and On-Demand Services via a Platform which aims to prevent data breach & leakages due to cloud misconfigurations and protect against unwanted cyber attacks.

Solutions

"Cloud Cybersecurity Services Ensuring Best Cloud Practices, Cloud Security Posture and Protection"

- **Compliance as a Service (COaaS) - ISO 27017 & 18, Gap Analysis**
- **SOC as a Service (SOCaaS) - Threat Intel, SIEM**
- **Web Security as a Service (WSaaS)**
- **Managed Detection and Response as a Service (MDRaaS)**
- **Compromise Assessment as a Service (CAaaS)**
- **Penetration Testing as a Service (PTaaS)**
- **Brand Monitoring as a Service (BMaaS)**
- **Incident Response as a Service (IRaaS)**
- **Cyber Awareness as a Service**

20?
ISMS ISO/IEC 27001:2013

20?
ISMS ISO 27017 & 27018

20?
CREST Certification (200th Member)

www.nexagate.com sales@nexagate.com

Securemetric offers a centralized login option that protect all applications from security breaches by using FIDO2 passwordless authentication. With its single sign-on feature, users can conveniently authenticate once and gain access to multiple applications without the hassle of managing separate login credentials. This simplifies the user experience and enhances security by providing a centralized authentication system. Centagate Cloud aims to streamline application access management and ensure a secure and seamless login process for users

Centralized Identification

Authentication-As-A-Service

Passwordless Authentication

Challenges VS Solutions

1. **Concerns on identity theft**, data security, login password security and system integrity
2. **BYOD,** Remote working policies and accessing office environment using personal device
3. **Inefficient User Management,** managing user accounts across multiple applications becomes complex and time-consuming
4. **Security Risks and Inconsistent Controls,** consistent access control policies and maintaining a robust security posture across applications becomes challenging, increasing the risk of unauthorized access and data breaches.
5. **Compliance Challenges:** Organizations may face difficulties in regulatory compliance requirements.

1. **SECURE:** A system that has strong digital security which eliminates phishing, fraud and password theft.
2. **ALL-IN-ONE:** Since the authentication is centralized, only one login credential is needed for all applications.
3. **COST EFFECTIVE:** Highly cost-effective with zero CAPEX and minimal OPEX.

Solutions

CENTAGATE CLOUD - Centralized Identification - Authentication-As-A-Service Passwordless Authentication

Security
Eliminate phishing, fraud and password theft.

Efficiency
Control, protect and secure all your applications through one login credential.

Compliance
Comply to PDPA and GDPR through MFA.

2017
Common Criteria EAL4+ Certification

2019
FIDO2® Certification

SECUREKI

SecureKi specialises in securing and managing credentials which helps many customers to stop targeted attacks, mitigate insider threats, achieve compliance, improve operations and secure the hybrid enterprise.

SecureKi solutions are designed and developed with futuristic and innovative security technologies designed to help organizations to secure and manage their enterprise passwords in an effective and automated way.

Challenges VS Product

One of the primary challenges is achieving seamless management across multiple cloud platforms and on-premises infrastructure simultaneously. Ensuring that the PAM solution can effectively handle diverse cloud environments and maintain consistent access controls, authentication, and auditing across different platforms requires careful consideration.

SecureKi Privileged Access Management SaaS is tailor for cloud environment. Enhance with secret management and cloud-to-cloud management, SecureKi PAM SaaS provide the best-in-class PAM solution for cloud environment. Equip with feature to support multi-cloud management and platform. A single SecureKi PAM SaaS could help to manage any cloud platform and on-premises infrastructure simultaneously with ease.

> SecureKi PAM SaaS: Tailored cloud PAM with secret management and cloud-to-cloud capabilities.

Solutions

Zero-Trust Privileged Access Management

SecureKi MFA

Endpoint Privileged Management

Identity Security Workforce

2016
Best of Security Award Winner APICTA Malaysia

2019-2022
Technologies Security Assurance

2022
FIDO® Certification

2017
Common Criteria EAL2 Certification

e-Lock Corporation Sdn. Bhd. is a premier IT security company that provides enterprises with solutions against identity thefts, advanced cyber-attacks and threats to corporate data integrity for more than 25 years.
Their multi-layered protection products and services cover all key aspects within an organization's security lifecycle from monitoring to protection which keeps your data safe from threats, including ransomware. Their award-winning solutions are designed to ensure that all organizations are well protected.

Challenges VS Product

- Conventional protections provided by firewalls, network intrusion detection systems and anti-malware solutions are no longer adequate to uphold the integrity of the inner sanctum of enterprise information systems against modern sophisticated attacks.
- Continuous unknown external and internal threats need to be detected, identified, analysed and responded to in a proactive manner at the earliest possible time.

- Last-line of defense at data level.
- **DETECT** system breaches by monitoring files, registry keys and decoy files.
- **IDENTIFY** known and unknown zero-day threats.
- **ANALYSE / HUNT** threat with correlation data (file, user, process, IP address, time)
- **VISUALISE and MANAGE** via cloud-based management console
- **RESPOND** with automatic data recovery, process termination and host isolation.

Solutions

> **"DeepDetect:** Enterprise System Integrity Protection, Breach Detection, Analysis, Visualisation & Response Solution"

File/Registry Monitoring

Breach Alerts

Analytics

Correlation

Cloud-based Management

Data Recovery

Process Termination

Host Isolation

2019
ISO 27001:2013 Certified, CSM - Cybersecurity Company of the Year

2020
CREST Accredited for Penetration Testing

2021
CREST Accredited for SOC and CSM - Cybersecurity Innovation of the Year

2022
SOC Team of the Year Asia and CSM - Cybersecurity Professional of the Year

2023
Cybersecurity Service Provider of the Year Asia

www.elock.com.my sales@elock.com.my

NETBYTESEC
SECURING YOUR DIGITAL ASSETS

Cyber 100. Cohort 3

NetByteSEC established since 2013 is a robust and passionate information technology and security-consulting firm who provides end-to-end consulting services from strategy to execution.
Our professionals provide industry-leading expertise to help organizations meet their evolving information security needs. We empower organizations to foster their cyber security culture and thinking to further drive for secured environment. By focusing on the actual outcome of our services on the cyber security solutions, we help businesses securing their environment by breaking into it, building the detection, developing secure codes and culturing the cyber security mindset

Challenges VS Product

- Cyber incidents always happen when you're least expect them, most organization is not well prepared to get the right information to the right individuals at the right time when cyber incident happened – Getting the organization to be prepared is the problem we want to solve
- Lacking of practical contents during the capacity building on cyber security is real problem to build the cyber security preparation and talents – Getting fully technical and practical contents for the capacity building is the problem we want to solve

- provide a realistic scenario within a controlled environment to allow organization to identify their strength and weaknesses
- provide opportunities for organization to validate the effectiveness of their policy and procedures in handling cyber incidents
- is the best platform for personnel to practice their respective roles, including improving their technical capabilities in a secured environment where mistakes can be made and learnt from
- Cyber training and exercise can be organized virtually since CAPTUREX is a web application platform, this is beneficial especially for decentralize large organizations scales

> CAPTUREX is a Centralize Platform for Cyber Drill Exercise and Security Training that include all comprehensive modules for cyber training.

Solutions

Cyber Drill Exercise

A planned event during which an organization simulates cyberattacks, information security incidents and other types of disruption that require players respond to the scenario

Capture The Flag

Computer security-based competition or training platform with integration with XLAB that test and train participant's skills and knowledge in the industry.

Table Top Exercise

An activity in which key personnel were assigned emergency management roles and responsibilities are gathered to discuss for various simulated emergency situations.

DNSVAULT

DNSVAULT is a comprehensive internet control and filtering solution based on DNS (Domain Name System) technology. It is hosted and managed by DNSVault in a secure cloud environment and provides complete protection from online threats such as malware, ransomware, and phishing. Our solution is very effective, and requires zero maintenance and can be set up in just a minute.

Challenges VS Solutions

Cyberattacks against big companies are well publicized by the news media, while attacks against small firms generate little attention. This can give small businesses a false sense of security. Yet, small firms are generally more vulnerable than large ones because they have fewer resources to devote to security

Cloud-Based Secure DNS

- On-Cloud High-Performance Secure DNS Platform
- Filtering Out Internet Malicious Content
- Block phishing, malware, botnets and other high-risk categories
- Provide clean internet browsing experiences
- Prevent web and non-web call-backs from compromised systems
- Low-maintenance and Easy to deploy from small business to enterprise level

Solutions

> We believe that everyone should have the right to live in a safe and protected online society without the fear of potential intrusion by cyber criminals.

Detect
Real time and historical analysis of global DNS data to detect security threats

Feed
Policy enabled recursive DNS servers are updated with real-time threat feed

Enforce
Servers examine DNS transactions and block domain and IP security threats and filtered sites and categories

Mitigate
Locate and quarantine infected devices

Report
Malicious activity is identified and reported

2017
Cyber Security Innovation Gold Medalist - ITEX 2017

2017
Cyber Security Company Of The Year - Cybersecurity Malaysia

2018
EAL2 - Common Criteria Certificate

2019
Cyber Security Innovation Of The Year - Cybersecurity Malaysia

2019
Excellence in IT Security - International Islamic Leadership Award

2019
Excellence In Cyber Security - Malaysia Excellence Business Awards

2020
Top 3 Winner Cyber100 - MDEC-NACSA

www.dnsvault.net hello@dnsvault.net

EC-Council Cyber Defense

EC-Council Cyber Defense (ECCD) is a division of EC-Council (the world's largest cybersecurity technical certification bodies and a Malaysian company success story). ECCD is also one of the leading Managed Security Services (MSS) providers in Malaysia. Together with our parent company, we provide end-to-end services ranging from advisory and consulting (including cybersecurity governance, risk, and compliance, RMiT based compliance, and technical assessment) to training and certification (including world-renowned Certified Ethical Hacker - CEH). We are also ISO 27001 and CREST certified in Security Operations Center (SOC), Cybersecurity Incident Response (CSIR), Penetration Testing, Vulnerability Assessment, and Application Security Testing Services (OVS Web and OVS Mobile).

Challenges VS Product

- Expertise - Lack of knowledgeable and experienced personnel
- Adoption - Non-comprehensive cloud adoption and migration strategies
- Managing - Hybrid and multi-tenancy cloud environments
- Security - Configuration of multiple interfaces and API integrations
- Visibility - Centralized monitoring and management
- Confidentiality - Data privacy and leakages
- Legal - Regulatory compliance

ECCD solutions provide services to manage cloud requirements:

1. **SOC and MSS,** Centralized / Hybrid SOC model (24x7 monitoring, triage, escalation), Brand Intelligence, Forensics Investigation, Incident Response, Staff Augmentation, and Threat Intelligence and Hunting through cybersecurity experts.
2. **Risk, Governance and Compliance,** Cloud Security Assessment, Cybersecurity Posture and Maturity Assessment (CSMA), RMiT Compliance Advisory, Third-Party Security Assessment.
3. **Technical Assessment and Solution Integration,** Vulnerability Assessment & Penetration Testing (VAPT), ScopeX, Red Teaming, Cyber Drill, Compromise Assessment.
4. **Awareness, Training and Certification,** Cybersecurity Technician, Cloud Security Specialist, Ethical Hacker, Certified CISO.

> Managed Cybersecurity Service Provider with End To End Capability in Cloud Assessing, Managing, Auditing, Operating, Certification, And Training

Solutions

Security Operations Center (SOC) and Managed Security Services (MSS)

2019
CREST accredited in Security Operation Center, Cybersecurity Incident Response, Penetration Testing, Vulnerability Assessment and OWASP Verification Standard in Apps and Mobile

Risk, Governance and Compliance

2022
Key Contributor to MITRE D3FEND Framework by National Security Agency, USA

Technical Assessment and Solution Integration

2022
Approved Vendor for Managed Cybersecurity Services and Penetration Testing by Cybersecurity Agency, Singapore

Awareness, Training and Certification

2023
Best Cybersecurity Training and Certification

egs.eccouncil.org egs.sales@eccouncil.org

Cydentiq is a leading identity security company specialized in helping organizations address the ever-evolving identity landscape by building an identity fabric that is governed by our identity security framework to protect business against digital risk – ensure the right people have the right access to the right data at the right time and doing the right thing for the right reason.

Challenges VS Services

Challenges

1. Most of the identity & access management (IAM) programs are using "one-time deploy and finish" approach, siloed, inefficient and difficult to scale operationally
2. Unreadiness of IAM technology adoption – business process & data gap, legacy apps that are not friendly for integration and poor project planning
3. Lack of visibility – who has access to what system & data
4. Sustainability of identity hygiene is beyond human capacity – manual identity management is labour intensive, error-prone and leads to repetitive identity-related audit gaps – standing privileged access, excessive access, orphaned accounts, unauthorized access.
5. Poor contractor/vendor access management puts organizations at high vulnerability risks of data breach

Services

1. Cydentiq Identity Maturity Assessment provides a quick assessment of organization's maturity level of their current identity hygiene against best practices, identify the gaps and provide practical recommendation to reach desired maturity level
2. Cydentiq Rapid IAM Roadmap Assessment provides organizations a rapid and insightful maturity level of their current IAM landscape against our identity maturity framework, mapping of application integration feasibility with market leading IAM capabilities, build actionable and practical IAM roadmap to jumpstart their identity initiatives.
3. Deployment of IAM enabling technologies to provide centralized view of who has access to what, automated identity lifecycle management with robust governance capabilities to manage employee, contractor & vendor access

Solutions

> Cydentiq's proven Identity Maturity Assessment Framework, vendor-agnostic advisory coupled with our deep experience of IAM & PAM domain, we are confident to help you building successful IAM journey ahead

- Privileged Access Management
- Single Sign-on & MFA
- Data Access Governance
- Insider Threat Management
- Identity Maturity Assessment
- Rapid IAM Roadmap Assessment
- Identity Governance & Administration

2023
Most Advanced Identity Security Solutions Company - South East Asia

2021
Best Identity Security Company - South East Asia

https://www.cydentiq.com info@cydentiq.com

Biocryptodisk

Advance Product Design Sdn. Bhd.

Biocryptodisk specialises in on board military grade hardware cryptograpfy which supported on board and on the fly file encryption, PKI, and random number generator. Biocryptodisk products are 100% designed and manufactured in Malaysia.

The Common Criteria validated products from Biocryptodisk ensure protection coverage of Data at rest, Data in transit, Data in use and Cryptomodule that supported AES-256, ECC-256, ECC384, etc. The supported protection type of our products are Confidentiality, Integrity, Authentication and Non-repudiation.

Challenges VS Product

- Data Leak Prevention had become a big challenge due to advanced of 5G and cloud technology. Your data are instantly copied onto multiple servers in independent data centers or even around the world
- Social Media Application had made a big challenge to both your Corporate and personal privacy especially on surveillance and scammer with the help of Artificial Intelligent..
- Surveillance, Ransomware and spyware had been a challenge to critical national and corporate information infratructure

- Biocryptodisk hardware encryptor which is Common Criteria validated was announced as Produk Kriptografi Terpercaya by Jabatan Perdana Menteri after Skim Penilaian dan Pensijilan Produk Kriptografi Terpercaya (SPPPKT). It was further announced by Surat Pekeliling Am Bilangan 2 Tahun 2021 Section 12.1.5 that "Pengunaan Produk Kriptografi Terpercaya adalah mandatori di dalam urusan yang melibatkan maklumat rahsia rasmi selaras dengan Dasar Kriptografi Negara.
- Biocryptodisk USB Data Diode is Common Criteria EAL2 validated. It protects data in use in your server and in Local Area Network against surveillance, ransomware and spyware

> Biocryptodisk Solutions ensure customer has the ownership and management of their encryption keys.

Solutions

- **Big Data Encryption/ Decryption for Cloud Storage**
- **Data Leak Prevention**
- **Multi-Factor Authentication**
- **Public Key Infrastructure**
- **Volume Encryption**

2015
Biocryptodisk Encryptor is CC EAL2+ validated

2020
Biocryptodisk Data Diode is CC EAL2 validated

http://www.biocryptodisk.com marketing@biocryptodisk.com

Infinity Consulting Technology Sdn. Bhd.

Aegis Cloud is a veteran and trendsetter in the Cloud Backup and Disaster Recovery industry in Malaysia. With over 15 years of dedicated experience, Aegis Cloud offers a complete range of Cloud backup and Disaster Recovery services that has been certified with ISO 27001 ISMS since 2019. With Aegis Cloud's Managed Services and 24x7 support, you can have peace of mind, knowing that your business is well prepared to handle any adverse situation.

Challenges VS Services

1. Concern on investing the wrong backup software for the company
2. Hefty investment to build and own a disaster recovery site
3. Insufficient skill to manage multiple backup software in heterogenous environment
4. Hesitation to perform DR Drill due to failure of data restoration
5. Unable to fulfill data security compliance standard

1. **Aegis 1PAT:** A cloud backup service that license customers to utilize any backup technologies at a fixed price
2. **Aegis DR-AS-A-Service (Draas):** A DR service equipped with complimentary unlimited DR resources ready to be utilized by customers during DR declaration
3. **Aegis Managed Services:** A service that undertakes tasks such as operations, maintenance and support of customers' backup and DR operations. Aegis Cloud has more than 15 years of experience in managing and troubleshooting on backup and DR matters, comprises of more than 30 local talents
4. DR Drills assisted by **dedicated Aegis DR Drill professionals** to guarantee successful DR Drills
5. Aegis Cloud's offering **Malaysia Digital Status Company**

> Aegis Cloud's aims to spearhead the Cloud DR trends with simplified, guaranteed workability and cost-effective Cloud DR deliveries. Aegis Cloud's Disaster Recovery Portal, the first in Malaysia, to consolidate all backup software, storages and DR resources onto a centralise control centre.

Solutions

Aegis 1Price-Any-Technlogies

Aegis DR-AS-A-Service

Fully Managed Service

Since 2012
Disaster Recovery Certified Expert (DRCE)

Since 2019
Information Security Management (ISO) 27001 ISMS

FIRMUS

Established in 2008 by Cyber Security veterans, FIRMUS is the Industry Leader in Cyber Security services and solutions They are ISO 27001 and CREST Accredited for the provision of Cyber Security services and a Malaysia Digital (MD) Status company

Challenges VS Services

Challenges

1. **Staffing/Resources**
   - Organizations that were already struggling to keep their security teams fully staffed are facing even greater challenges as they adopt innovative security technologies to address the evolving threat landscape

2. **Privileged Access Management**
   - Many IT organizations rely on manually intensive, error prone administrative processes to rotate and update privileged credentials

3. **Unpatched Vulnerabilities**
   - This risk is compounded by increasing IT complexity and cloud deployment if you don't know what you've got, how can you secure it?

Services

1. **Managed Detection Response (MDR)**
   - Combines technology and human expertise to perform threat hunting, monitoring, and response.
   - Rapidly identify and limit the impact of threats without the need for additional staffing.

2. **Managed PAM**
   - Designed to meet the specific reporting, governance, and compliance needs of organizations
   - Backed by a team of experts who provide ongoing support and guidance to ensure the security and compliance of privileged access.

3. **Managed Vulnerability Services**
   - Includes regular vulnerability assessments, validation and weekly, monthly or quarterly operational reporting which are conducted by a team of security professionals

"You Change The World, We Secure It."

Solutions

MANAGED SERVICES

Managed Detection and Response (MDR)

2012
Malaysia Cyber Security Awards

Managed Privileged Access Management (PAM)

2016
Malaysia Cyber Security Awards

Manages Vulnerability Services

2021
Malaysia Cyber Security Awards

www.firmusses.com presales@firmusses.com

Securelytics

Securelytics Sdn Bhd based in Selangor, Malaysia, is an independent cyber security advisory firm founded in 2014 We specialize in cyber security and ICT solutions With the growing threat landscape, we recognize the importance of strong cybersecurity measures for businesses to protect their operations

As a leading provider of cybersecurity services, Securelytics offers a range of cutting edge solutions tailored to our clients' needs Our services include Managed Security Services, Cybersecurity Lab Testing, Strategy, Risk Compliance, Cybersecurity Training, and ICT Software Hardware Integration

Challenges VS Services

Cloud computing offers numerous benefits, including scalability, flexibility, and cost effectiveness However, it also presents unique challenges when it comes to security.

1. Data Breaches Cloud environments are attractive targets for hackers, and a successful breach can result in the theft or unauthorized access to sensitive data.
2. Insider Threats Insider threats refer to risks posed by individuals within an organization who have authorized access to cloud resources.
3. Insecure APIs Unsecure APIs can be exploited by attackers to gain unauthorized access to cloud resources.
4. Compliance and Legal Issues Ensuring cloud security and compliance with industry regulations can be complex if the cloud service provider's practices don't align with necessary standards.

Securelytics offers the following cloud security services:

1. Cloud Security Assessment Architecture Design.
2. Identity and Access Management (IAM)
3. Data Protection and Encryption
4. Cloud Security Monitoring and Incicdent Response
5. Cloud Compliance and Governance

Solutions

Advancing The Evolution, A comprehensive end-to-end cyber security solutions provider that move you forward, faster.

Managed Security Services
For today's hybrid multi cloud world

Cybersecurity Lab and Testing
Staying ahead of cyber criminal

Strategy, Risk & Compliance
Meet requirements, comply with standards

Software & Hardware Integration
Extensive software and hardware integration services.

2017
Cyber Security Innovation Company of The Year

2018
25 Hottest Companies APAC CIO Outlook

2020
Partnership with TUV-SUD Singapore

2022
Cyber Security Company of The Year

www.securelytics.my info@securelytics.my

Provintell

Cyber 100 Cohort 3

Over 90% of the IT assets and services overseen by **PROVINTELL** are residing in various public and private clouds infrastructure. We have successfully helped many customers who are well-versed in cloud technology in the region in managing the cloud security operation challenges and regulatory compliance risks due to unmanaged attack surface and vulnerability, shadow IT, cloud service misconfiguration and data breach, to name a few. We employ the 'Threat Intelligence As First Line Of Defense' approach and methodology to help our customers to Identify, Detect and Response to various cloud security threats and vulnerabilities.

Challenges VS Services

Main cloud security risks and operation challenges.

1. **Unmanaged Attack Surface**
   - Unmanaged exposure risk.
   - Publicly exploitable vulnerability.
2. **Human Error and Misconfiguration**
   - System misconfiguration.
   - Shadow IT.
3. **Data Breach**
   - Insider threat
   - Malware infiltration
4. **Regulatory Compliance**
   - Multifaceted cloud logging and data repository infrastructure.
   - Minimal log retention period.
5. **Account Takeover (ATO)**
   - Weak identity and access management control.
   - Exposed services to password spraying attack due to leak user credentials.

'Threat Intelligence As First Line Of Defense' approach for cloud security and compliance management.

1. **Code Red ASM™ (External Attack Surface Management)**
   - External threat intelligence and attack surface management to identify, analyze and monitor your attack surface, data breach and exposure risk.
2. **Code Red IR (Incident Response)**
   - Compromise assessment and incident response with external and internal threat intelligence.
3. **PenTestBox® VM (Vulnerability Management)**
   - Assess and reduce your exposure risk with vulnerability management and security validation
4. **MXDR (Managed Extended Detection and Response)**
   - Next-gen CyberSOC for continuous external and internal threats hunting and intrusion monitoring with machine learning (ML/AI) data processor.Security orchestration, automation and response.'X' means anywhere and everything.

> **Cloud computing** is one of the biggest cybersecurity challenge, but one can start with attack surface management to continuously identify and reduce the exposure risk caused by human error, security misconfiguration, easily exploitable vulnerability and user credentials leak.

Solutions

CODEREDASM

Security Intelligence
Threat Intelligence and Attack Surface Management (ASM)

PenTestBOX

Exposure Reduction
Vulnerability Management (VM) and Security Validation

MXDR

Detection & Response
Managed Extended Detection and Response (MXDR)

2019
ISO/IEC 27001:2013 Certification

2020
AT&T Cybersecurity MSSP Partner

2022
Stellar Cyber Government MSSP Partner of The Year & Fastest Growing MSSP Award

2022
Arctic Security First MSSP Partner in Malaysia

2023
Arctic Security Strategic Partner

TecForte is an award winning company that specialises in Cybersecurity Information and Threats Management With over 15 years of dedicated focus, our solution has been leveraged to create better and stronger cyber defence and resilience among Governments and all critical Industries

Challenges VS Solutions

Challenges

1. Cybersecurity Management becoming more and more challenging!
2. Too many new devices and new cyber threats to manage and monitor.
3. Lack of resources and tools, many fail to process security events and attacks in real time
4. Most organizations within the Sector works independently in silo
5. Cannot achieve timely response on Sectoral threats

Solutions

1. Sector wide situational awareness for all organizations under the sector with threat intelligence sources, attack surface management, logs monitoring etc. improves ability to regulate and to increase the cyber security standards within the Sector via a single on cloud platform
2. A single on cloud platform allowing anonymous threat intelligence sharing and promotes collaboration to address cyber threats.
3. A single on cloud platform that encompasses all participating organizations within the Sector.
4. Sharing of threat intelligence on the single on cloud platform reduces MTTR, while improving the ability to regulate within the Sector

Solutions

> … our experience and domain expertise have been leveraged to create stronger cyber defense and resilience among Governments alongside key Industries in the region.

- **Sectoral Security** on cloud platform for 100s of Participating Organizations
- **Integrated** with Global Commercial and Open Source Threat Intelligence
- **Correlation** with network security logs
- **On-platform** Ability to communicate and collaborate between organization
- **Outside - in view** With External Attack Surface Management capabilities
- **Built in Incident** Management Capabilities

2013
Common Criteria EAL2 Certification

2015
Malaysia's Cybersecurity Company of the Year 2015

2018
Malaysia's Cybersecurity Product of the Year 2018

2019
Malaysia's Cybersecurity Professional of the Year 2019

www.tecforte.net sales@tecforte.com

SysArmy

Cyber 100. Cohort 3

We believe that effective cloud cybersecurity is the culmination of several elements to achieve maximum visibility in any environment. The three areas that have enabled us to best assist organizations are our strengths in Process, People and Technology.

Facts VS Services

1. **Highlights:**
   - CloudWatch covered 30 AWS services including CloudTrail and VPC Flow.
   - Recommended monitor CloudTrail and VPC Flow.
   - Multiple Azure logs type including activity logs, Azure AD.
2. **Advantage:**
   - CloudWatch enables you to monitor your complete stack (applications, infrastructure, network, and services) and use alarms, logs, and events data.
   - Azure provides identify gaps in your security policies and mechanisms
3. **Key Consideration:**
   - Cost on additional AWS Services and S3 Bucket
   - Logstash specification
   - On-prem storage
   - Log retention on Eventhub, S3 Bucket and On-prem storage

1. **Borderless:**
   Integration is possible regardless customer's locality, service providers or architectural design.
2. **Approachable:**
   We believe that cybersecurity should not be complex and difficult. We offer not only standard package but also customizable approach.
3. **Feasible:**
   Cybersecurity should not be a short-term achievement, but its framework should be a future proof risk strategy in line with business objectives

> "Rather than fearing cyber-attacks, build your resilience."

Solutions

- **Cybersecurity as a service**
  Cohesive approach to risk
- **Manage security services**
  Tailored to address specific risks
- **Managed security operation center**
  All-in and/ or tailored cybersecurity incident monitoring and management
- **Complete managed cybersecurity operation,**
  Tailored holistic management of both end of cybersecurity operation and governance.

2015
ISO27001:2013

2016
Cybersecurity Malaysia Innovation of the Year (NGSOC)

2018
CREST certification

2018
Award winning 2nd NGSOC Malaysia

www.sysarmy.net info@sysarmy.net

04 SUCCESS CASES

PROVINTELL TECHNOLOGIES SDN.BHD

SECUREMETRIC BERHAD

HEITECH PADU BERHAD

DNSVAULT

TECFORTE

NEXAGATE SDN. BHD.

SIGNINGCLOUD SDN.BHD

Our next generation cyber defense approach - "Threat Intelligence As First Line of Defense" with XDR Kill Chain and Machine Learning.

IDENTIFY

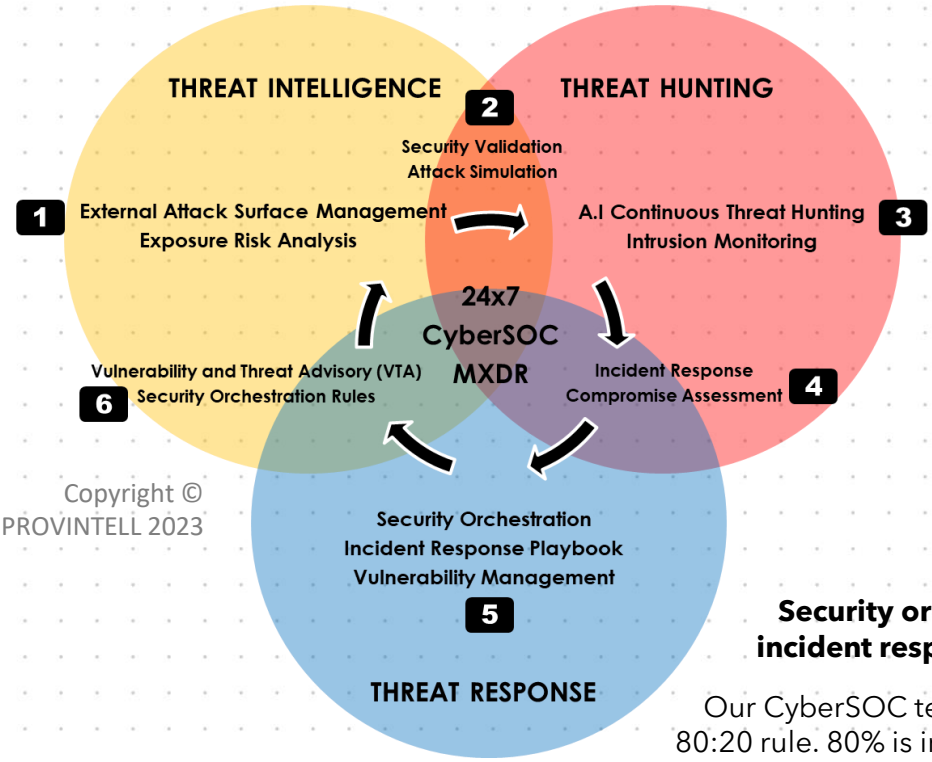
1 Identify your attack surface, data breach and exposure risk.

CODEREDASM

A product trademark (TM) of PROVINTELL

External attack surface management of any organization which involves data collection processes and continuous monitoring of external threats, vulnerabilities and anomalies of the publicly accessible application infrastructure and services, cloud storage and third-party services, public records and data breaches that would highly increase the exposure risk of any organization being the primary target of the cyber criminals.

Supporting organizations in exposure risk management and attack surface reduction to protect business reputation and operations with good cyber hygiene practices.



MXDR

Security orchestration and incident response playbook 5

Our CyberSOC teams operate based on 80:20 rule. 80% is in security orchestration and playbooks with the utilization of SOAR (Security Orchestration, Automation and Response) technology in responding to threats more efficiently with the minimum involvement of our customers, and the 20% is for the investigation and engagement with our customers for threat mitigation.

Provintell

Assess and reduce your exposure risk with vulnerability management and security validation 2

PenTestBOX

A registered product trademark (R) of PROVINTELL

It is a fact that a threat only materializes when there is a vulnerability. Therefore, vulnerability management is essential to help organizations in continuously assessing and managing the security vulnerabilities in the clouds, networks and systems to reduce the exposure risk to cyber threats.

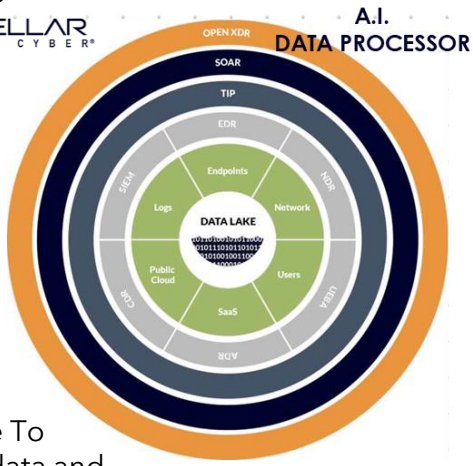
The security validation systems and techniques employed with operational threat intelligence of CODERED ASM would help organizations in managing their cyber security risks more efficiently.

DETECT

MXDR

3 **Continuous threat hunting and intrusion monitoring with XDR Kill Chain and machine learning**

STELLAR CYBER



How does an organization efficiently respond to cyber threats without breaking the bank? Open XDR is the key in collecting, processing and responding to the cyber threat data in the most complex environment that requires the Extended Detection and Response (XDR) components such as EDR, NDR, UEBA, SOAR and NG-SIEM, to name a few.

The XDR Kill Chain and Machine Learning technologies are the vital tools for our 24x7 CyberSOC teams in responding to threats more efficiently by reducing the MTTR (Mean Time To Respond) and minimizing human error that is highly due to data and alerts fatigue. Machine learning helps to reduce the effort and time required for incident triage and fidelity analysis.

RESPOND

CODERED IR

Compromise assessment and incident response with external and internal threat intelligence 4

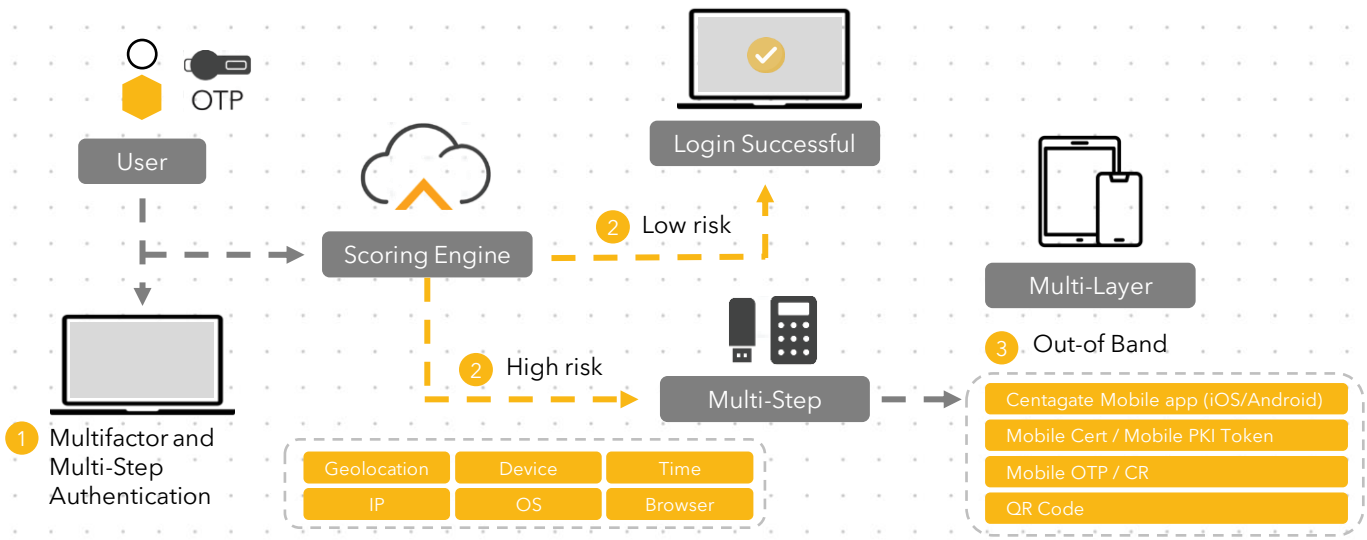
With proper utilization of the strategic, operational and tactical threat data attributes from the external and internal threat intelligence platforms, our CyberSOC is equipped with most of the essential data sources in assessing and responding to cyber threats for our customers, holistically from endpoints to clouds, and dark web.

CENTAGATE®
Next Gen Authentication Platform

CENTAGATE . Next Gen Authentication Platform

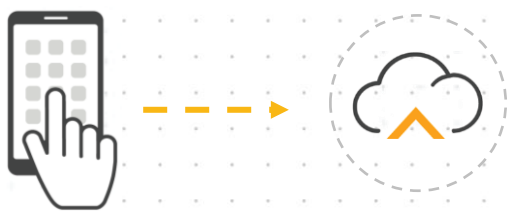
CENTAGATE® is a gateway that provides various kind of authentication services for corporate Web, client/server, and existing applications. CENTAGATE® is also a comprehensive authentication and fraud detection platform with its Adaptive Intelligence System.

Multi-Factors & Multi-Steps Authentication

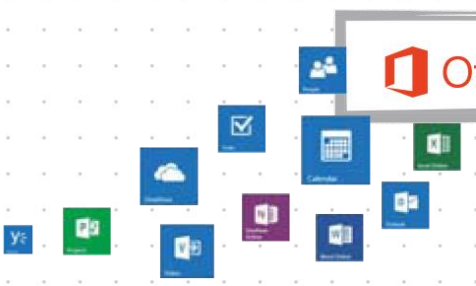


Multi-Channels Compatibility

BYOD
Android / iOS, Centagate Mobile App



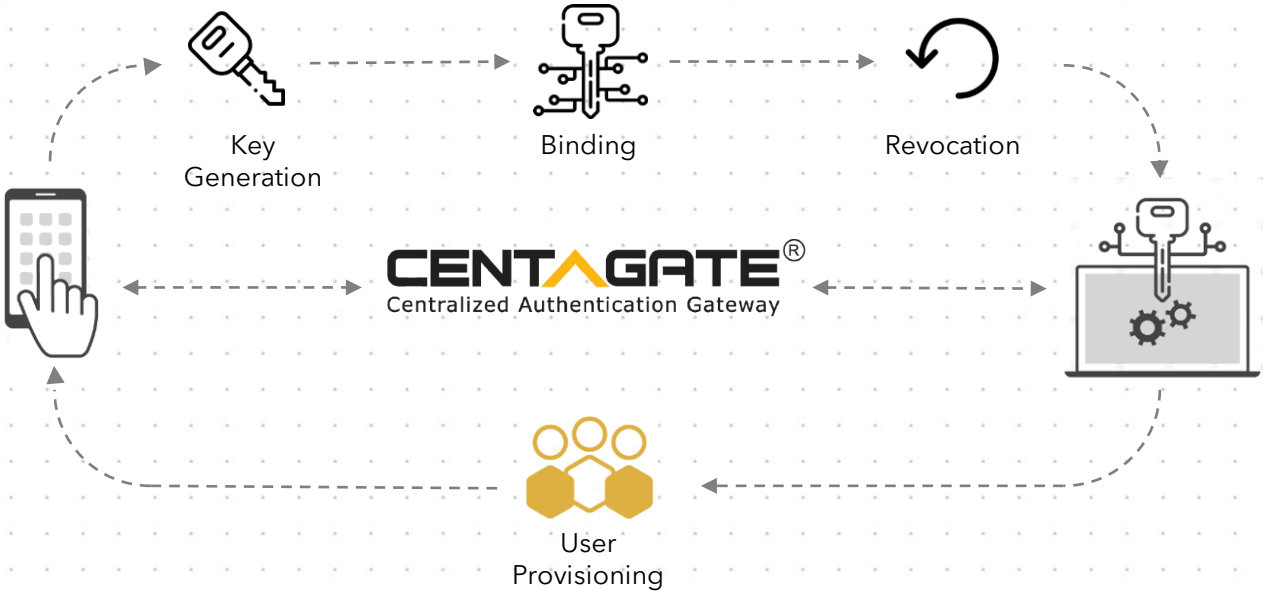
Centralized Mobility Management



Challenges

- Self service option for device management
- Tokenization and KMS to ensure SECURITY stability of BYOD
- Mobile software SDK for integration
- Centagate solution to organizations mobile apps

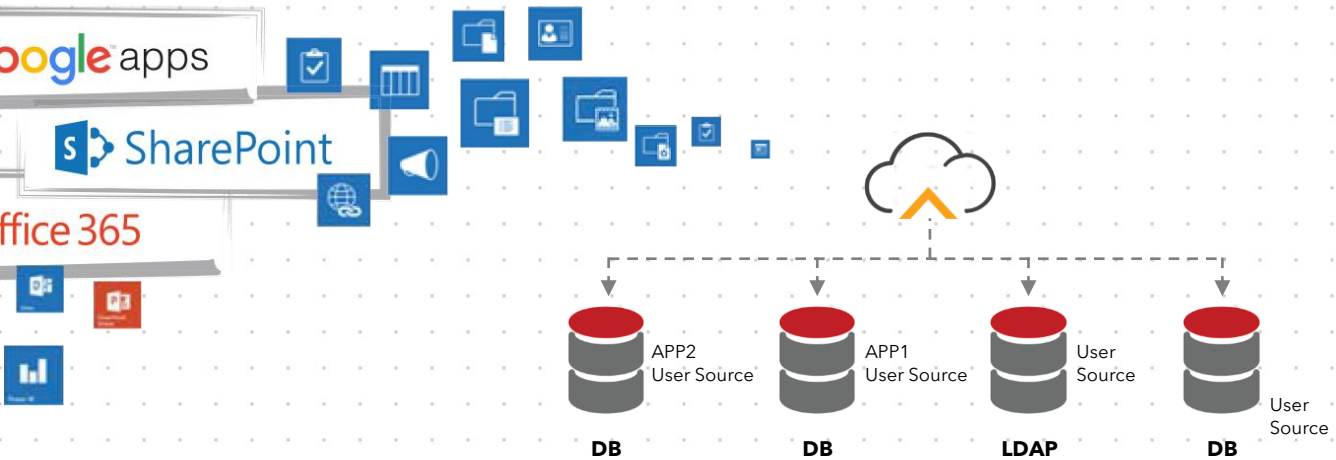
Multi-Layer Protection



Key Management System

Multi-Interfaces Platform

Integration Method



Centralized Identity Management

SECURE-X . PRESCRIBE.PRACTICE.CURE

Bridge your organization's cyber security skills gap with exclusive training courses, certifications and real-world exercises led by top experts in the field.

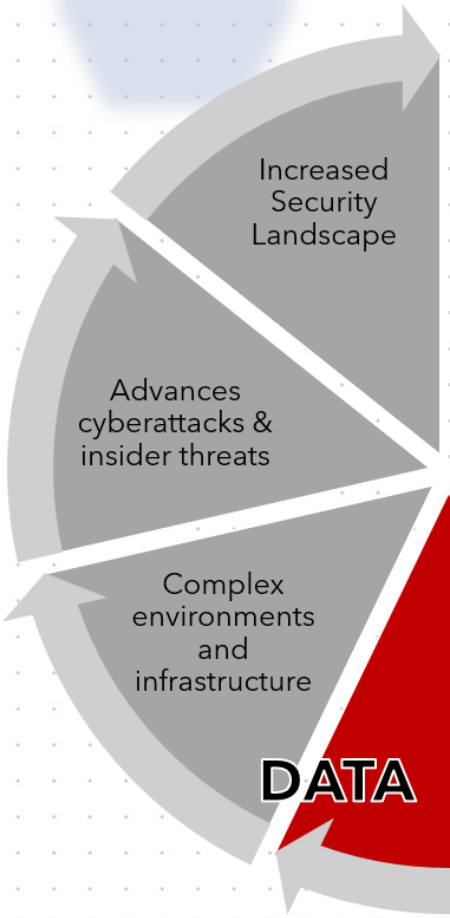
Client's Nature

- Handle Companies Registration
- Registration of Businesses
- Regulations on corporations, Companies & Businesses
- Promotes Good Corporate Governance & Business Conducts

Client's Goals

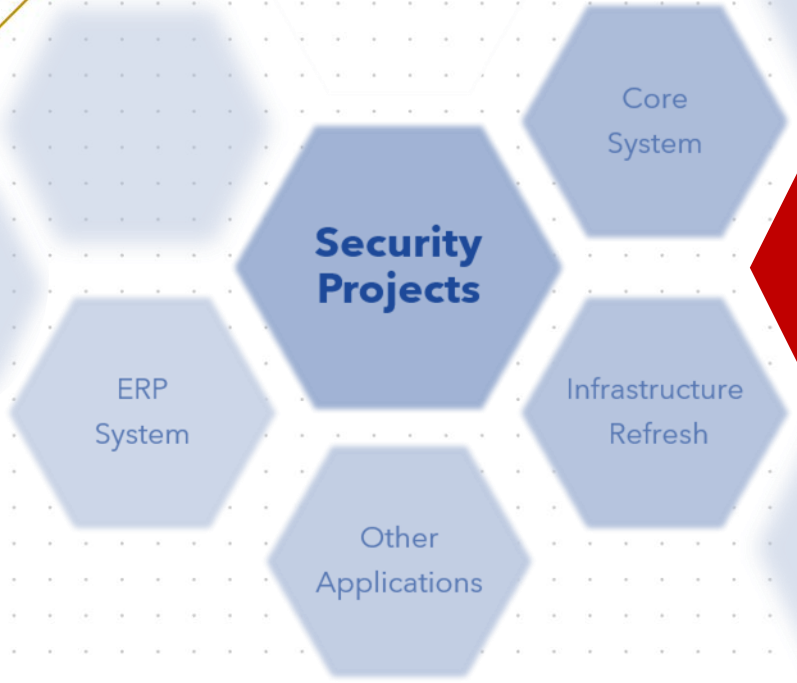
To Be a Top Tier Corporate Registry and Regulatory Authority

To ensure success and sustainability of this digital transformation, Client needs to properly address the cybersecurity needs of the modern enterprise



Security Concerns

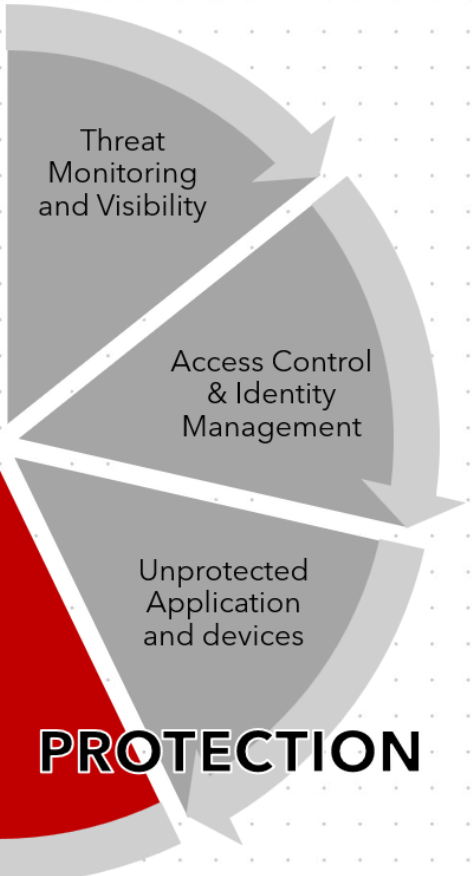
- Security should be at the forefront of all digital transformation initiatives, ideally at the planning and design stages right at the beginning.
- Requirement for security is changing, The company is seeing a shift in focus now for a more integrated and complete security platform that enables defence, detection and response.



Integration of Security With Other Transformation Programme

KEY CONSIDERATIONS:

- Overall Infrastructure Security Platform
- Database Protection
- Identity Management
- SSO Management
- Performance vs Security



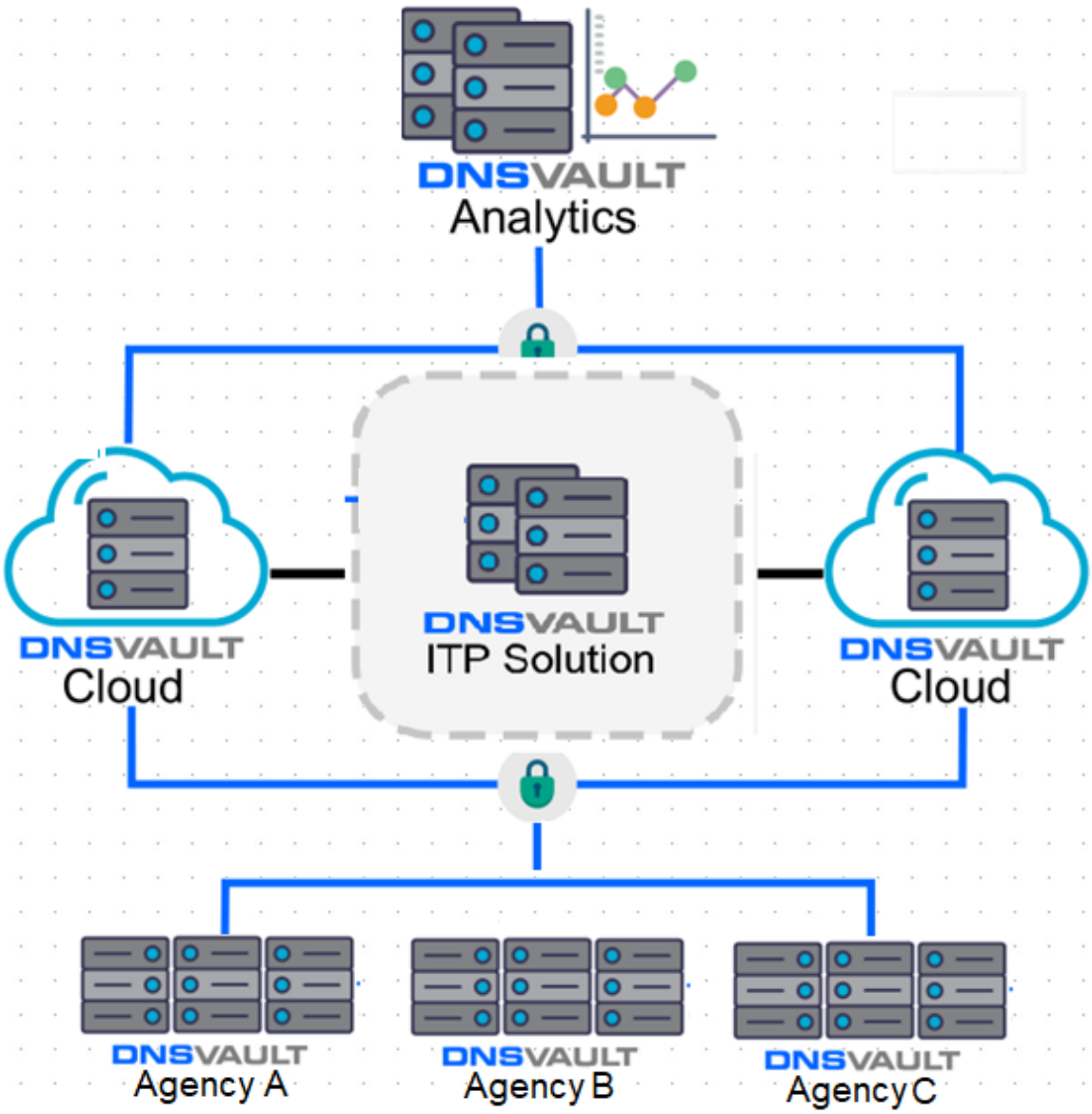
Secure-X Success Outcome

- IDENTITY MANAGEMENT
- HIGH AVAILABILITY AND RESILIENCY DESIGN
- CENTRALIZED 24 x 7 SECURITY OPERATION CENTER
- INTEGRATED LAYERED THREAT ENDPOINT, DETECTION & RESPONSE
- PLAYBOOK SECURITY FOR PROCEDURE FOR INCIDENT RESPONSE MANAGEMENT

DNSVAULT

Protecting Malaysia Government DNS with DNSVault Hybrid

The Malaysia government is using DNSVault Hybrid to improve DNS security and efficiency. It includes a central management dashboard and advanced security features to protect against threats and ensure smooth operation of e-Government.



Challenges

- Ensuring the security of the DNS system against cyber threats such as DNS spoofing, cache poisoning, DNS amplification attacks and DDoS attacks.
- Ensuring the efficiency of the DNS system to handle growing number of government agencies and volume of DNS traffic
- Integrating the DNS systems of different government agencies into a single, centralized system.

Solutions

- Implementing DNSVault Hybrid for enhanced security and management
- Implementing a scalable and robust DNS infrastructure that can handle the growing demands on the system
- Implementing a comprehensive DNS solution with advanced management and maintenance processes

Achievements

- Implemented advanced DNS solution DNSVault Hybrid
- Ensured security of government's DNS system by protecting against various threats
- Implemented scalable and robust DNS infrastructure
- Implemented comprehensive and flexible DNS solution for government agencies
- Addressed challenges and ensured security and reliability of government's DNS system
- Ensure smooth operation of the DNS system

SECTORGARD

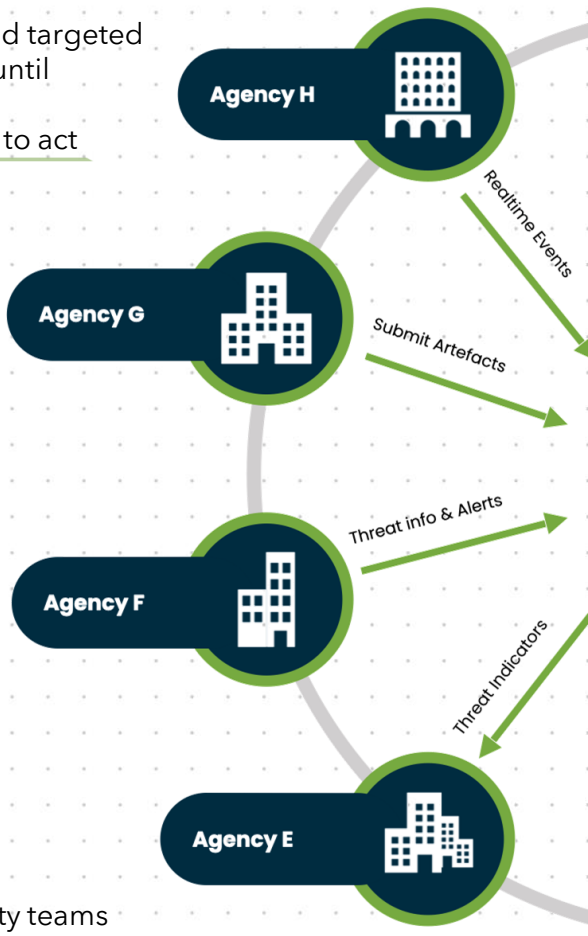
" There are no available solutions that can address needs of the Sector Leads and the challenges they face... "

In 2021, FinTIP was deployed using **Tecforte's SectorGard** platform and services for up to 100 Financial Institutions (FIs) under the purview of the Central Banking

Challenges faced by Sector Leads Addressed

Sector Leads serves the nation's public and other stakeholders Any security incidents within the Sector will impact the country and the respective stakeholders

1. No real time visibility and situational awareness for the entire sector
2. Sectoral members do not know they are vulnerable and targeted
   - They may not even know they are compromised until alerted or operations are impacted
   - Lose the chance to prevent or even miss the time to act
3. Sector Lead and Member Organizations are unable to see what the hackers see – an outside-in view of the risks and vulnerabilities
4. Unable to effectively assist Member Organizations on what to do to prevent, respond and recover
5. Unable to minimize MTTR for the Sector as a whole
6. Unable to contextualize Global Threat Intelligence
7. Unable to effectively, securely communicate & Share threat intelligence across hundreds of Member Organizations with different CIOs and security teams



SectorGard Achievement

1ST OF ITS KIND, ALL-IN-ONE PLATFORM 01
- Facilitating aggregation and analysis of TI and logs
- Allows threat intelligence to be exchanged dynamically and anonymously among members

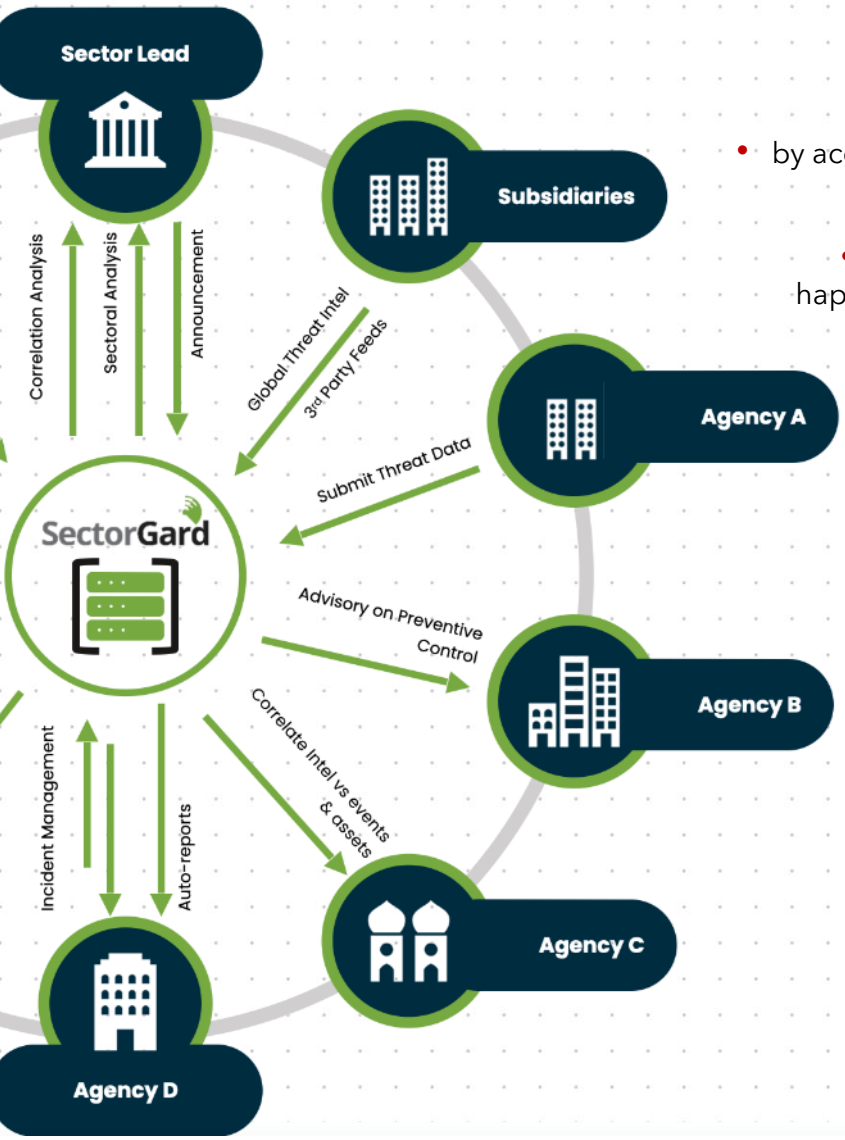
GATHERS TI FROM LOCAL FIs AND GLOBALLY 02
- Allowing preventive measures to be taken

RISK SCORINGS 03
- Understand risk level and allows prioritization of actions

ALLOW FIs TO CONDUCT INVESTIGATIVE WORK 04
- by acessing our database and analysts

PHASE 2 OF FinTIP 05
- Confirm the threats are already happening and if any resolutions are available to lower MTTR

COMPLIANCE REPORT 06
- (ISO27001, PCI DSS, etc),
- Threat Landscape Reports, Benchmarking, and etc



NSI . NEXA SECURITY INTEL

Instant Protection with hassle-free deployment of cloud or hybrid-based security solution ... and enjoy a simplified cyber security management with NSI

Challenges

Pandemic lockdown
- Borders are closed for any international projects

ISMS Certification Procedure
- All ISMS process are limited as the procedures required consultant to be on site.

Timeline ISMS Certification
- Normal ISMS Certification procedure takes more than a year

nexagate

NSI Success Solutions

DIGITAL EXPERIENCE

- All ISMS documents able to approve by our digital routed approval system
- 100% successful remote consulting
- Communication is fully virtual with Indonesian Certification Body

COMPLETED TIMELINE

- Complete a project earlier than estimated timeline (9 Months)

TOTAL VISIBILITY

- Live tracking Compliance Progress for management report

Power your businesses with digital signatures on a trusted, secure and seamless platform.

Employee On-Boarding

Challenges

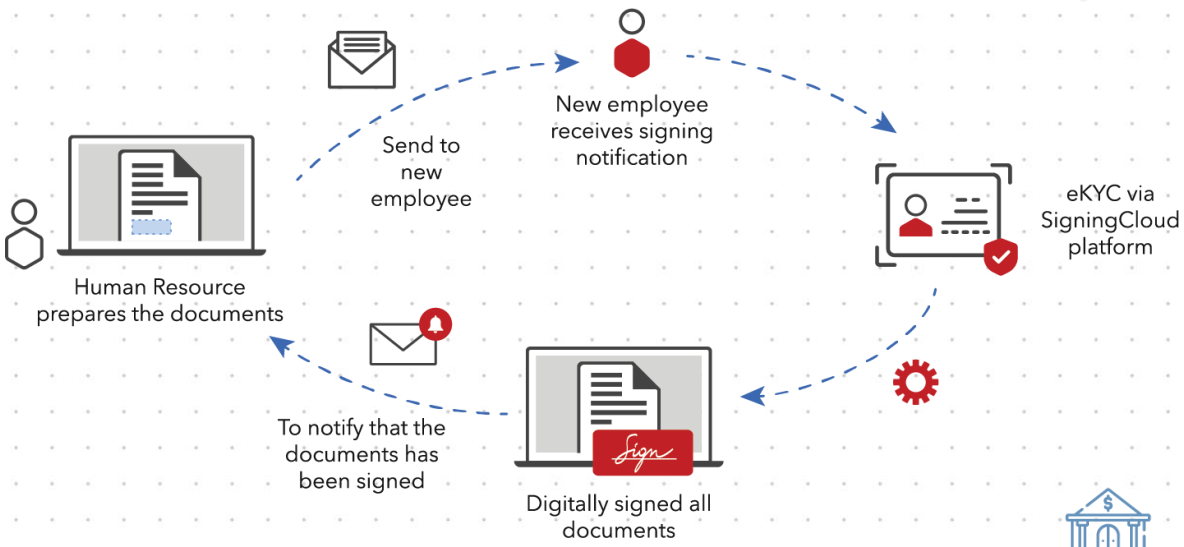
01 Plenty of paperwork document such as an NDA, contract form, salary offer, etc.

02 The new employee is require to come to the office for signing the document.

03 HR needs to send multiple emails and follow ups.

Solution

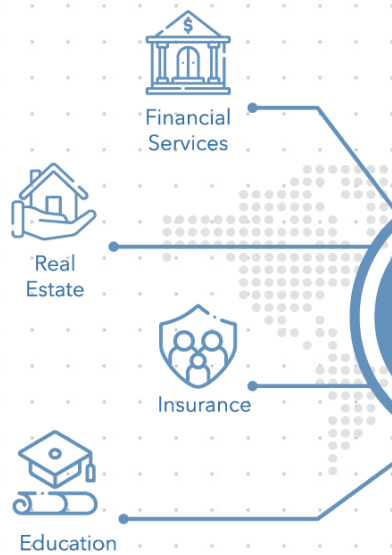
All the documents can be handled easily by using digital signing solution where the new employee doesn't require to come to the office for signing the document.



Employee On-Boarding User Journey Flow

Results

- Streamlined interactions with new employees
- Effectively manage employee data
- Saves time and manpower
- Eliminate human errors and mistakes



SigningCloud

Business Non-Disclosure Agreements

Solution

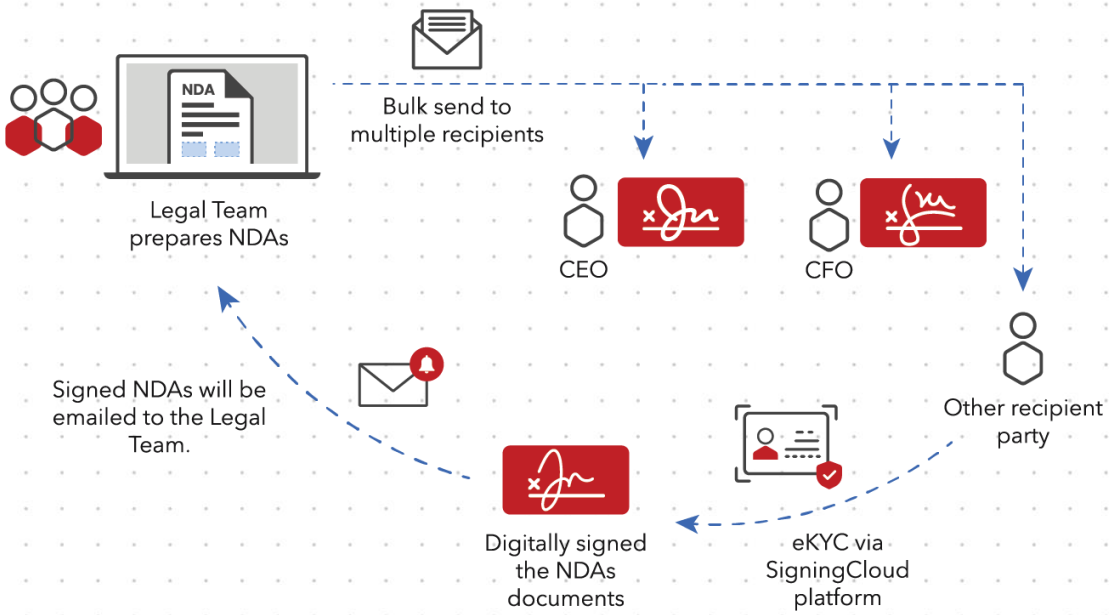
All the documents can be handled easily by using digital signing solution where the new employee doesn't require to come to the office for signing the document.

Challenges

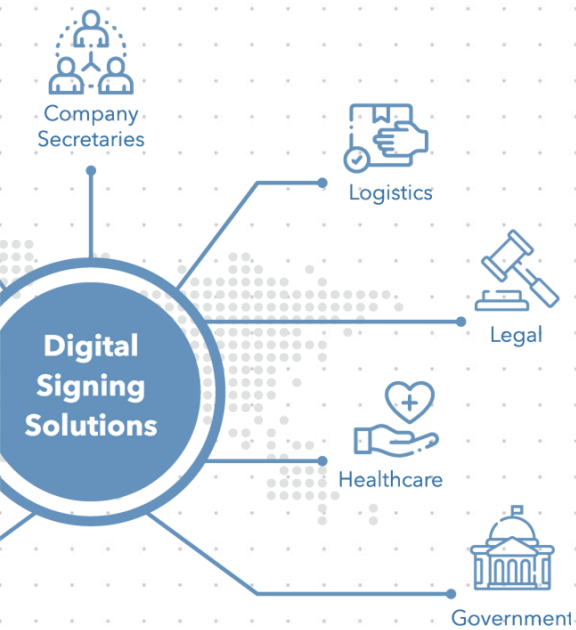
01 Concerned about the disclosure of trade secrets by another party.

02 Pen and paper are inconvenient to use.

03 Signing documents is difficult if both parties are not in the same place.



Business NDAs User Journey Flow



Results

- Streamlined documents workflows
- Faster return of signed documents
- A signed NDA can be obtained without delay

05 SUPPORTED AGENCIES

CYBERSECURITY LEADERS

The supporting agencies have key role in driving the country's cybersecurity community and position as a digital hub

KEMENTERIAN KOMUNIKASI DAN DIGITAL

Empowering the society to be Connected, Informative, Creative and Digitally Cultured

JABATAN PERDANA MENTERI
UNIT PEMODENAN TADBIRAN DAN PERANCANGAN PENGURUSAN MALAYSIA (MAMPU)

Spearheading the digital government initiatives

KEMENTERIAN EKONOMI

Leader in the nation's socioeconomic development, which are inclusive, progressive and sustainable for the wellbeing and prosperity of the rakyat

MDEC™

Leading Malaysia's digital economy forward to ensure easy access. With the goal of achieving shared prosperity, for all.

NACSA
AGENSI KESELAMATAN SIBER NEGARA
NATIONAL CYBER SECURITY AGENCY

Driving National Cyber Security Initiatives

MCMC

Establishing a communications and multimedia industry that is competitive, efficient and increasingly self-regulating, generating growth to meet the economic and social needs of Malaysia

CGSO
CHIEF GOVERNMENT SECURITY OFFICE

Empowering holistic, integrated and high-impact security protection and critical target management

MyDIGITAL CORPORATION

Innovating Malaysia's Digital Landscape

CyberSecurity MALAYSIA

Leading the development of a safer and more resilient cyber ecosystem to enhance national security, economic prosperity, and social harmony

NACSA
AGENSI KESELAMATAN SIBER NEGARA
NATIONAL CYBER SECURITY AGENCY

MDEC™