

ATTACK SURFACE MANAGEMENT (ASM)

Name:



GOIP Group - A Leading Network and System Integration Service Provider in Hong Kong & Mainland China.

Our team is built-up with certified engineers and professional project managers in providing innovative solutions and to solve mission critical tasks in order to simplify customers' operations.



ATTACK SURFACE MANAGEMENT (ASM)



- Source scanning
Native protection
- Vulnerability assessment
- Penetration testing
- Remedies
- Security operation centre (soc)


Consequences of Company Data Leakage

CYBERATTACK NEWS (2023)

sky news · 1 天 · on MSN

Royal Family's official website targeted in cyber attack


The royal website has been hit by a cyber attack, a royal source has told Sky News. The denial of service attack, or DDoS, is ...



BLEEPINGCOMPUTER · 6 天

Sony investigates cyberattack as hackers fight over who's responsible


Sony says that it is investigating allegations of a cyberattack this week as different hackers have stepped up to claim ...



MARKETS INSIDER · 13 小時

Clorox Shares Could Rally As Operations Revive After Cyberattack, Says Bullish Analyst

Clorox Co (NYSE:CLX) continues to estimate the financial impact of a crippling cyberattack. The company's shares spiked on ...



Financial Loss




Loss of Customer Trust



Reputation Damage



Data Breach and Privacy Concerns



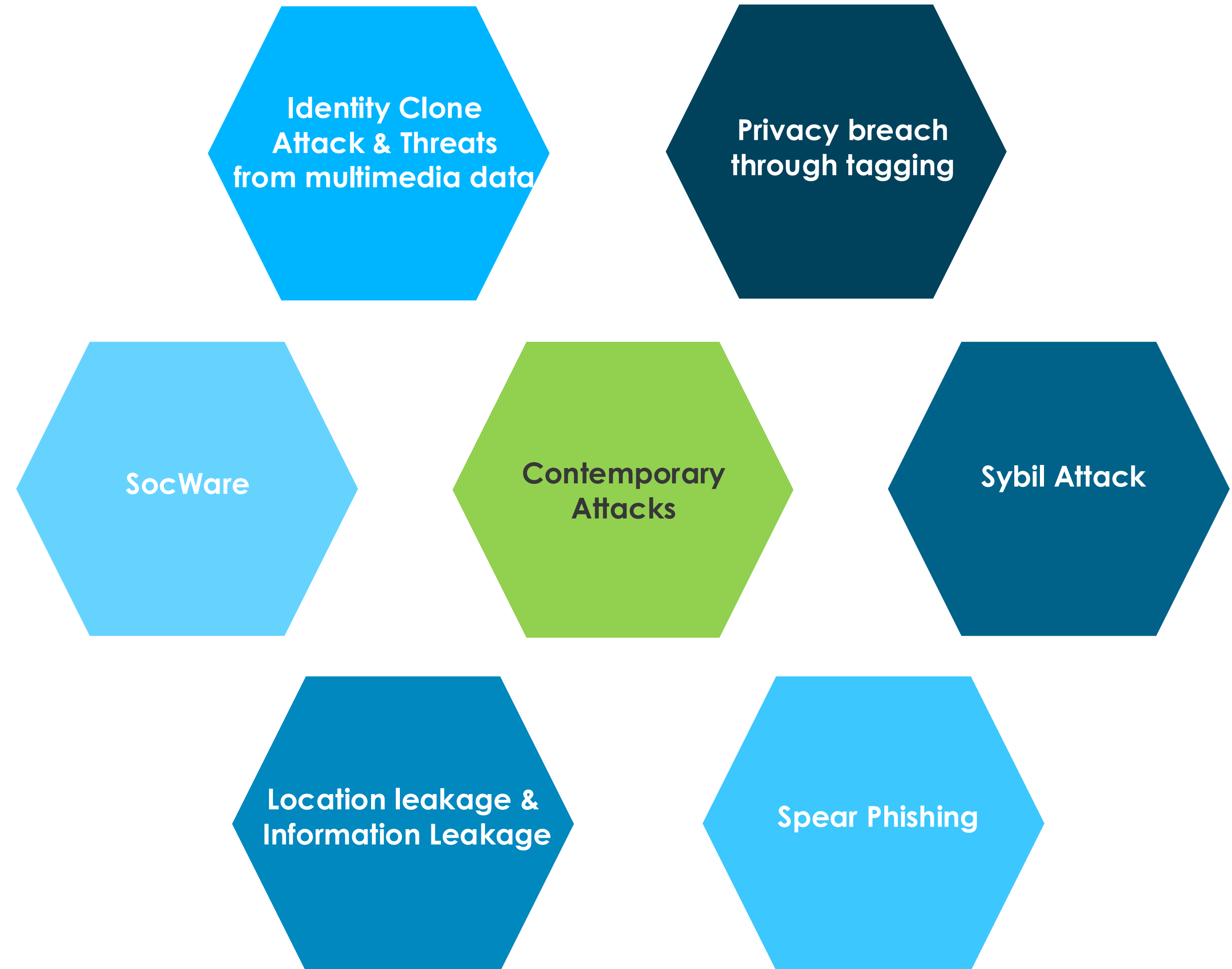
Disruption of Operations



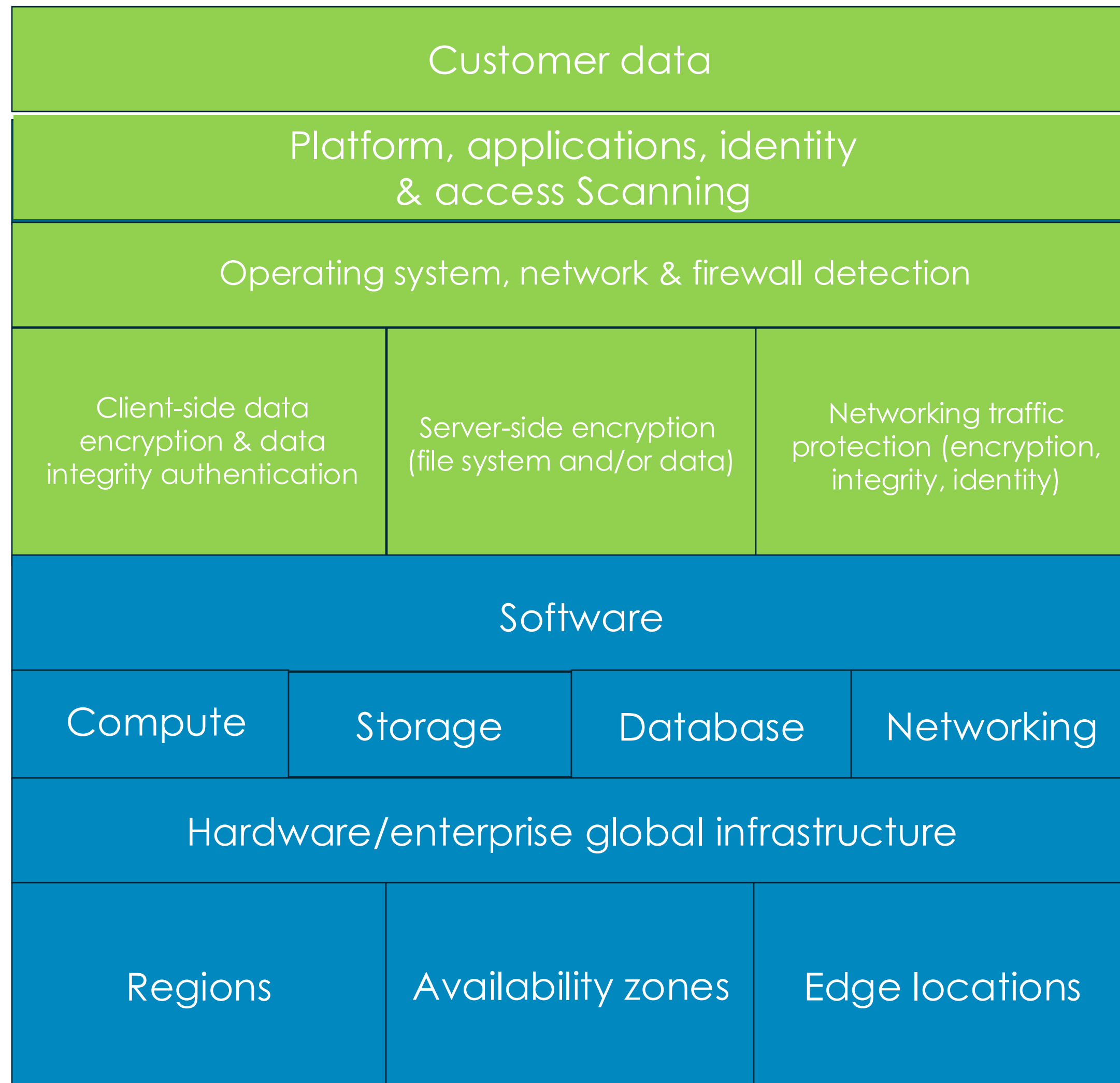
Legal and Compliance Issues



Cyber attacks **are increasing every day** with the increased use of **mobile and Web applications**, Globally, statistics show that more than **70 per cent** of the applications either have vulnerabilities which could potentially be exploited by a hacker, or worse, they have already been exploited.



Delivering Security in the Cloud Requires Close Collaboration



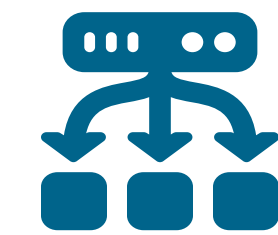
GOIP Group



Network Security

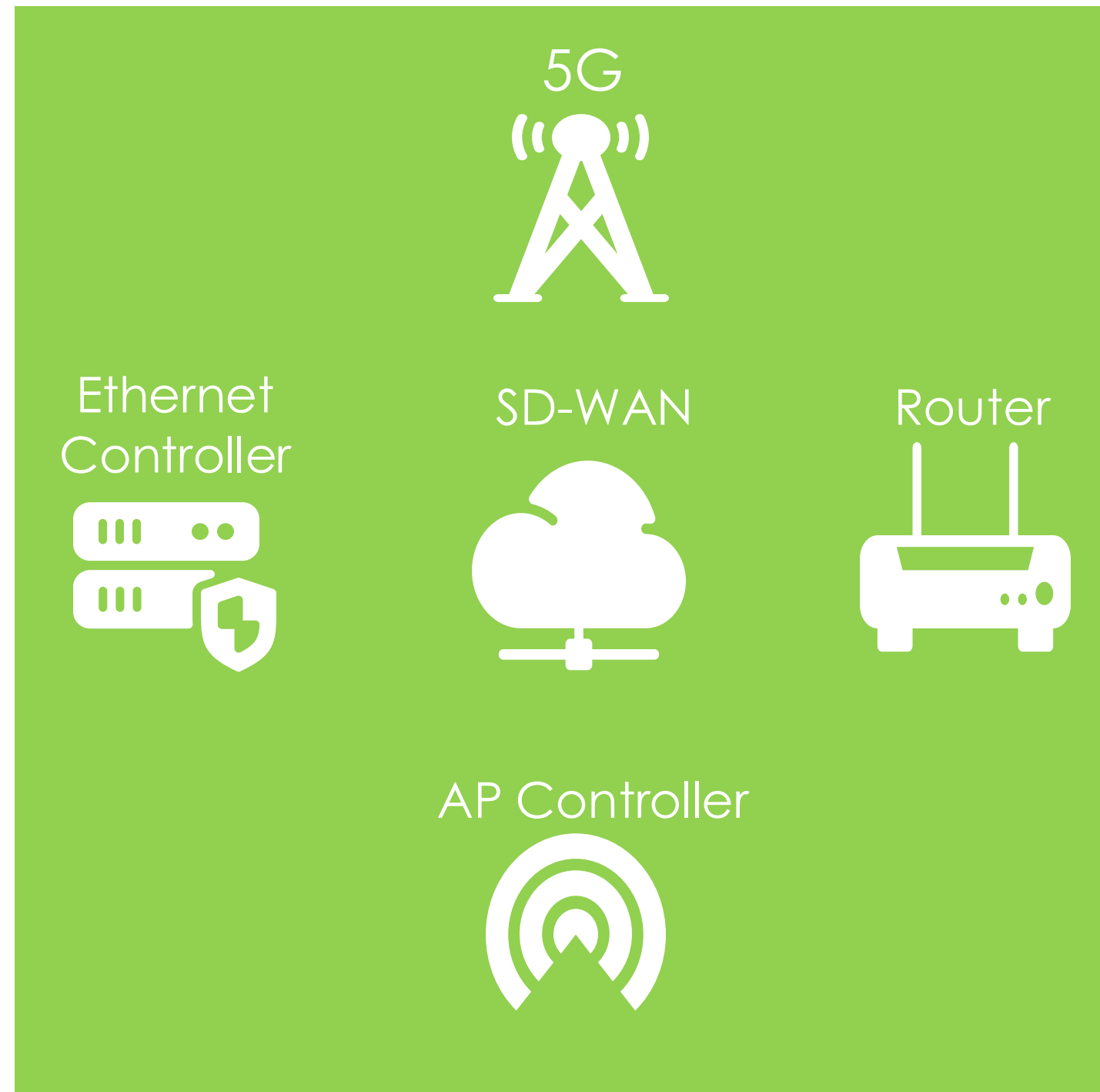


Application Security

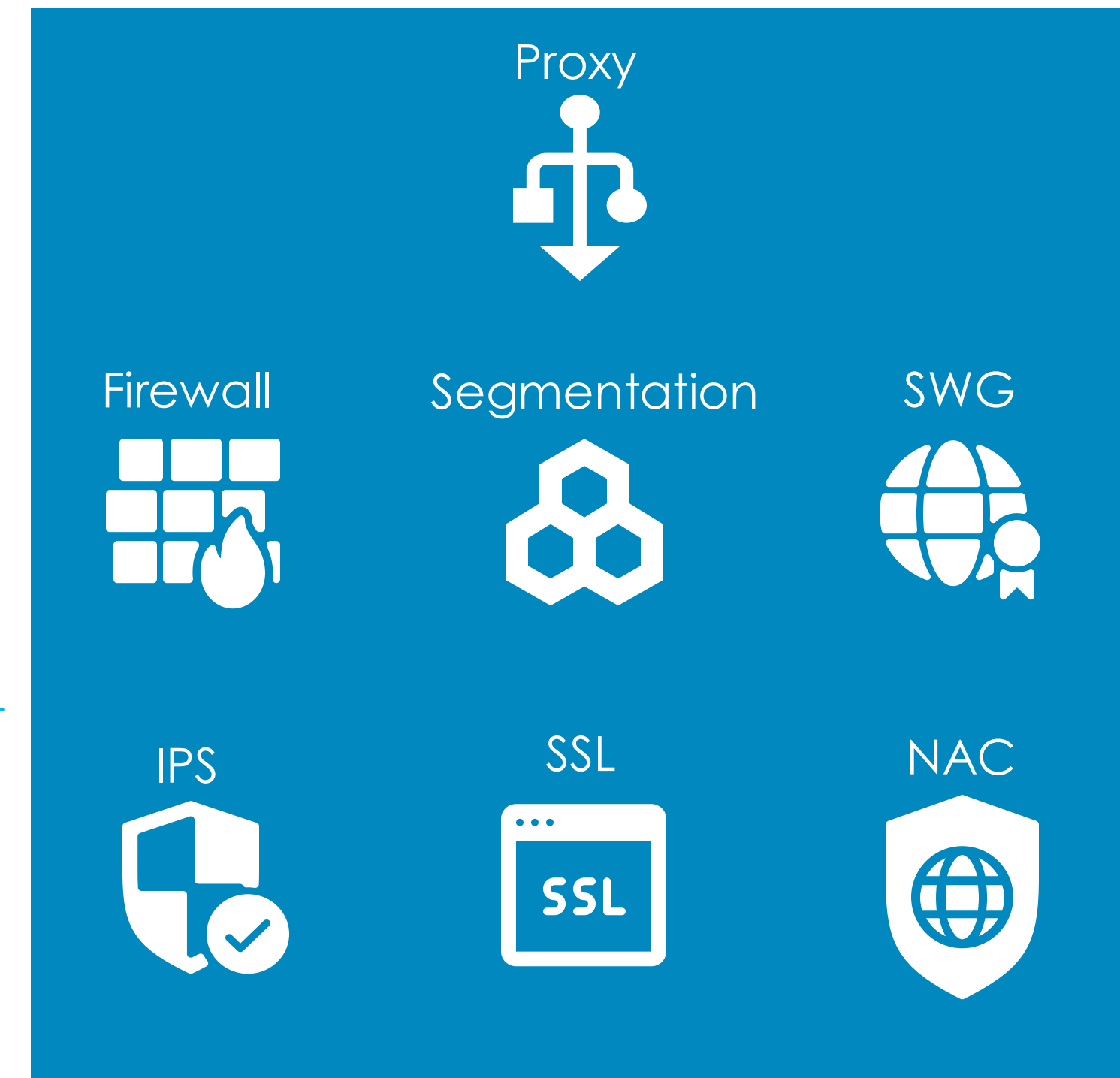


Platform Visibility & Control

Networking

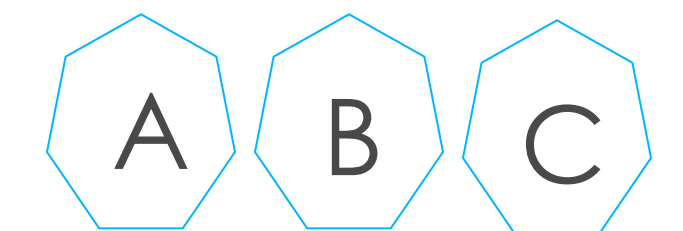


Security

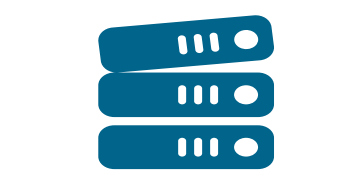


Actionable Threat Intelligence Management

EDGENETIC



Appliances Lack Awareness



Appliance



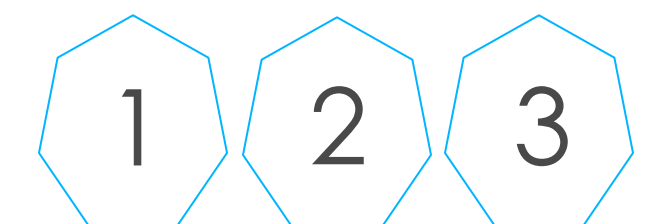
Virtual



Container



SaaS



Software Delivers Network Awareness

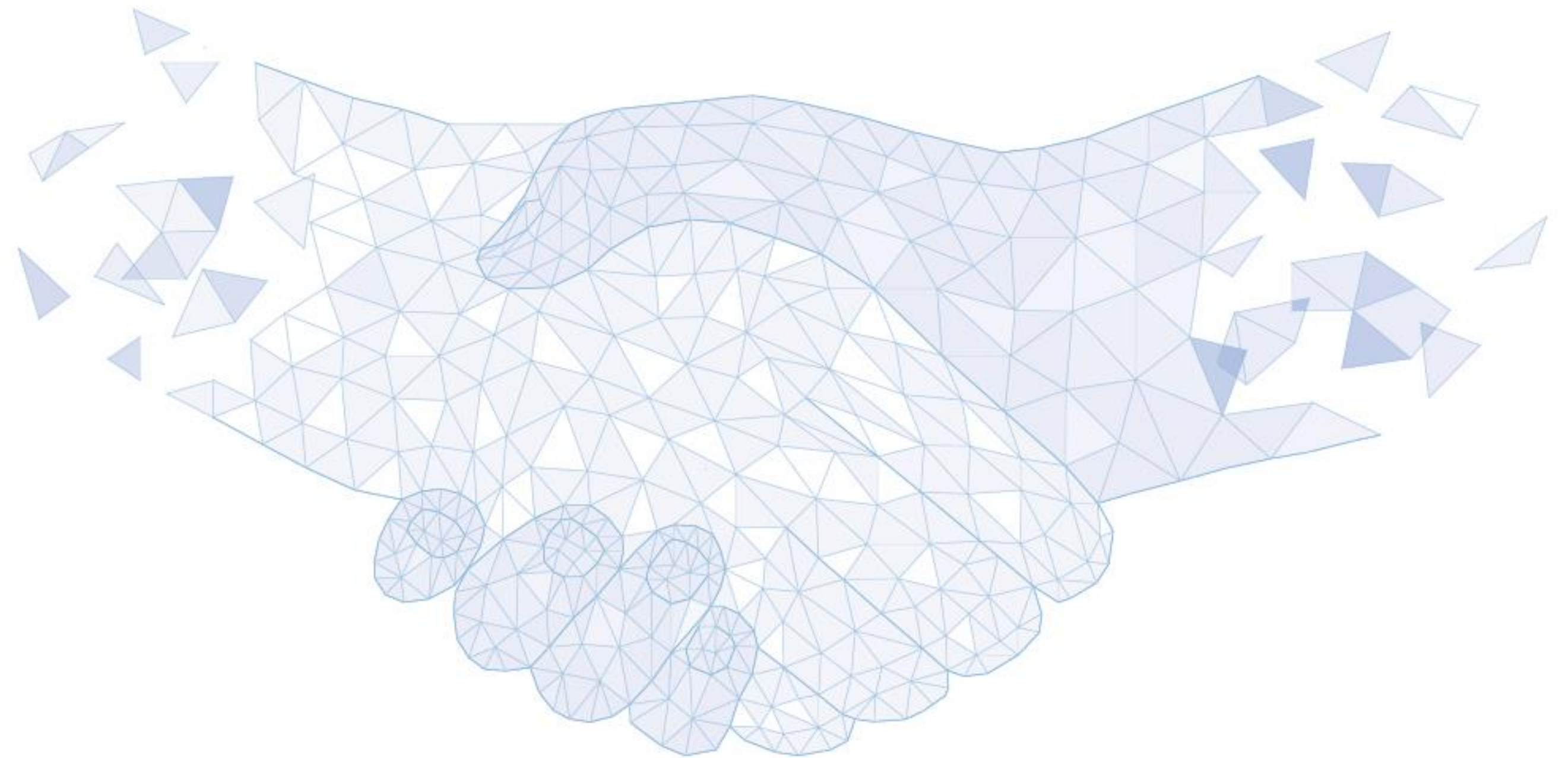
EDGENETIC Native Protection Source Scanning

Source Scanning

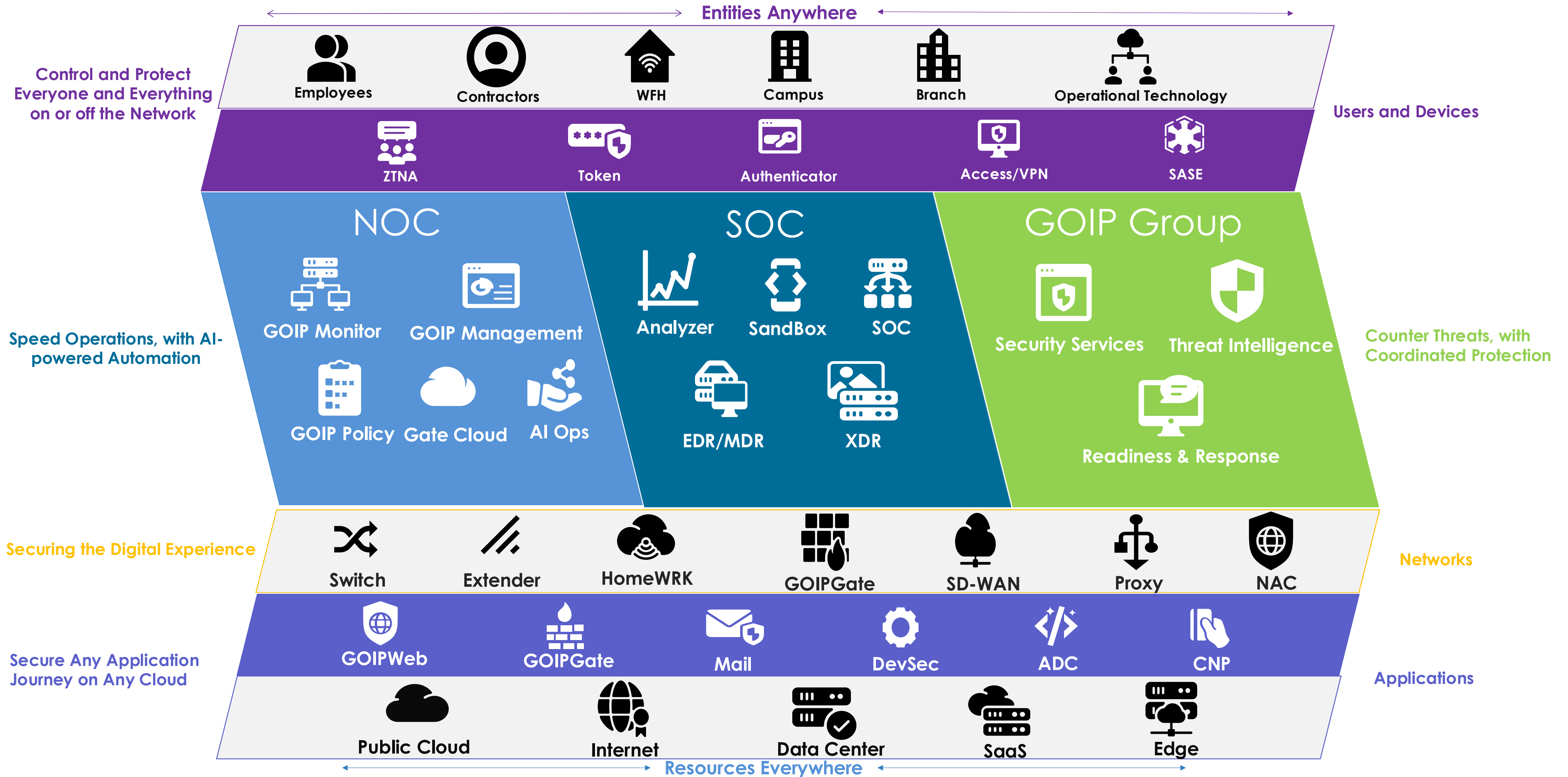
■ KEY CAPABILITIES

■ PROCESSING

■ REPORT



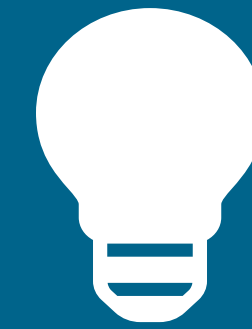
GOIP Group Technology Vision



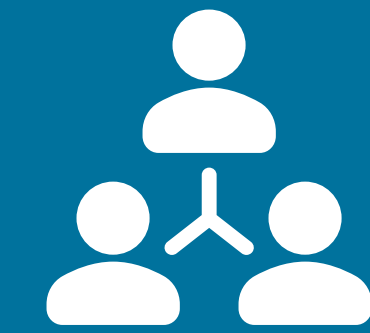
What is Source Scanning?

To solve the problem of unclear asset sorting in the interconnected network, **GOIP Group** uses its unique high-precision asset tags to help customers quickly sort out the assets exposed on the interconnected network side.

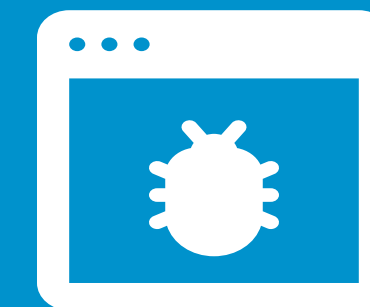
This is done by:



Scanning the exposed devices in the interconnected space



Assisting in discovering the device occupancy in different regions



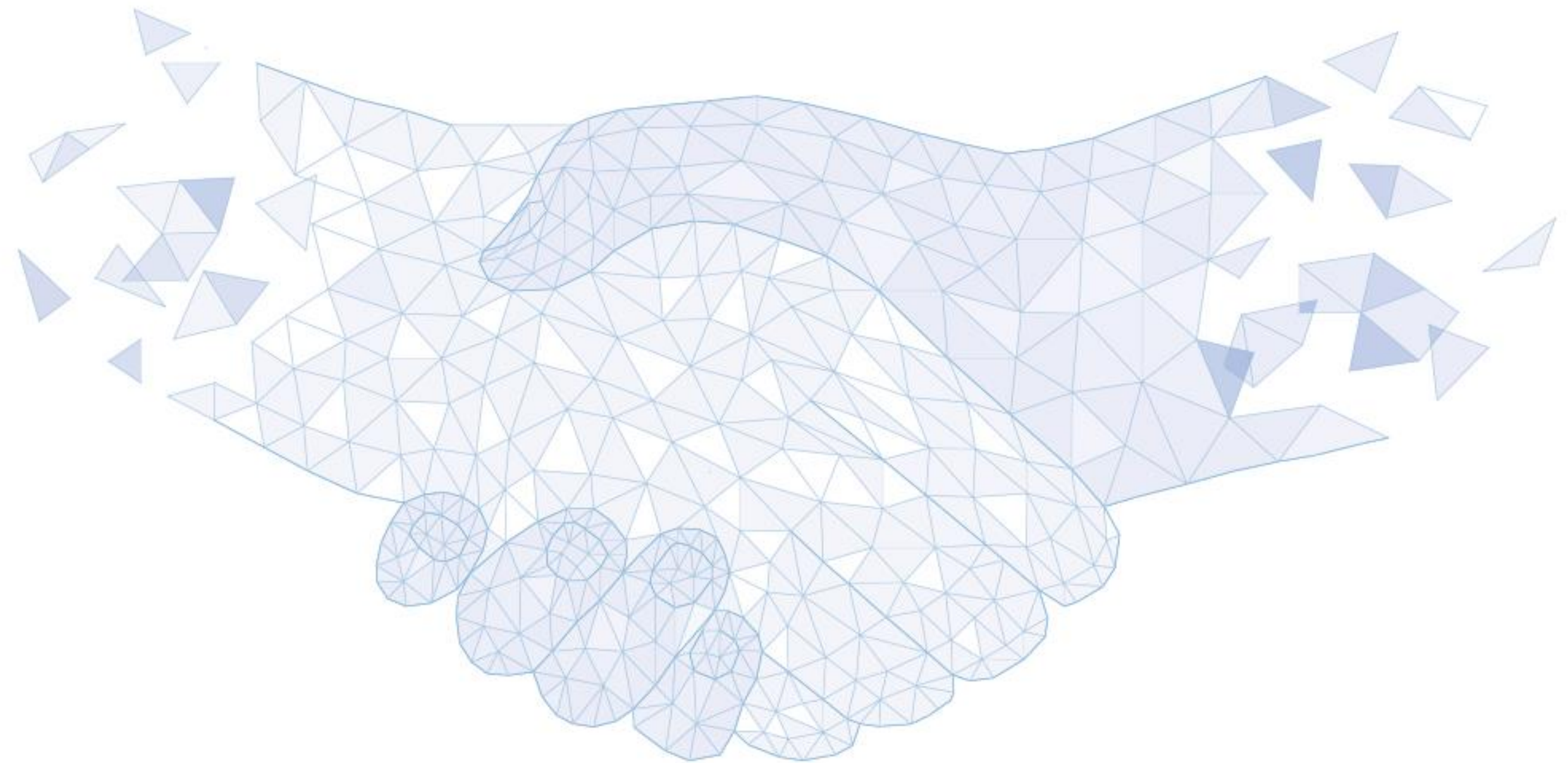
Helping customers understand which Internet assets should be focused on



Providing information about the potential unknown risks of exposed assets

Source Scanning

- KEY CAPABILITIES
- **PROCESSING**
- REPORT



Source scanning helps organizations proactively detect and address security vulnerabilities, ensure compliance with industry standards, improve code quality and maintainability, optimize performance, mitigate risks associated with third-party components, and protect intellectual property.



Step 1

Simple
Questionnaire



Step 2

GOIP Group
Permission Letter

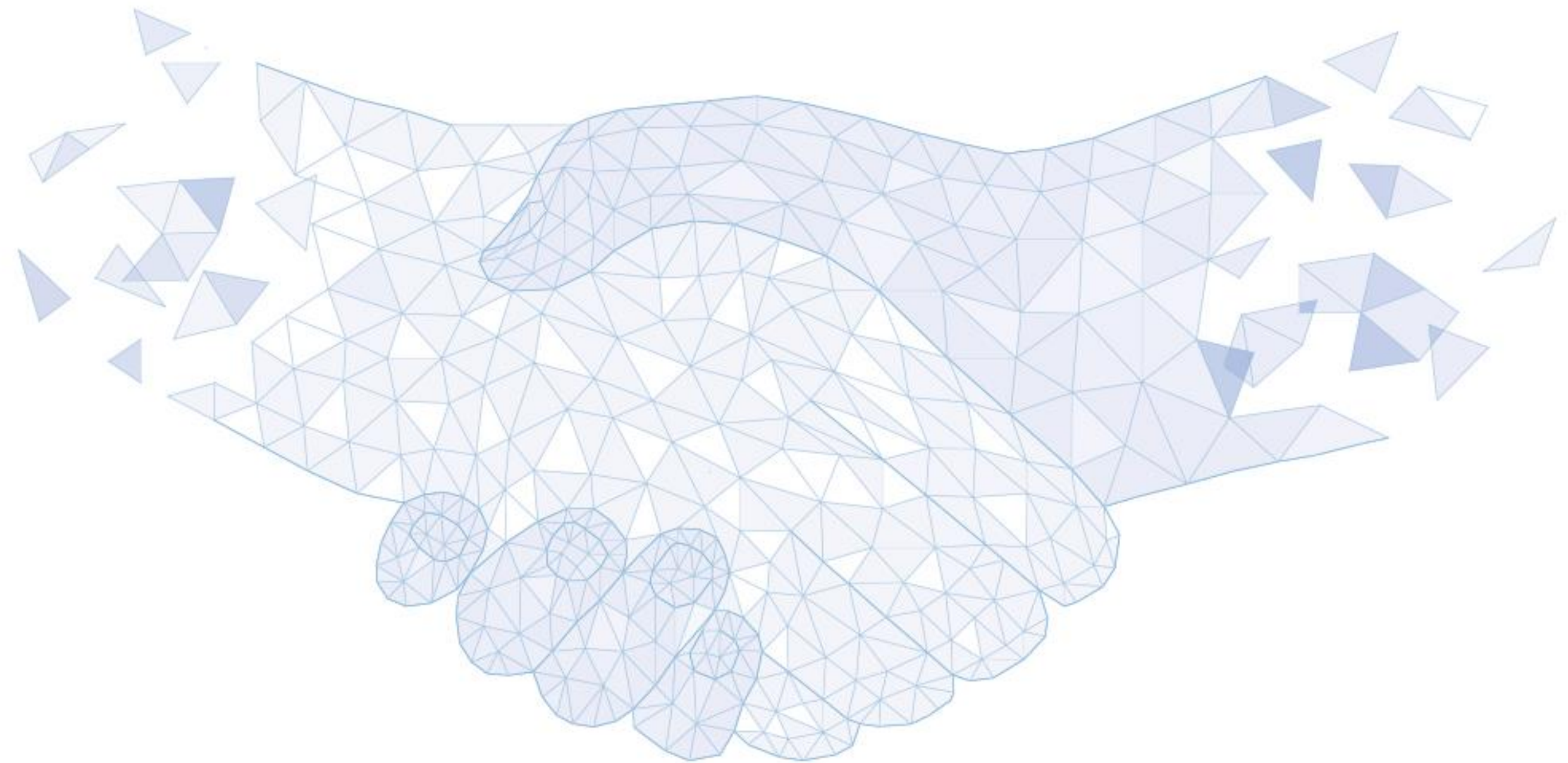


Step 3

Report
(3 Business days)

Source Scanning

- KEY CAPABILITIES
- PROCESSING
- **REPORT**



- Includes detailed statistics on Internet scanning of assets, providing clear visibility into network assets and risks.
- Ensures legality and compliance, meeting the inspection requirements of higher-level regulatory authorities and fulfilling the needs of IT operations and maintenance.
- Comprehensive analysis and statistics of risk assets, offering professional Internet risk mitigation solutions to address specific issues.



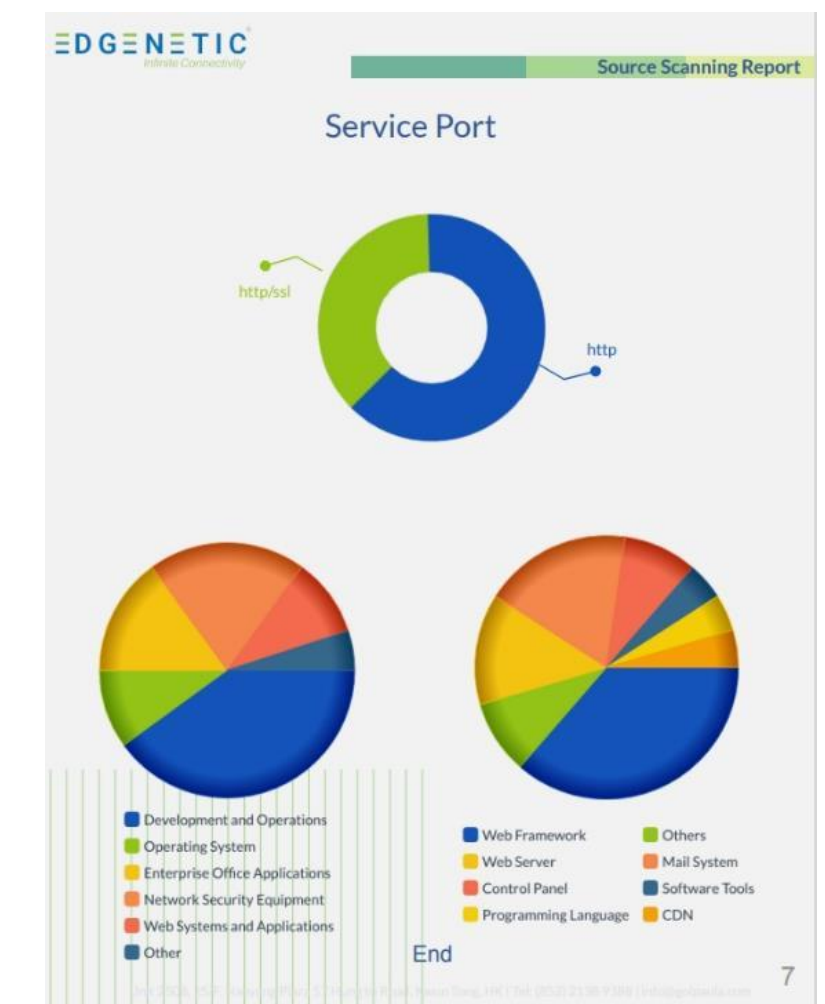
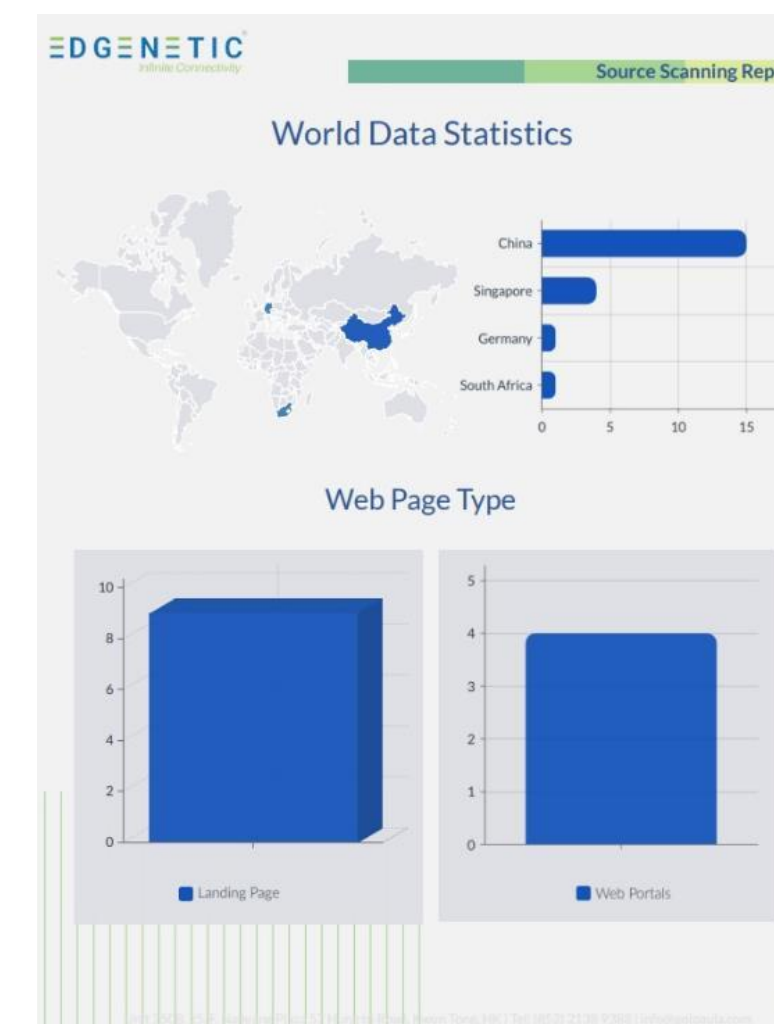
Source Scanning Report

The scanning results of this Attack Surface Management.
Total of 21 associated results. Among them, 10 associated IPs and 11 associated domains were detected.

HOST	DOMAIN	PORT & SERVICE	WEBSITE TITLE	
1	20.190.190.132	msoid.ncar.etc.com	443 http/svl	Object moved
2	23.306.49.70	oncarecc.com.hk	443 http/svl	IT Managed Services Provider Hong Kong CN-CARE Hong Kong
3	40.99.222.184	autofiscover.oncarecc.com	80 http	...
4	47.90.111.134	bmponcarecc.com	80 http	CN Care
5	47.112.27.149	oncarecc.com	443 http/svl	CN Care
6	47.112.27.149	www.oncare.tech	80 http	CN Care
7	47.112.27.149	oncarecc.com	80 http	CN Care
8	47.112.27.149	www.oncare.tech	80 http	CN Care
9	47.112.27.149	oncare.tech	80 http	CN Care
10	101.100.210.50	autofiscover.oncarecc.com	80 http	Default Web Site Page
11	101.100.210.50	webmail.oncarecc.com	443 http/svl	Webmail Login
12	101.100.210.50	webmail.oncarecc.com	80 http	Webmail Login
13	103.215.3.89	oncarecc.com.hk	2083 http/svl	cPanel Login
14	103.215.3.89	oncarecc.com.hk	2082 http	cPanel Login
15	103.215.3.89	oncarecc.com.hk	2086 http	WHM Login
16	103.215.3.89	oncarecc.com.hk	2095 http	Webmail Login
17	103.215.3.89	oncarecc.com.hk	2096 http/svl	Webmail Login
18	103.215.3.89	oncarecc.com.hk	2087 http/svl	WHM Login
19	125.77.142.198	www.oncarecc.com	443 http/svl	CN Care
20	183.60.153.17	cm.oncarecc.com	80 http	Fee/Ec
21	220.181.125.251	www.oncarecc.com	80 http	CN Care

Source Scanning Report

APPLICATION VERSION	MIDDLEWARE	LOCATION	AUTONOMOUS SYSTEM	AUTONOMOUS SYSTEM NUMBER
1	None	Johannesburg, Gauteng Province, South Africa	Microsoft Corporation	8075
2	jQuery +5	Singapore	Leaseweb Asia Pacific pte. Ltd.	59253
3	Microsoft IIS WebServer +5	Frankfurt am Main, Hesse, Germany	Microsoft Corporation	8075
4	Bootstrap +3	China Hong Kong	Alibaba Cloud	45102
5	ThinkPHPDevelopmentFramework +6	Shenzhen City, Guangdong Province, China	Alibaba Cloud	37963
6	LayNSThinkPHP+LayUI+6	Shenzhen City, Guangdong Province, China	Alibaba Cloud	37963
7	jQuery +6	Shenzhen City, Guangdong Province, China	Alibaba Cloud	37963
8	jQuery +6	Shenzhen City, Guangdong Province, China	Alibaba Cloud	37963
9	LayNSThinkPHP+LayUI+6	Shenzhen City, Guangdong Province, China	Alibaba Cloud	37963
10	Apache Web Server	Singapore	Vodien Internet Solutions Pte Ltd	58621
11	Horde +3	Singapore	Vodien Internet Solutions Pte Ltd	58621
12	Horde +3	Singapore	Vodien Internet Solutions Pte Ltd	58621
13	cPanelVirtual host management system+2	China Hong Kong	HUAWEI	136907
14	cPanelVirtual host management system+2	China Hong Kong	HUAWEI	136907
15	cpanel WHM +4	China Hong Kong	HUAWEI	136907
16	cPanelVirtual host management system+2	China Hong Kong	HUAWEI	136907
17	cPanelVirtual host management system+2	China Hong Kong	HUAWEI	136907
18	cPanelVirtual host management system+4	China Hong Kong	HUAWEI	136907
19	Tengine +7	Quanzhou City, Fujian Province, China	China Telecom	133776
20	Nginx Web Server	Dongguan City, Guangdong Province, China	China Telecom	4134
21	Tengine +7	Beijing China	China Telecom	23724



EDGENETIC Native Protection Vulnerability Assessment

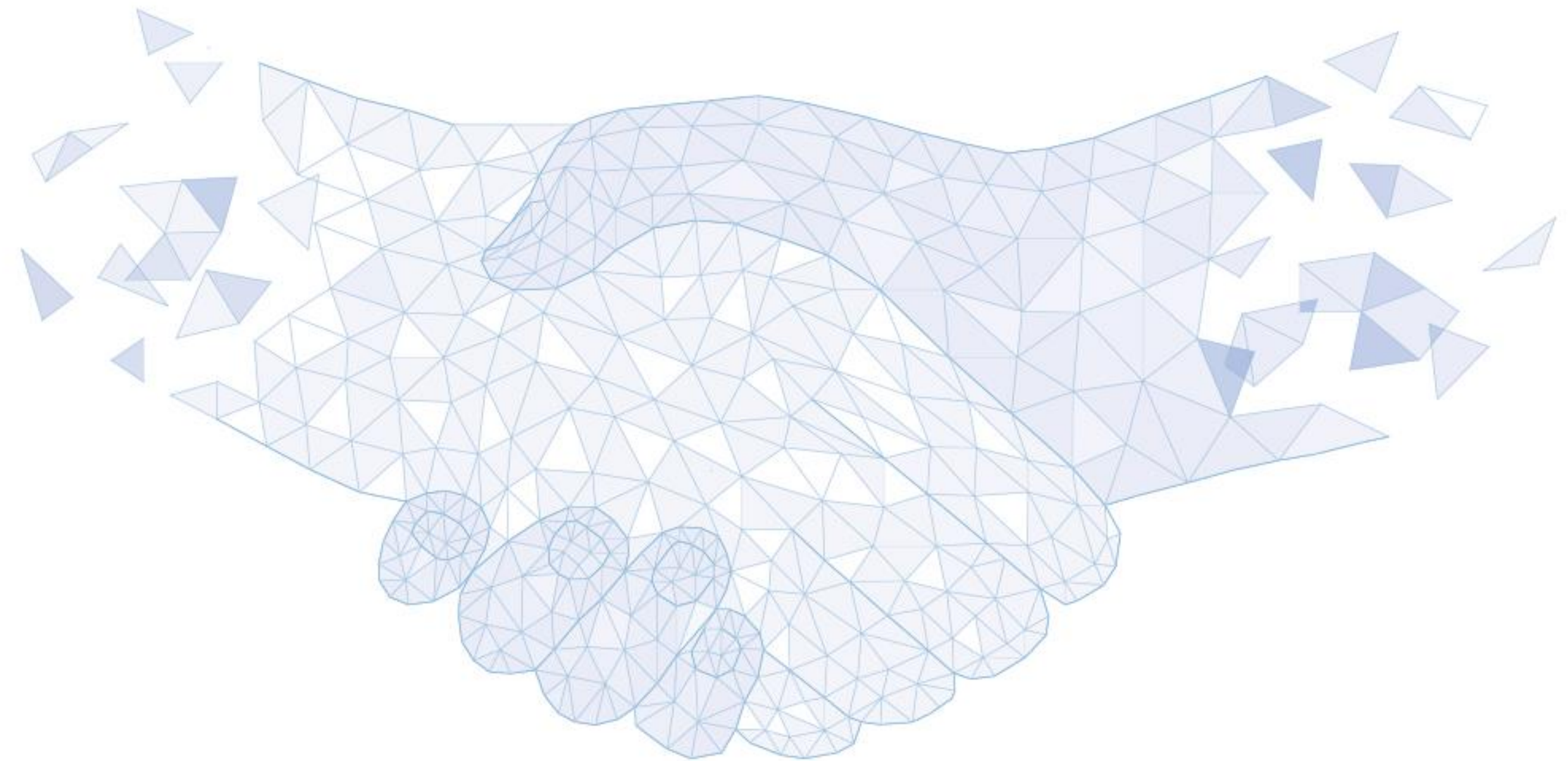


Vulnerability Assessment (VA)

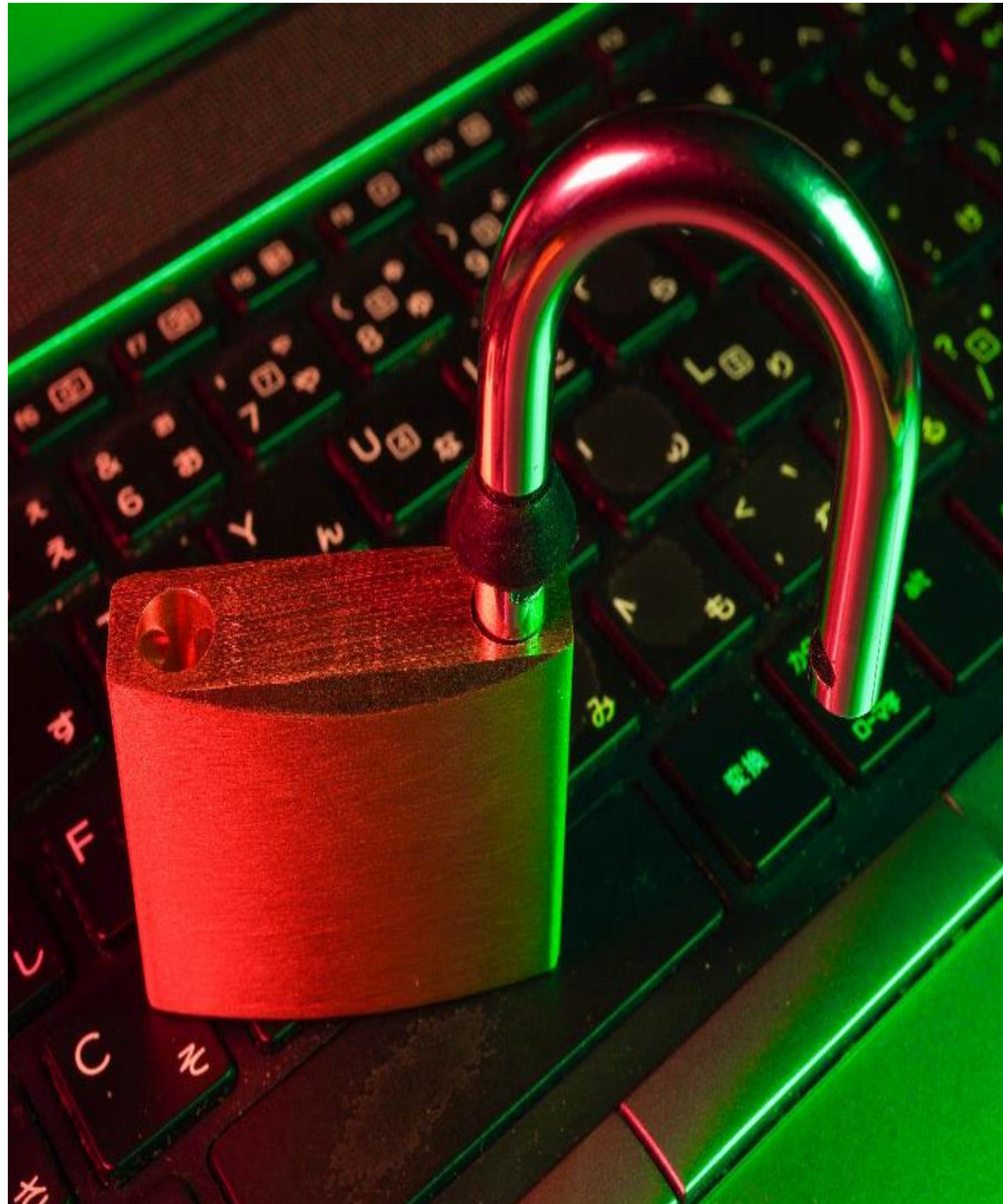
■ KEY CAPABILITIES

■ VA PROCESSING

■ REPORT & COMPARISON



What is Vulnerability Assessment?



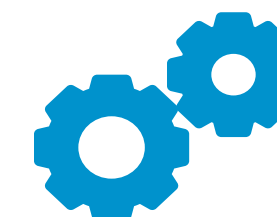
(VA) is a systematic technical approach to finding the security loopholes in a network or software system.



It primarily adopts a scanning approach which is done both manually and performed by certain tools.



The outcome of a VA process is a report showing all vulnerabilities, which are categorized based on their severity.



This report is further used for the next step, which is Penetration Testing (PT).



There are Two Types of VA Scans:

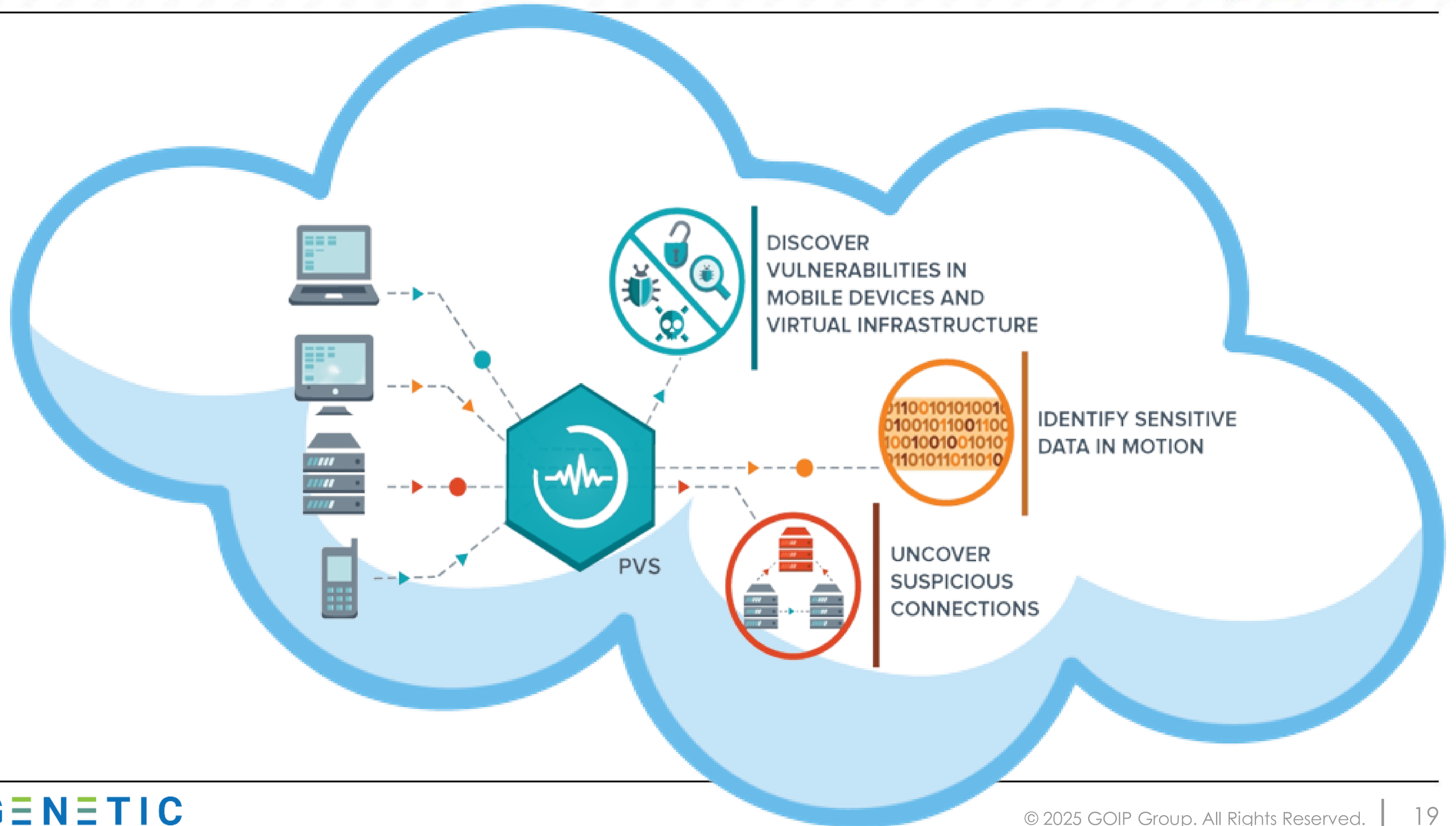
■ Internal VA scans:

Scan the internal network for access, vulnerabilities, and compliance issues. They are used to identify security risks before they can be exploited by attackers from inside the organization.

■ External VA scans:

Scan the external network for access, vulnerabilities, and attack surfaces. They are used to identify security risks that could be exploited by attackers from outside the organization.

Product should meet a certain consumer demand, or it should be so compelling that consumers believe they need it.



Internal VA Scanning

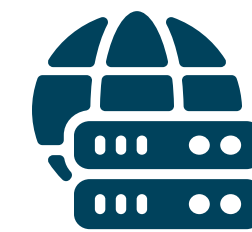


Performed Location Access Scanning

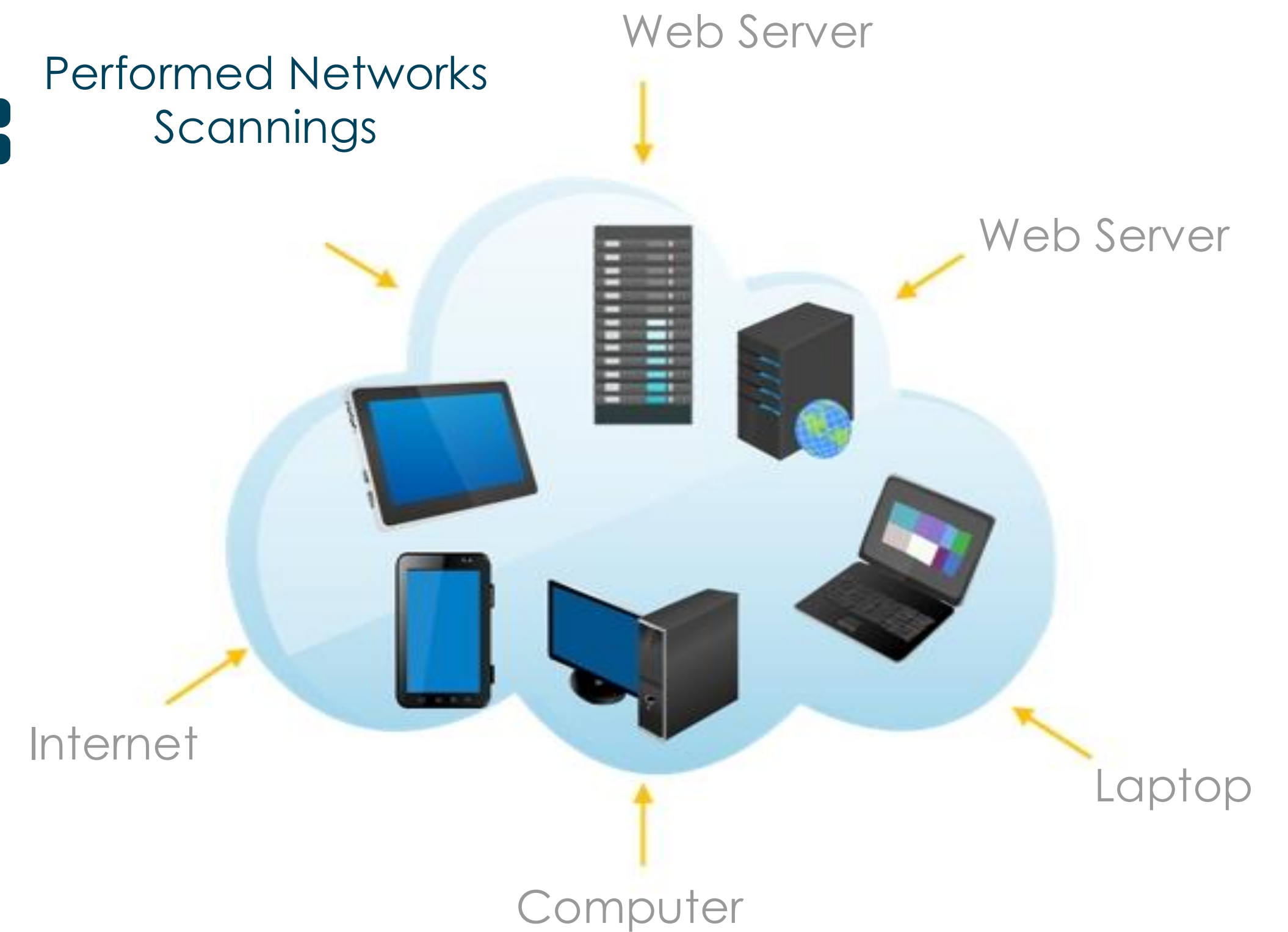


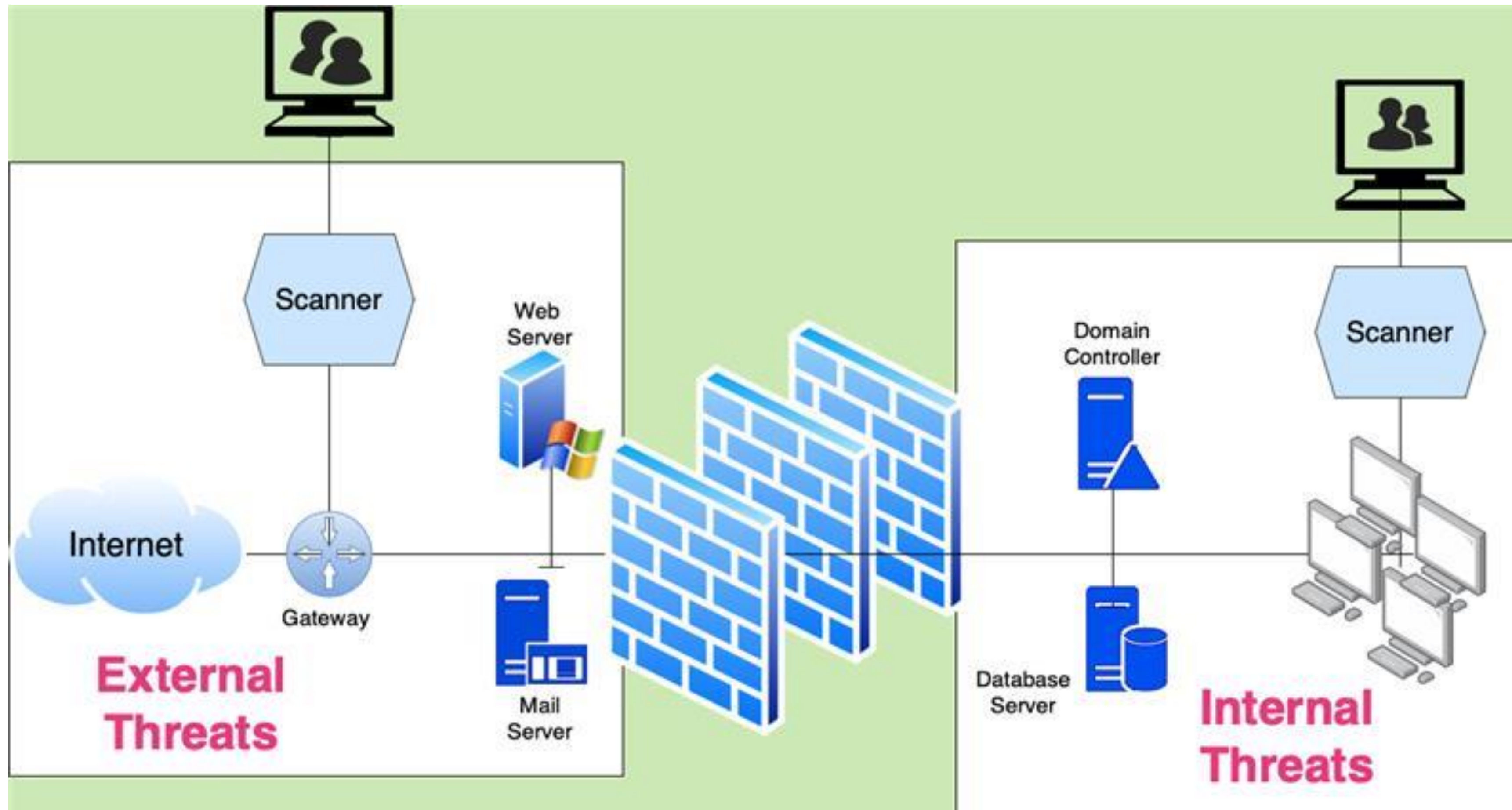
VS

External VA Scanning



Performed Networks Scannings







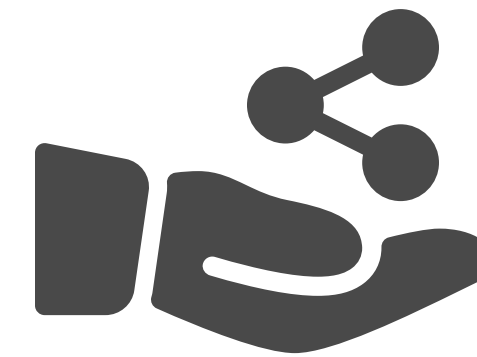
Improved Security Posture

By identifying vulnerabilities, organizations can take appropriate measures to strengthen their security posture, protecting their systems and data.



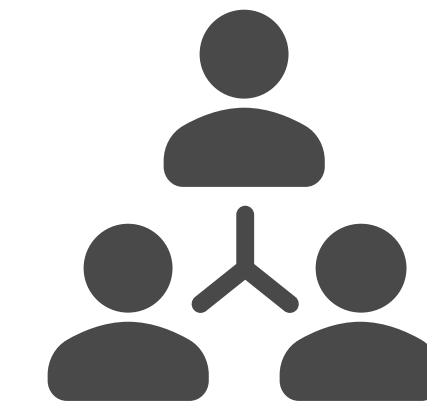
Prioritization of Remediation Efforts

VA helps prioritize vulnerabilities based on their severity, allowing organizations to allocate resources effectively and address the most critical issues first.



Cost-Effective Security Investment

Identifying vulnerabilities through VA helps organizations identify and address security issues before they can be exploited, potentially saving significant costs associated with security breaches.

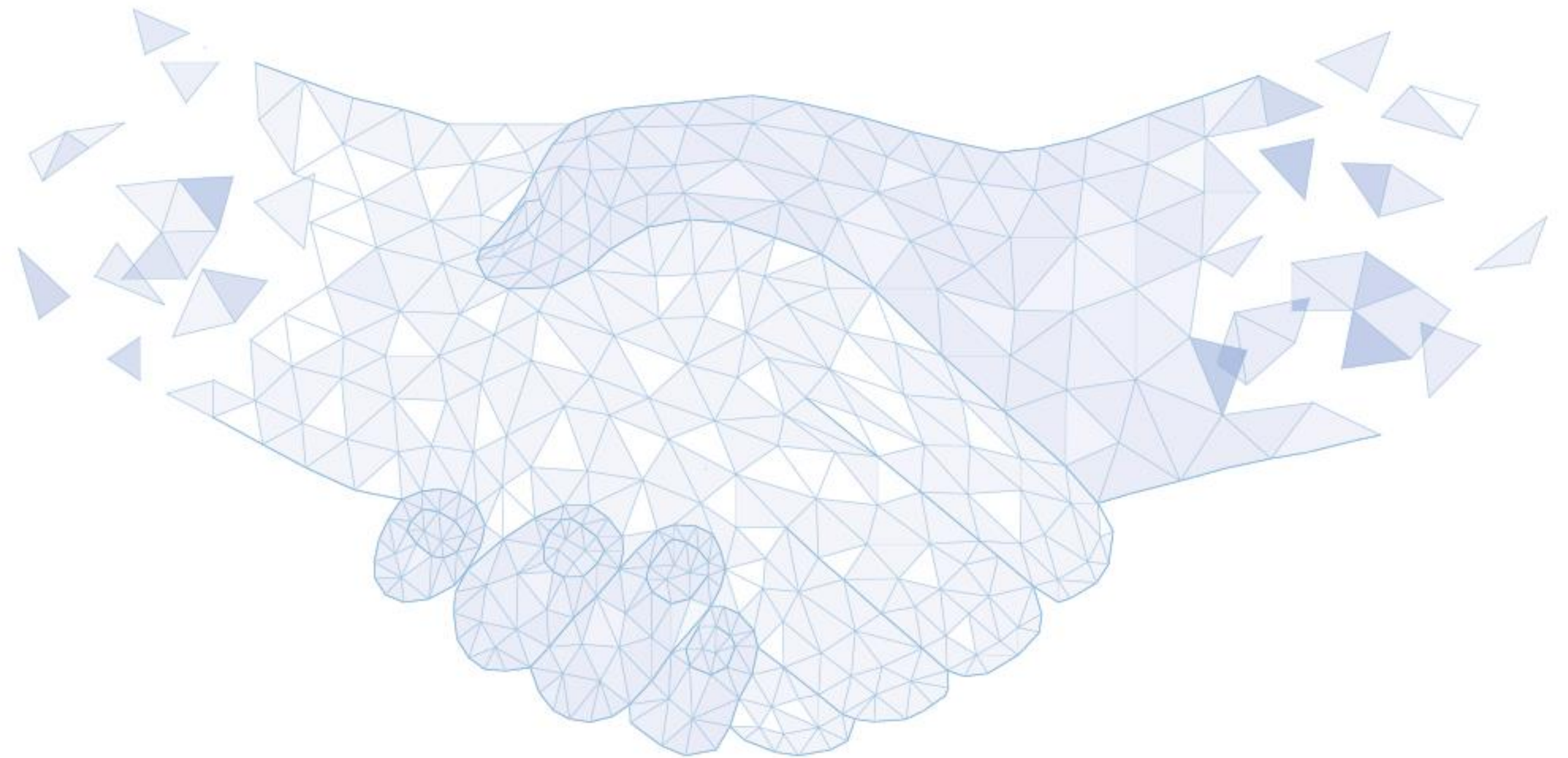


Third-Party Risk Management

Demonstrating a commitment to vulnerability assessment and proactive security measures enhances customer trust and helps maintain a positive reputation in the marketplace.

Vulnerability Assessment (VA)

- KEY CAPABILITIES
- **VA PROCESSING**
- REPORT & COMPARISON



■ Compliance Requirement Fulfillment:

Simple and fast self-assessment to determine compliance with security inspection requirements of cybersecurity and regulatory agencies.

■ Enhanced Security Level:

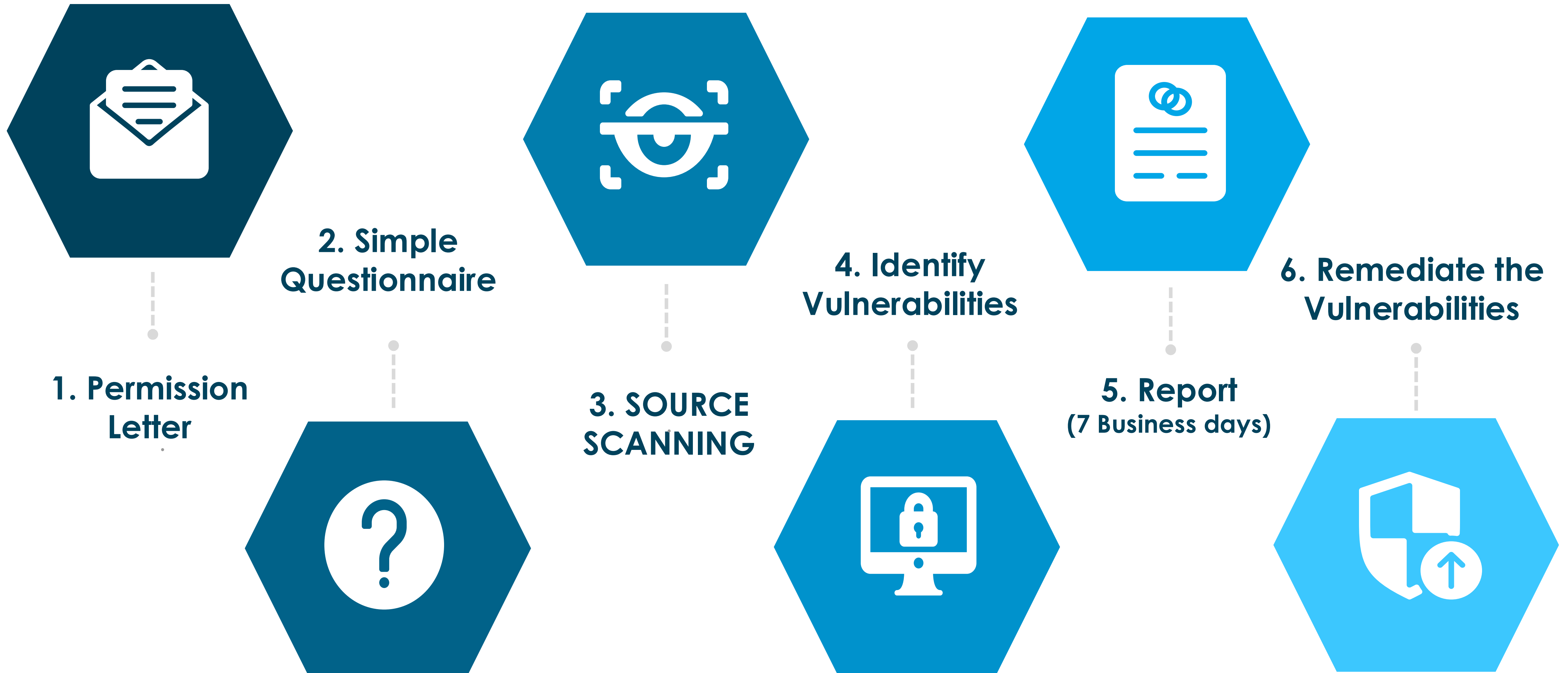
Self-testing and self-inspection of security vulnerabilities to improve the level of security operations and maintenance management and enhance user security reinforcement capabilities.

■ Improved Operational Efficiency:

Formulate professional and intuitive vulnerability scanning reports based on the scan results. Classify identified security vulnerabilities and provide remediation suggestions.

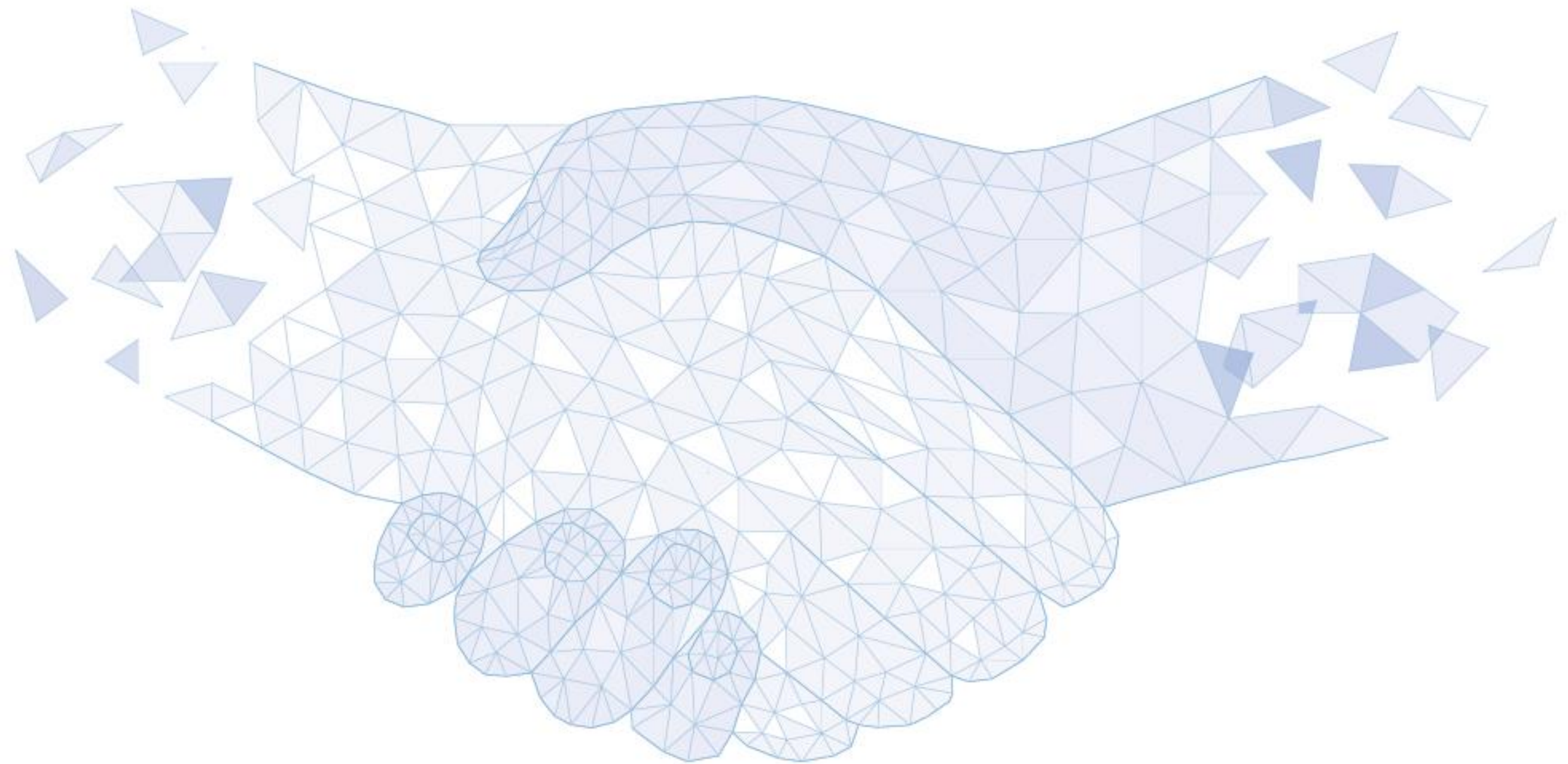






Vulnerability Assessment (VA)

- KEY CAPABILITIES
- VA PROCESSING
- **REPORT & COMPARISON**



GOIP VA Scanning	FREE	PAID
SOURCE SCANNING	Maximum 30 Minutes	Full-System Scan
Vulnerability Remediation Recommendations	Show 1 Only	Full
Source Analysis Report	Simplified Report	Comprehensive Report
Professional Report	Not Included	Full List of Report
Expert-Advised Remediation	Not Included	Included



Date: 28/9/2023

Comprehensive Report

Scan Informations

Target	Scan Type	Start Time	Scan Duration	Requests	Average Response Time	Maximum Response Time
http://*****	Full Scan	****, 2023, 11:18:08 AMGMT+8	30 minutes	18088	146ms	723ms

Threat Level 3

One or more high-severity type vulnerabilities have been discovered by the scanner.

Severity	Vulnerabilities	Instances
High	2	3
Medium	4	6
Low	3	3
Informational	5	5
Total	14	17

3 Cross site scripting

Instances: 1

High Severity

6 Basic authentication over HTTP

Instances: 1

Medium Severity

3 Clickjacking: X-Frame-Options header

Instances: 1

Low Severity

5 Access-Control-Allow-Origin header with wildcard (*) value

Instances: 1

Informational

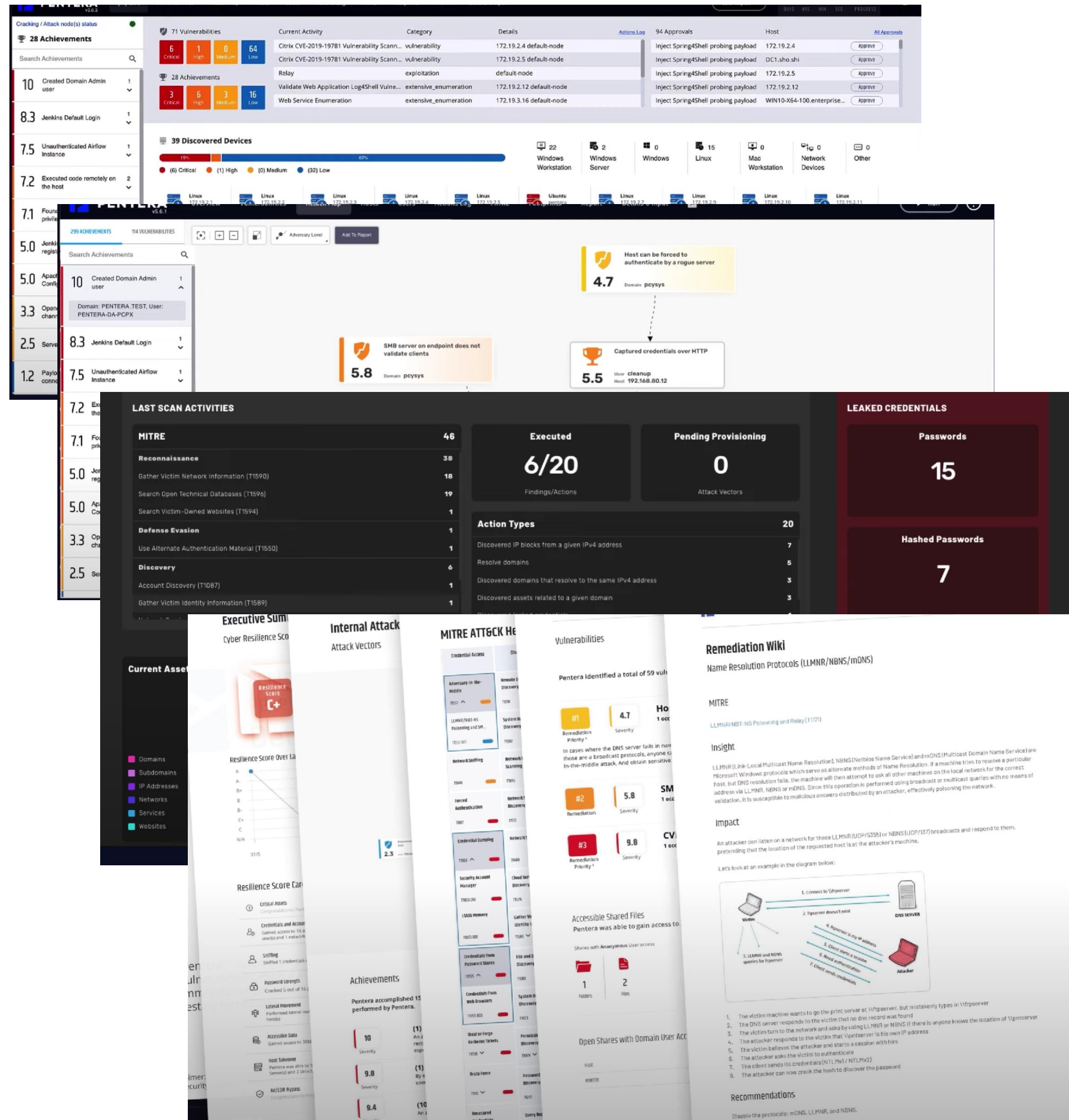
END

Unit 2508, 25/F, Nanyang Plaza 57 Hung to Road, Kwun Tong, HK | Tel: (852) 2138 9388 | info@goipaula.com

EDGENETIC Native Protection Compliance



- 01 PCISS- Payment Card Industry Data Security Standard
- 02 HIPAA- Health and Insurance Portability and Accountability Act
- 03 Privacy
- 04 ISO27001 / 27002
- 05 Cyber Security Certificate in SG IMDA



Customer Challenge

- Data Breaches
- Cost
- Data Compliance
- Lack of Security Expertise
- Data Silos

GOIP Group Benefits

- Protection from data breaches
- Use GOIP security information and event management (SIEM) solution
- Compliance with data protection laws and regulations
- Reduced risk of financial losses

Customer Challenge

- Cost
- Complexity
- Integration
- False positives
- Lack of skilled staff

GOIP Group Benefits

- Reduced costs
- Improved compliance
- Reduced risk of data breaches and other security incidents
- Competitive advantage
- Improved productivity

Threat Level 1
One or more low-severity type vulnerabilities have been discovered by the scanner.

Activity (Completed)

- Start URL changed (initial request to https://complusam.com/ was redirected to https://complusam.com/) Oct 7, 2023, 10:01:35 AM
- Scanning complusam.com using v23.7.230728157 Oct 7, 2023, 10:01:35 AM
- Antivirus not found Oct 7, 2023, 10:01:35 AM
- Scanning of complusam.com completed Oct 7, 2023, 10:06:02 AM

Scan Duration	Requests	Average Response Time	Paths Identified
4m 26s	7,238	47ms	15

Target Information

Address	complusam.com
Server	DPS/2.0.0-beta+sha-f6169cc
Operating System	Unknown
Identified Technologies	
Responsive	Yes

Latest Alerts

- Cookies with missing, inconsistent or contradictory properties Oct 7, 2023, 10:03:02 AM
- Cookies without HttpOnly flag set Oct 7, 2023, 10:03:02 AM
- Clickjacking: X-Frame-Options header Oct 7, 2023, 10:03:01 AM
- Permissions-Policy header not implemented Oct 7, 2023, 10:03:01 AM
- HTTP Strict Transport Security (HSTS) not implemented Oct 7, 2023, 10:03:01 AM

Discovered Hosts (12)

- https://www.complusam.com [Create Target](#)
- https://img1.wsimg.com [Create Target](#)
- https://www.linkedin.com [Create Target](#)
- http://complusam.com [Create Target](#)
- https://contact.apps-api.instantpage.secureserver.net [Create Target](#)

Severity	Vulnerability	URL	Parameter	Status	Confidence %
Low	Clickjacking: X-Frame-Options header	https://complusam.com/		Open	95
Low	Cookies with missing, inconsistent or contradictory properties	https://complusam.com/		Open	100
Low	Cookies without HttpOnly flag set	https://complusam.com/		Open	100
Low	HTTP Strict Transport Security (HSTS) not implemented	https://complusam.com/		Open	95
Informational	Content Security Policy Misconfiguration	https://complusam.com/		Open	100
Informational	Content Security Policy Misconfiguration	https://complusam.com/		Open	100
Informational	Email addresses	https://complusam.com/		Open	95
Informational	Outdated JavaScript libraries	https://complusam.com/		Open	95
Informational	Outdated JavaScript libraries	https://complusam.com/		Open	95
Informational	Permissions-Policy header not implemented	https://complusam.com/		Open	95

The screenshot displays a security scanner interface with the following components:

- Scan Summary:** Shows 0 Critical, High, and Medium vulnerabilities, and 1 Low vulnerability. It includes a donut chart for 'Top 5 Operating Systems Detected During Scan' and a 'Scan Durations' section with three 00:07:54 entries.
- Scan Details:** Lists scan name, plugin set, CVSS score, and scan template.
- Vulnerabilities Table:** A table with columns for Severity, CVSS, VPR, Name, Family, and Count. It lists various plugins like Nessus SYN scanner, CPE, Device Type, etc.
- Plugin Families Table:** A table with columns for Status, Plugin Family, Locked, and Total. It lists various security checks like AXI Local Security Checks, Alma Linux Local Security Checks, etc.
- Scan Details Panel:** Shows policy, status, severity base, scanner, start/end times, and elapsed time.
- Vulnerabilities Legend:** A small donut chart with a legend for Critical, High, Medium, Low, and Info.

Customer Challenge

- Lack of visibility
- Manual processes
- Integration challenges
- Reporting challenges
- Keeping up with changes

GOIP Group Benefits

- Reduced risk of penalties and fines
- Improved reputation
- Competitive advantage
- Improved productivity

EDGENETIC Native Protection Penetration Test (Pen Test)



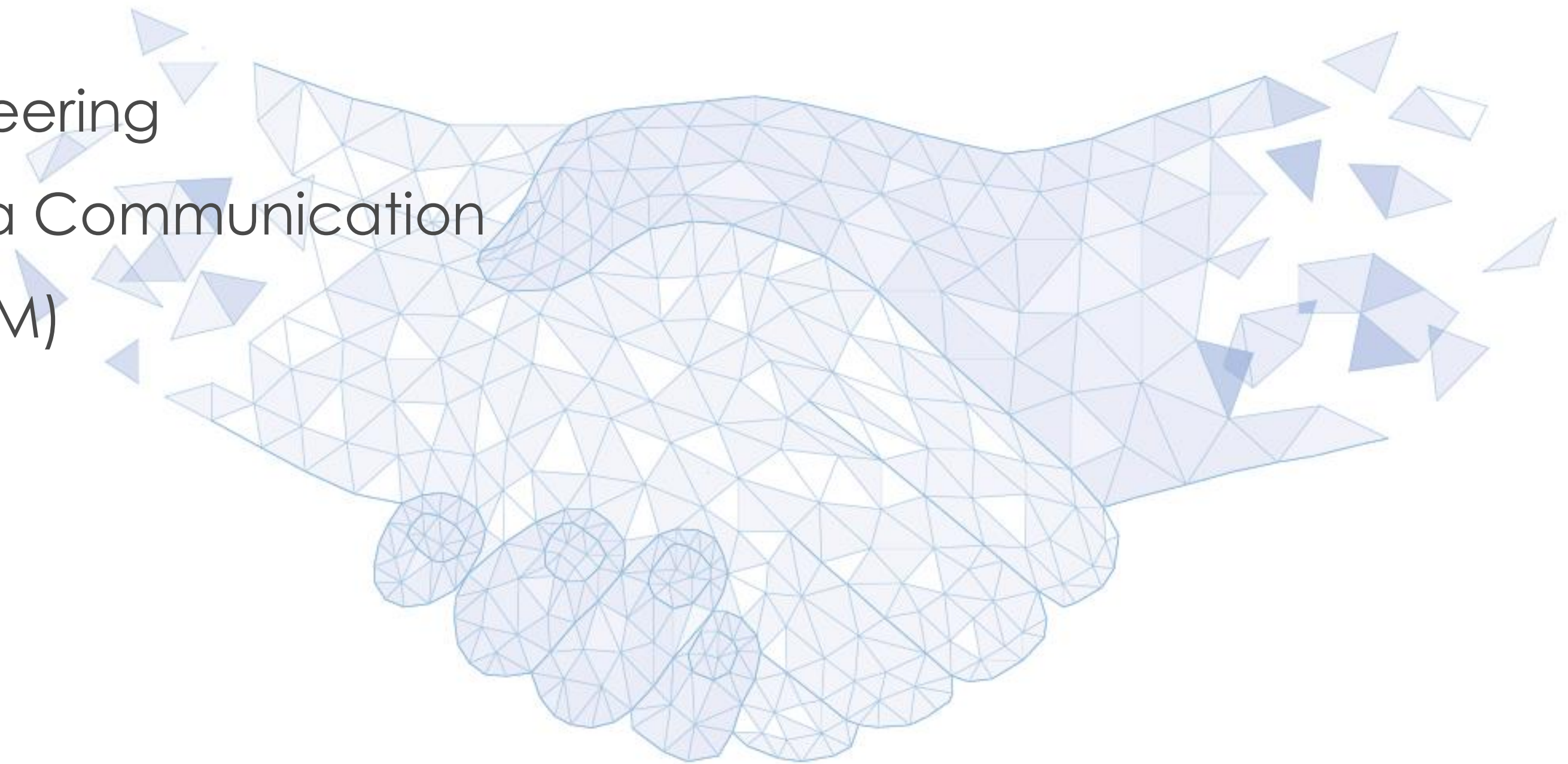
EDGENETIC Native Protection Penetration Test (Pen Test)

- 
- Security and Risk Management
 - Cybersecurity Asset Management
 - Cybersecurity Architecture and Engineering
 - Secure network Transmission and data
 - Communication Identify and Access Management (IAM)
 - Security Data Assessment and Testing
 - Backup and Disaster Recovery (BDR)
 - Data Security Operation Other

Penetration Test (Pen Test)

■ Security and Risk Management

- Asset Management
- Cybersecurity Architecture and Engineering
- Secure Network Transmission and Data Communication
- Identify and Access Management (IAM)
- Security Data Assessment and Testing
- BACKUP and DISASTER RECOVERY
- Data Security Operation
- Other



<1> Security and Risk Management

<1.1> Evaluate and apply security government principles

- Objectives

1. To ensure your policies and procedures keeps your organization up to date with regulations in law and industry best practice (HK/China)
2. Review any other relevant policies, regulations and compliance are mandatory complied (HK/China)

- Our team shall

- Cooperate with registered auditor and legal representative to review the contents in each lines with current documents, and ensure that are satisfied the compliances and regulation in law between Hong Kong and China
- Report the findings and share our recommendations for management review in scheduled meeting
- Add and follow the task with relevant department until completed at the end.
- Schedule the regular meeting with management board if necessarily.

- Other service shall include:

- To compile Personal Protection law and DCMM standard in China, our additional cost may incur :
- Language translation (Chi <> Eng)
- Documents (It has to be notarized or certified and recognized by China Government)
- Shipping
- More communications among different parties
- Searching any specialist to support any data clarification if necessarily.

Product should meet a certain consumer demand, or it should be so compelling that consumers believe they need it.

<1> Security and Risk Management

<1.1.1> Alignment of Alignment of the security function to business strategy, goals, mission and objectives

- Our team shall
 - Require our Chief Information Security Officer, CISO to ensure the alignment of security functions and business within your specific role in organization, and effectively to communicate the importance of data security to all level of organization.
 - Propose appropriate security measures under budgets while developing new policies, procedures, and guidelines with her concerns.
 - Prepare the Questionnaire and interview with relevant people at different level of organization, then collect the data for designing the measures and guidelines.

• <1.1.2> Establish Security control Frameworks

- Our team shall
 - Establish security control frameworks for managing risk and reducing vulnerabilities
 - Contain a series of documented processes that define policies and procedures around the implementation and ongoing management of information security controls.
 - Security Control Frameworks consist:
 - To define and prioritize the tasks required to manage organize security
 - To help for preparing compliance and other IT audits, such as ISO 38505, ISO 8000 and DCMM (China) Standard

Product should meet a certain consumer demand, or it should be so compelling that consumers believe they need it.

<1> SECURITY AND RISK MANAGEMENT



<1.2> Determine other compliance and requirements

- Our team shall
 - Summarize and finalize all relevant standard, compliance and regulations in terms of data security across China and Hong Kong, such as
 - <Item 1.2.1> ISO38505 / ISO 8000
 - <Item 1.2.4> DCMM (China)
 - Our CN Team shall review and verified your supporting documents through pre-evaluation. if failure, our team may advise to alter the document formats and language until it's pass.
 - <Item 1.2.2> Personal Data Privacy (Hong Kong)
 - <Item 1.2.3.1 > Personal Protection Law (China)
 - Besides, it might be considered as :
 - The Guidance on Personal Data Protection in Cross-Boarder Data Transfer
 - The cross-border transfer outside mainland China (data export)
- Communicate decision-marker to consider whether these relevant requirement compliance added into compliance checklist, for example:
 - Communication by email / meeting / Interview
 - Establish Risk Acceptance and tolerable period of disruption (MTPD)
 - Business Impact Assessment
 - Specialist information security advice

POLICY: ISO 27001:2013
Responsible: AIC
Date: 01/01/2018

REQUIREMENT	Current Requirements (Company/Proc./Norm./Sector)	Gap Description	Action Required	Priority	Start Date	Due Date	Priority	Complete	Status
SECURITY POLICY									
2.2.3	Information security	Yes	ACQ	Yes	Yes	Yes	High	Yes	Yes
2.2.2	Review and revision	Yes	None	Yes	Yes	Yes	High	Yes	Yes
2.2.3	ISMS	Yes	Yes	Yes	Yes	Yes	High	Yes	Yes
2.2.3	ISMS	Yes	Yes	Yes	Yes	Yes	High	Yes	Yes
ASSET CLASSIFICATION AND CONTROL									
2.2.2	Inventory of assets	Yes	Yes	Yes	Yes	Yes	High	Yes	Yes
2.2.2	Information labeling	Yes	Yes	Yes	Yes	Yes	High	Yes	Yes
2.2.2	Information labeling	Yes	Yes	Yes	Yes	Yes	High	Yes	Yes
PHYSICAL AND ENVIRONMENTAL SECURITY									
2.2.3	Physical security perimeter	Yes	None	Yes	Yes	Yes	High	Yes	Yes
2.2.3	Physical security perimeter	Yes	None	Yes	Yes	Yes	High	Yes	Yes
2.2.3	Physical security perimeter	Yes	None	Yes	Yes	Yes	High	Yes	Yes
COMMUNICATIONS AND OPERATIONS MANAGEMENT									
2.2.3	Physical security perimeter	Yes	None	Yes	Yes	Yes	High	Yes	Yes
2.2.3	Physical security perimeter	Yes	None	Yes	Yes	Yes	High	Yes	Yes
2.2.3	Physical security perimeter	Yes	None	Yes	Yes	Yes	High	Yes	Yes

Table 1. Results of security gap analysis for 21 agencies
Red = ineffective, Orange = partially effective, Green = effective

Agency	Effective	Partially Effective	Ineffective
Agency 1	15	5	1
Agency 2	10	10	1
Agency 3	12	8	1
Agency 4	14	6	1
Agency 5	11	9	1

Issue	Impact	Resolution
Information security policy not reviewed	High	Review and update the policy and ensure it is aligned with current requirements.
Information labeling not implemented	Medium	Implement information labeling across all assets and ensure staff are trained on the process.
Physical security perimeter not defined	High	Define the physical security perimeter and implement appropriate controls.

Product should meet a certain consumer demand, or it should be so compelling that consumers believe they need it.

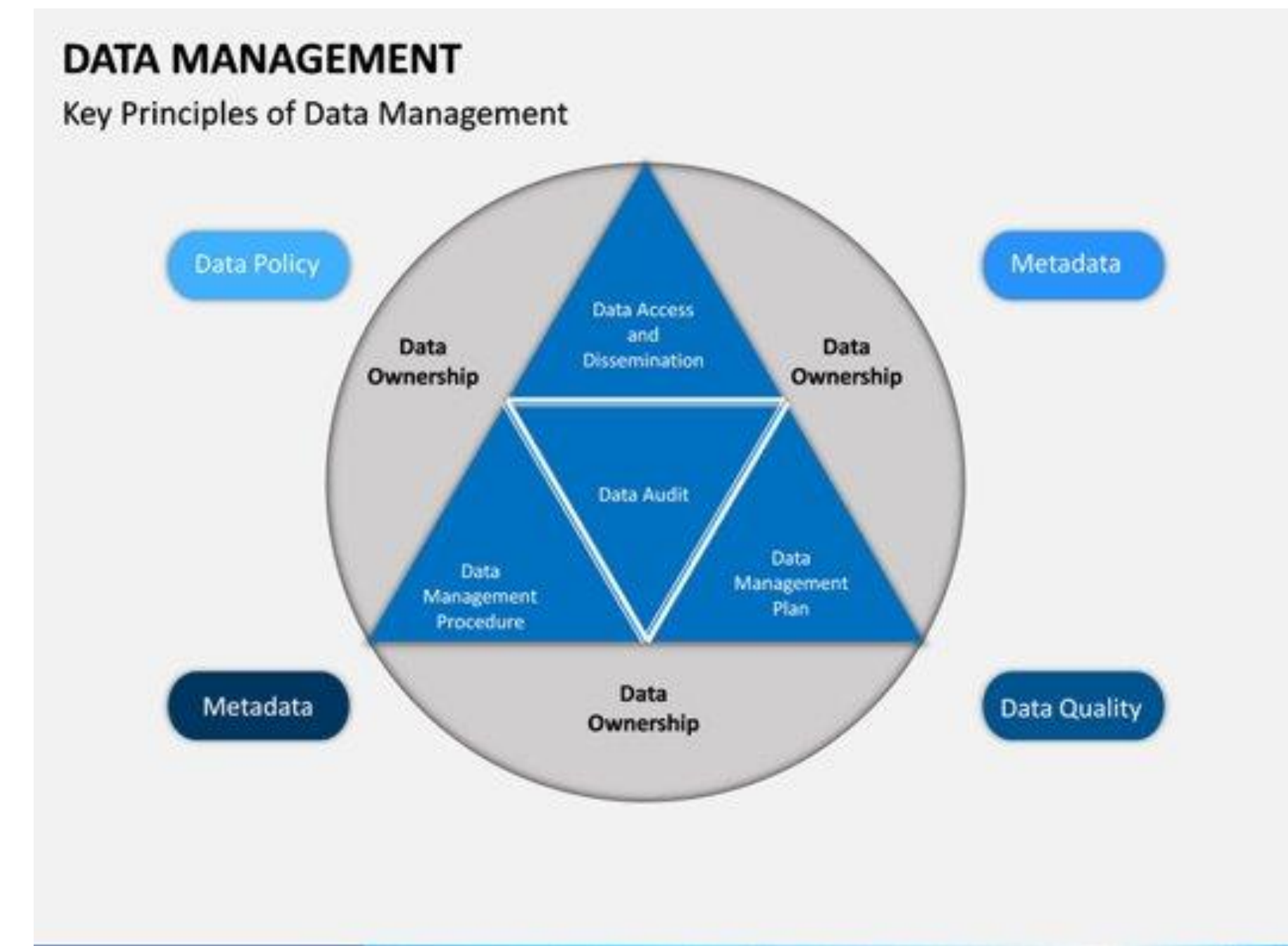
<1> SECURITY AND RISK MANAGEMENT

<1.3> Develop, Document and implementation

(Data Security Policy / Standards / Procedures / Guidelines)

In reference by industry standards, security policies and legal principles across Hong Kong and China, we shall >>> Set out these specific set of principles and process relating to data governance, there are:

- <Item 1.3.1> Data Management Manuel with frameworks policies and guidelines
 - Data Policy development
 - Data Ownership
 - Metadata Compilation
 - Data Lifecycle Control
 - Data Quality; and Data Access and Dissemination etc.
- <Item 1.3.2> Data Cross Boarder Transfer Management Guideline
 - Cross Data Policy development
 - Cross Data Ownership
 - Metadata Compilation
 - Data Lifecycle Control
 - Data Quality; and Data Access and Dissemination etc.



<1> SECURITY AND RISK MANAGEMENT

<1.4> Boost Security Awareness

(Training / Model Appropriate Behavior/ POP-UP Alerts tool etc.)

• Our team shall



GDPR: THE DATA PROTECTION OFFICER (DPO)

DPO: mandatory in 3 cases

- 01 PUBLIC AUTHORITY**
Processing of personal data done by public authority, except for courts or independent judicial authorities when acting in their judicial capacity.
- 02 LARGE SCALE REGULAR MONITORING**
Processing by a controller whose core activities consist of processing operations that require regular and systematic monitoring of the data subjects on a large scale.
- 03 LARGE SCALE SPECIAL DATA CATEGORIES**
Core activities of the controller or the processor consist of processing on a large scale of special categories of personal data and data relating to criminal convictions and offences.

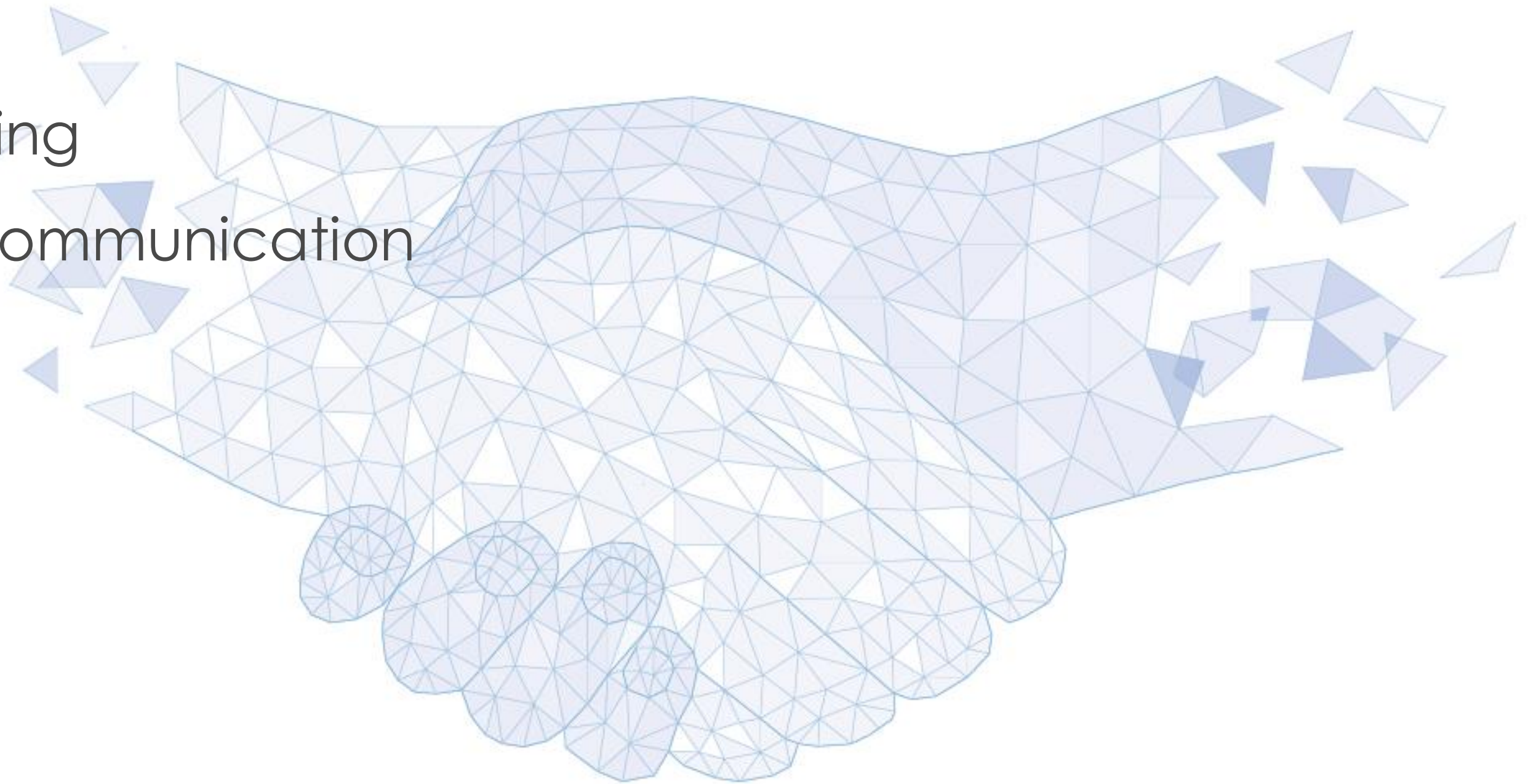
DPO: who/what

- GDPR/PRIVACY EXPERT
- EMPLOYEE/EXTERNAL
- MONITOR COMPLIANCE
- ASSIST WITH GDPR
- INDEPENDENT
- REPORT TO MGMT
- SPOC/REGISTERED
- SECRECY
- CONFIDENTIALITY

- <Item 1.4.1> Present latest Data threat protection technique with legal awareness in training, including
 - Training material and certified tutor
 - Invite speakers to presentation
 - Activities
 - Assist to set up the **POP-UP** awareness tool for reminder in Help desk
 - Remarks : the cost is considered the number of employee engagement; the minimum Charge is \$300K(HK\$)
- <Item 1.4.2> Understanding requirement for investigations either by legal authorities or Auditors
 - Providing training material
 - Invite guest Tutor : legal practitioner / the Specialist of data security/ accredited auditor
 - Invite speakers to presentation
 - Set-up and plan education activities after training

Penetration Test (Pen Test)

- Security and Risk Management
- **Asset Management**
- Cybersecurity Architecture and Engineering
- Secure Network Transmission and Data Communication
- Identify and Access Management (IAM)
- Security Data Assessment and Testing
- BACKUP and DISASTER RECOVERY
- Data Security Operation
- Other



- **Our team shall**

- <Item 2.1 > Collecting, Identify and classify data information, scan and categorize assets in inventory automatically.
 - Require Data Inspection team to use the tools for data scanning and integration during office hour.
 - Use "source scanning" tool to collect data information from different sources and creating a single, unique, dataset for visualization and analysis.
 - Using a platform that automatically integrate and optimize these data in storage.
 - Remarks : The cost is subjected to the total number of IP or device at the end points, then will choose the greater number in total.
- <Item 2.2 > provide " Manage Data Life Cycle (DLM) Guidelines"
 - Review the result from the summary of compliance and business continuity
 - Set-up the policy-based approach to oversee the flow of data information from data entry to data destruction.
 - Allocating experienced people to coordinate the tasks and communications among parties in organization.

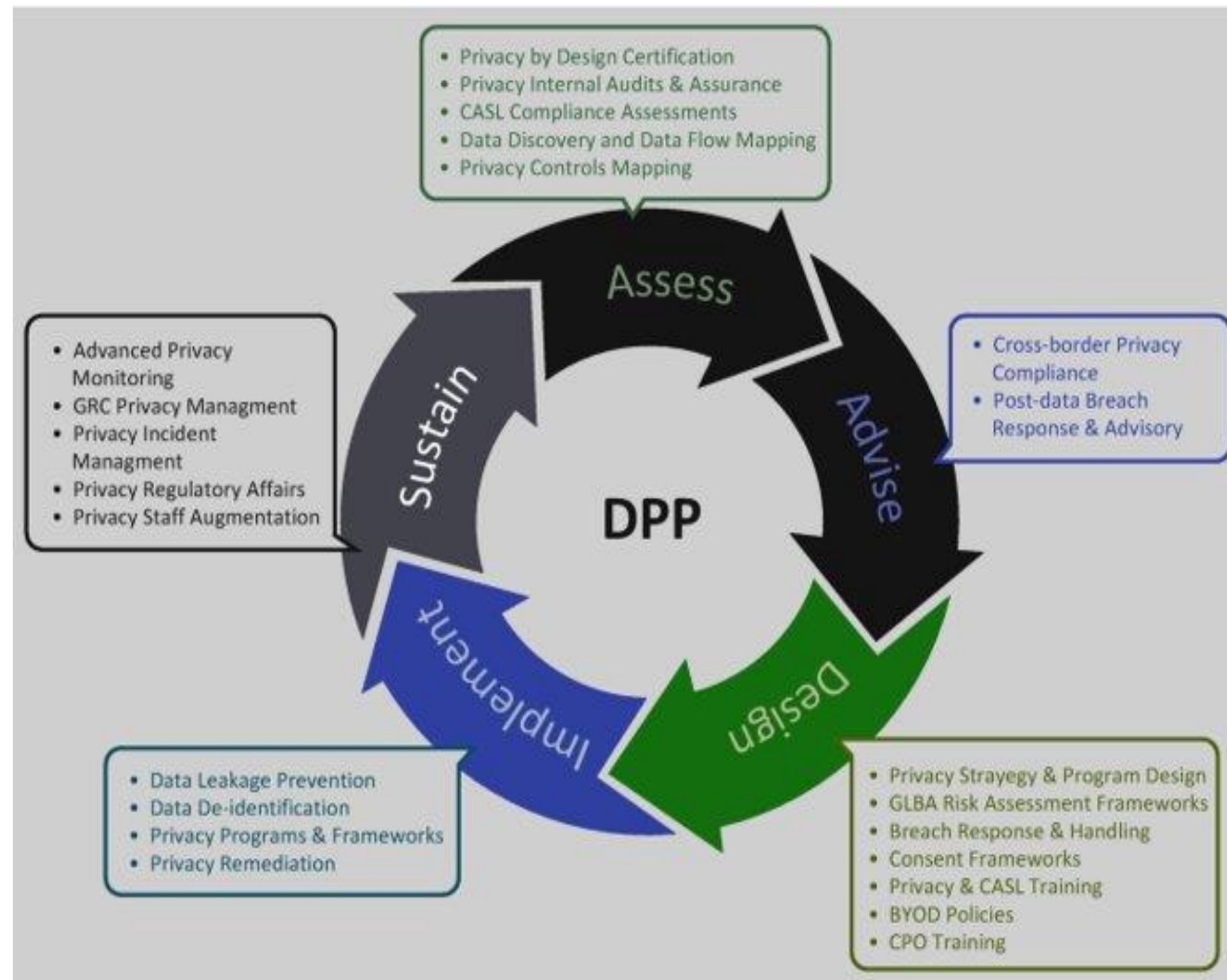
Product should meet a certain consumer demand, or it should be so compelling that consumers believe they need it.

- Our team shall
 - <Item 2.3 > Data Assessment : the states of data / Scoping and tailoring / standard selection
 - Objectives: Managed all technology assets from purchase through disposition, both physical and virtual, to ensure secured use, regardless of the asset's location.
 - Completeness check
 - Our audit identified an error in the calculation of the PI re"Percentage of planned of responsive repairs". Void repairs were treated as planned but they should responsive. The PI was recalculated and was then assessed as being fairly stated
 - Data quality spot checks
 - carried out an in-depth review, using a series of audit tests, of a sample of PIs to determine whether arrangements to secure data quality are delivering accurate, timely and accessible information

File ref	Finding	Recommendation	Priority	Response	Target date	Responsible Officer
R17 EX.82 K.7.PS	The indicator was not correctly stated as it was based on incomplete data (ie some quarterly returns were not loaded onto SPOCC) and data relating to the wrong time period (ie 2006/07).	Recalculate indicator based on complete data and correct time period. Also, put in place procedures to ensure that all returns are loaded to SPOCC and the associated data included in the calculated PI.	High	Revised report provided 12 October 2006, giving indicator of 66.85 per cent.	2006/07	Tracey Chapman, Supporting People Co-ordinator
Average relet times						
R18 EX.66 K.8.PS	The original data provided for this indicator related to the wrong period and was therefore incorrect.	Revised indicator to be submitted using the correct time period.	High	Revised data provided. PI amended to 45.87.	2005/06	Clare Dowds, Letting Manager
R19 EX.76 K.8.PS	In a sample of 20 cases tested the void start dates were incorrect in all cases. 16 cases had the date the keys were handed in, instead of the day following per the HIP indicator instructions. 4 cases where the tenant had given notice to quit and the final day of the notice was used as the void start date instead of the day following receipt of the keys from the tenant.	The correct void start date should be used. The errors noted had a non material effect on the PI which was reported as fairly stated.	High	Our practices reflected new BVPI 212 (effective from 2006/07) in taking the void as end of tenancy. By using day key received which was routinely Monday, for the tenancy ending at midnight on Sunday we showed more accurately the time keys with us and available even if this meant additional void days.		Clare Dowds, Letting Manager
R20 EX.77 K.8.PS	The Council used the incorrect end of void date in cases where the tenant collected the keys after the tenancy date.	The correct end date must be used. ie the date the tenant collected the keys if it is later than the tenancy date. The errors noted had a non material effect on the PI which was reported as fairly stated.	High	Agreed Guidelines were issued during the period to advise that keys should not be issued later than start of tenancy, except in exceptional cases, at the request of the incoming tenant. These cases were very rare and guidance will be reissued to reiterate.	2006/07	Clare Dowds, Letting Manager

- Our team shall
 - <Item 2.3 > Data Assessment : the states of data / Scoping and tailoring / standard selection
 - Objectives: Managed all technology assets from purchase through disposition, both physical and virtual, to ensure secured use, regardless of the asset's location.
 - Completeness check
 - Our audit identified an error in the calculation of the PI re "Percentage of planned of responsive repairs". Void repairs were treated as planned but they should responsive. The PI was recalculated and was then assessed as being fairly stated
 - Data quality spot checks
 - carried out an in-depth review, using a series of audit tests, of a sample of PIs to determine whether arrangements to secure data quality are delivering accurate, timely and accessible information

File ref	Finding	Recommendation	Priority	Response	Target date	Responsible Officer
R17 EX.82 K.7.PS	The indicator was not correctly stated as it was based on incomplete data (ie some quarterly returns were not loaded onto SPOCC) and data relating to the wrong time period (ie 2006/07).	Recalculate indicator based on complete data and correct time period. Also, put in place procedures to ensure that all returns are loaded to SPOCC and the associated data included in the calculated PI.	High	Revised report provided 12 October 2006, giving indicator of 66.85 per cent.	2006/07	Tracey Chapman, Supporting People Co-ordinator
Average relet times						
R18 EX.66 K.8.PS	The original data provided for this indicator related to the wrong period and was therefore incorrect.	Revised indicator to be submitted using the correct time period.	High	Revised data provided. PI amended to 45.87.	2005/06	Clare Dowds, Letting Manager
R19 EX.76 K.8.PS	In a sample of 20 cases tested the void start dates were incorrect in all cases. 16 cases had the date the keys were handed in, instead of the day following per the HIP indicator instructions. 4 cases where the tenant had given notice to quit and the final day of the notice was used as the void start date instead of the day following receipt of the keys from the tenant.	The correct void start date should be used. The errors noted had a non material effect on the PI which was reported as fairly stated.	High	Our practices reflected new BVPI 212 (effective from 2006/07) in taking the void as end of tenancy. By using day key received which was routinely Monday, for the tenancy ending at midnight on Sunday we showed more accurately the time keys with us and available even if this meant additional void days.		Clare Dowds, Letting Manager
R20 EX.77 K.8.PS	The Council used the incorrect end of void date in cases where the tenant collected the keys after the tenancy date.	The correct end date must be used. ie the date the tenant collected the keys if it is later than the tenancy date. The errors noted had a non material effect on the PI which was reported as fairly stated.	High	Agreed Guidelines were issued during the period to advise that keys should not be issued later than start of tenancy, except in exceptional cases, at the request of the incoming tenant. These cases were very rare and guidance will be reissued to reiterate.	2006/07	Clare Dowds, Letting Manager



- Our team shall

<Item 2.4 >

Design and Establish Data Protection methods (eg. Data Loss Prevention, DLP, Digital Rights Management (DRM) and Identity and Asset Management (IAM) Completeness check

- i. Our plan is referred by “DPP work cycle” as shown on picture.
- ii. Remarks: The cost is subjected to the number of IP, the scale of data size with minimum charges 200K(HK\$) and the level of data protection

Penetration Test (Pen Test)

- Security and Risk Management
- Asset Management
- **Cybersecurity Architecture and Engineering**
- Secure Network Transmission and Data Communication
- Identify and Access Management (IAM)
- Security Data Assessment and Testing
- BACKUP and DISASTER RECOVERY
- Data Security Operation
- Other



<3> CYBERSECURITY ARCHITECTURE AND ENGINEERING

- Our team shall

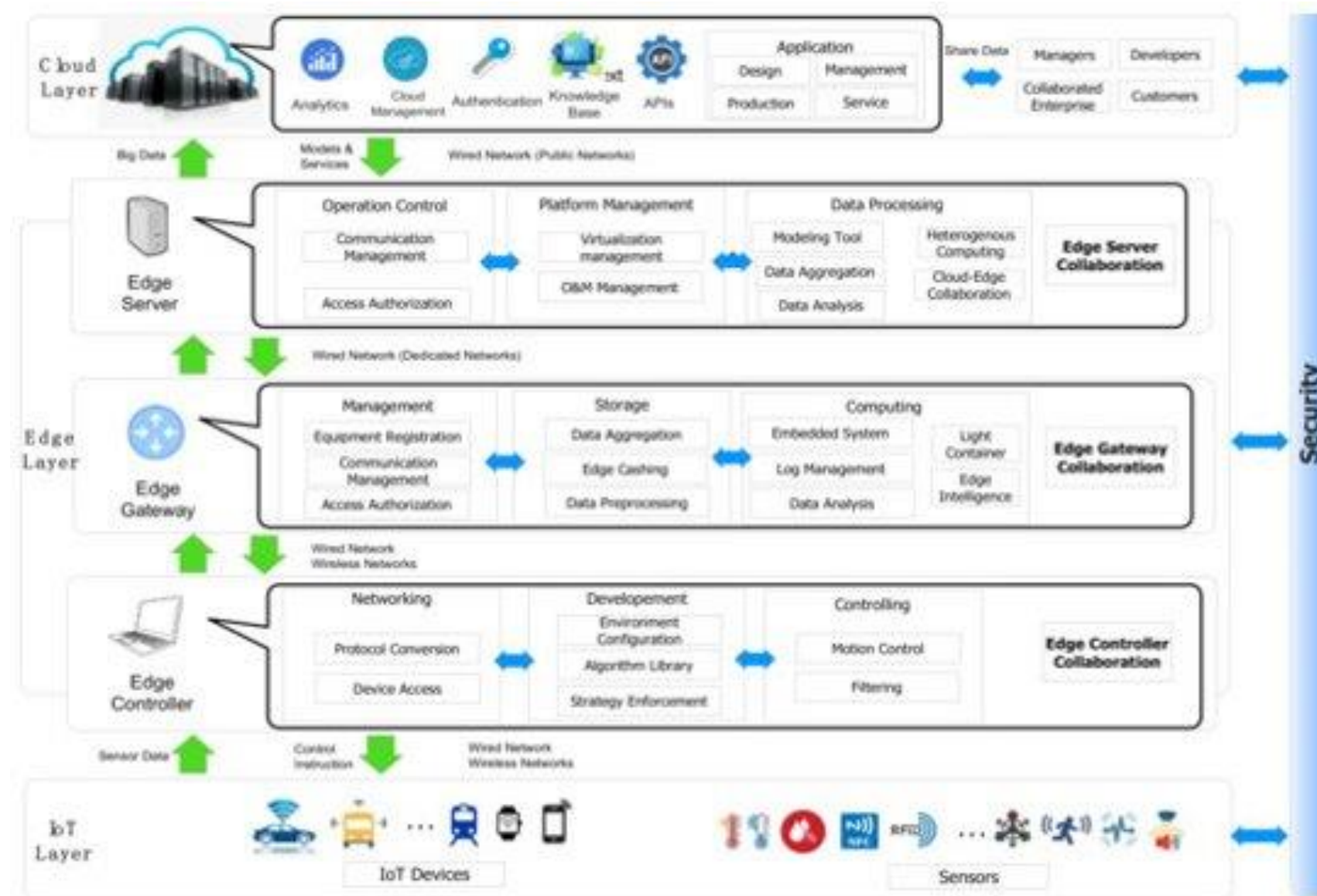
<Item 3.2 > Assess and mitigate the internal vulnerabilities of security architectures, designs and solutions elements

(Our assessment covered the device and system, such as Client-base systems / server-based systems / Satabase systems / Industrial Control Systems or Internet of Things, IOT etc.)

- By satisfying the data protection policies in China and Hong Kong, we choose CN government recognized platform so called “啟明星辰” and “Acunetix” for assistance.
- Require one CN and HK team to conduct this internal vulnerabilities assessment on site and consolidate two different results into one, also share our comments for improvement accordingly.



<3> CYBERSECURITY ARCHITECTURE AND ENGINEERING



- Our team shall

<Item 3.2 > Design site and Facility security controls eg. data evidence storage

- Require certified expertise to conduct site survey whether has any potential impacts on data storage and the result would be showed on the site inspection report.
- Design and plan the facility security control in view of data protection requirement, including access control, CCTV and Video Surveillance and Security integration and Growth Monitoring

- Our team shall

<Item 3.2 > Assess and mitigate the internal vulnerabilities of security architectures, designs and solutions elements

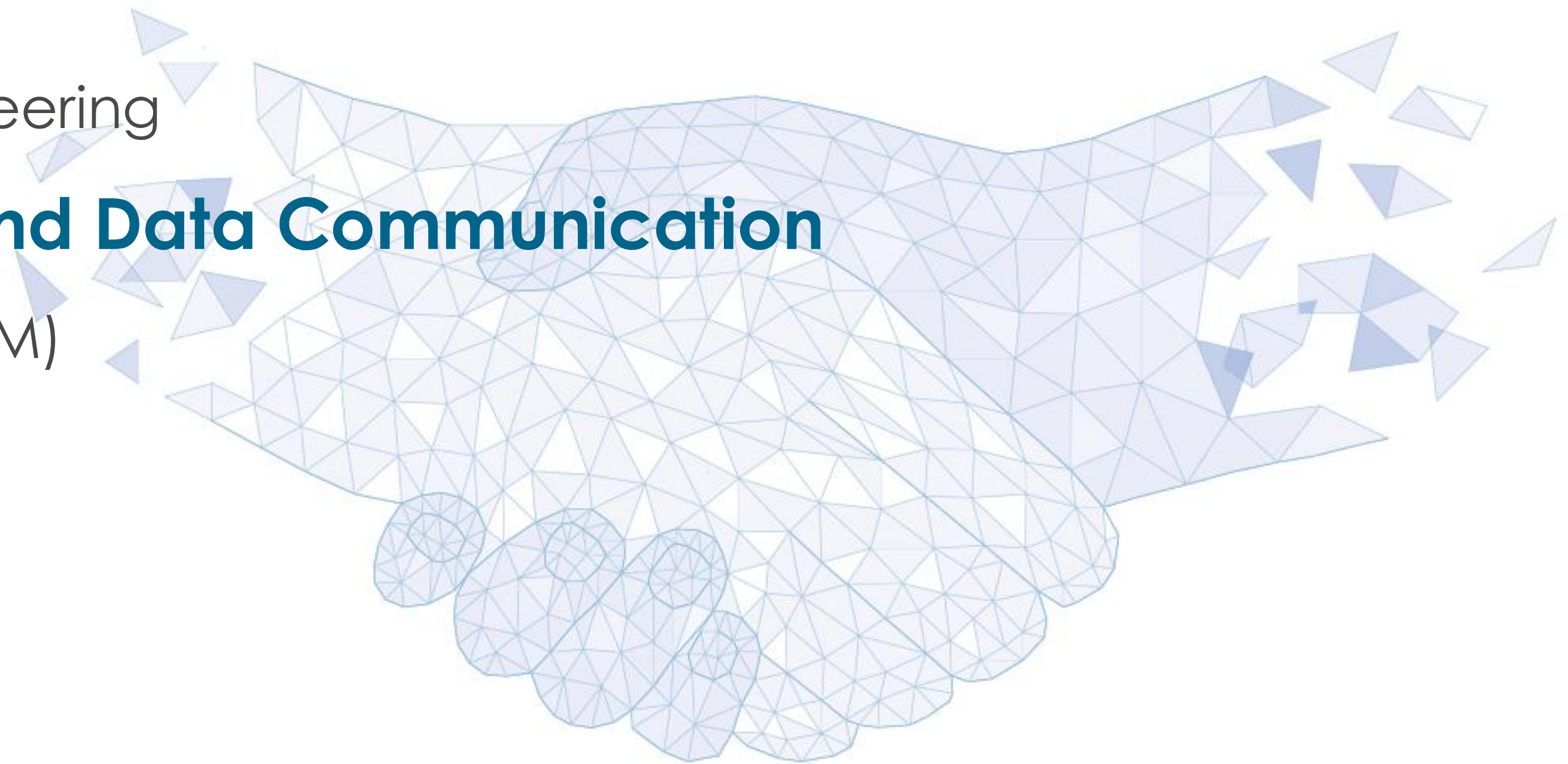
(Our assessment covered the device and system, such as Client-base systems / server-based systems / Satabase systems / Industrial Control Systems or Internet of Things, IOT etc.)

- By satisfying the data protection policies in China and Hong Kong, we choose CN government recognized platform so called “啟明星辰” and “Acunetix” for assistance.
- Require one CN and HK team to conduct this internal vulnerabilities assesment on site and consolidate two different results into one, also share our comments for improvement accordingly.



Penetration Test (Pen Test)

- Security and Risk Management
- Asset Management
- Cybersecurity Architecture and Engineering
- **Secure Network Transmission and Data Communication**
- Identify and Access Management (IAM)
- Security Data Assessment and Testing
- BACKUP and DISASTER RECOVERY
- Data Security Operation
- Other



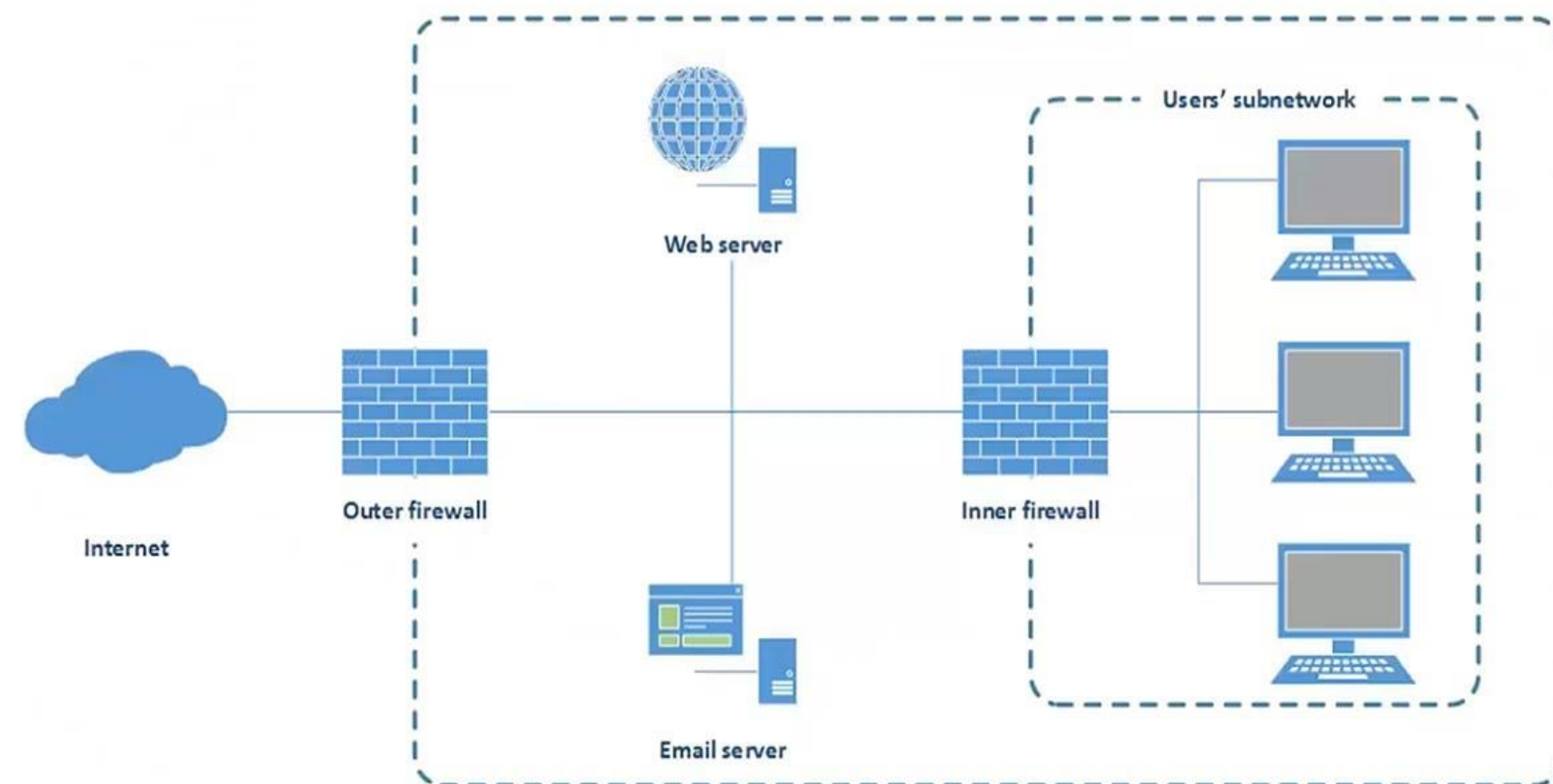
<4> SECURE NETWORK TRANSMISSION AND DATA COMMUNICATION

- Our team shall

<Item 4. 1> Check the network protocols, patching, systems and hardware, which are sufficient to guard your data transmission in the current physical network.

- Require the experienced network field engineer to perform the on-site inspection.
- Remarks : This service is covered the range of data originated hosting location only, otherwise, the cost shall be subjected to change by the total number of IP and devices.

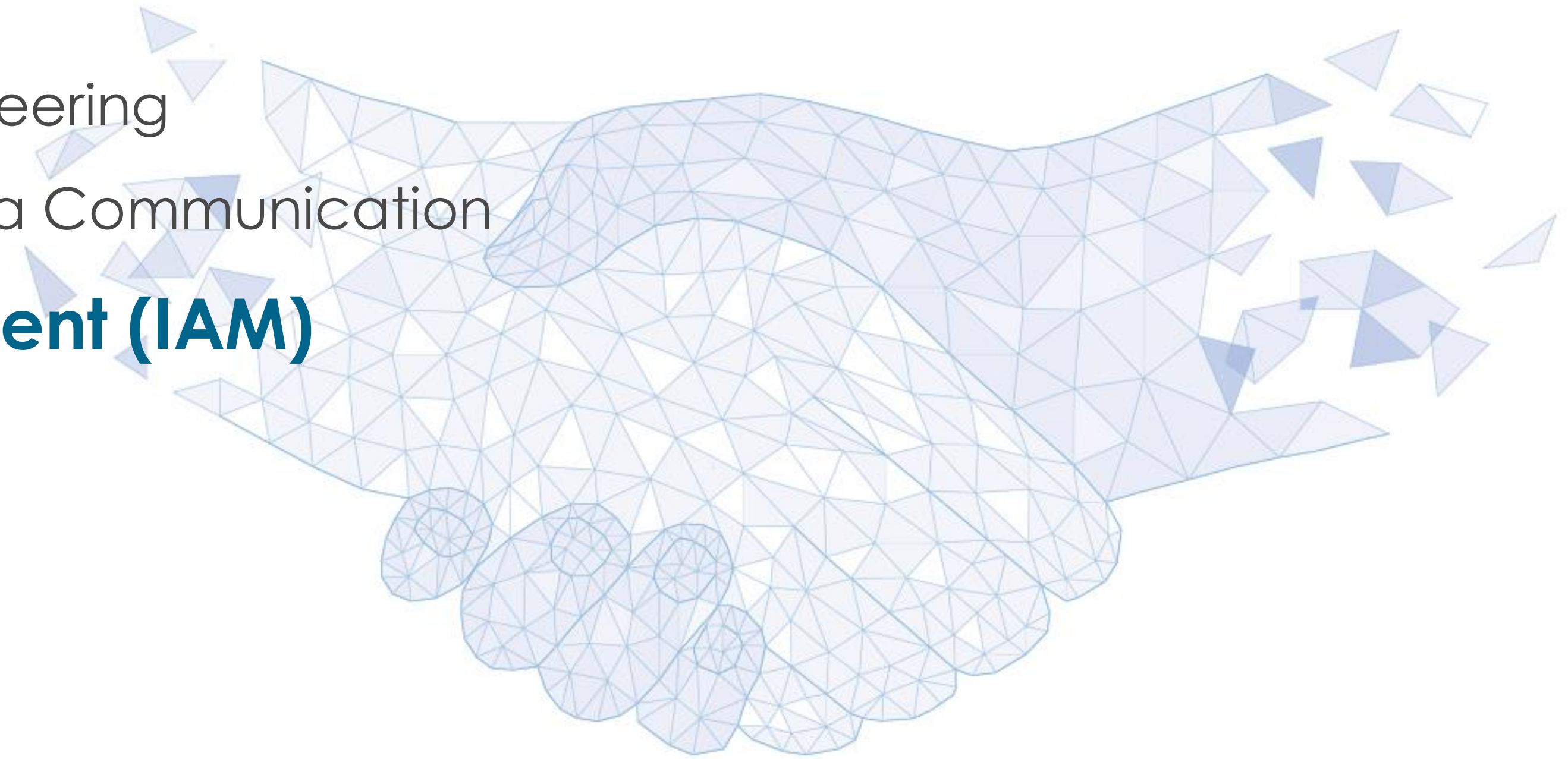
Multiple Network Security Perimeters



OSI Model Layers	Protocols	
Application Presentation Session	SMTP, FTP, DNS, WWW, HTTP, TELNET	Application Layer
Transport	TCP, UDP	Transport Layer
Network or Internet	ARP, RARP, IP, ICMP	Network Layer
Datalink Layer Physical Layer	Specific to the underlying media at hardware level.	Interface Layer

Penetration Test (Pen Test)

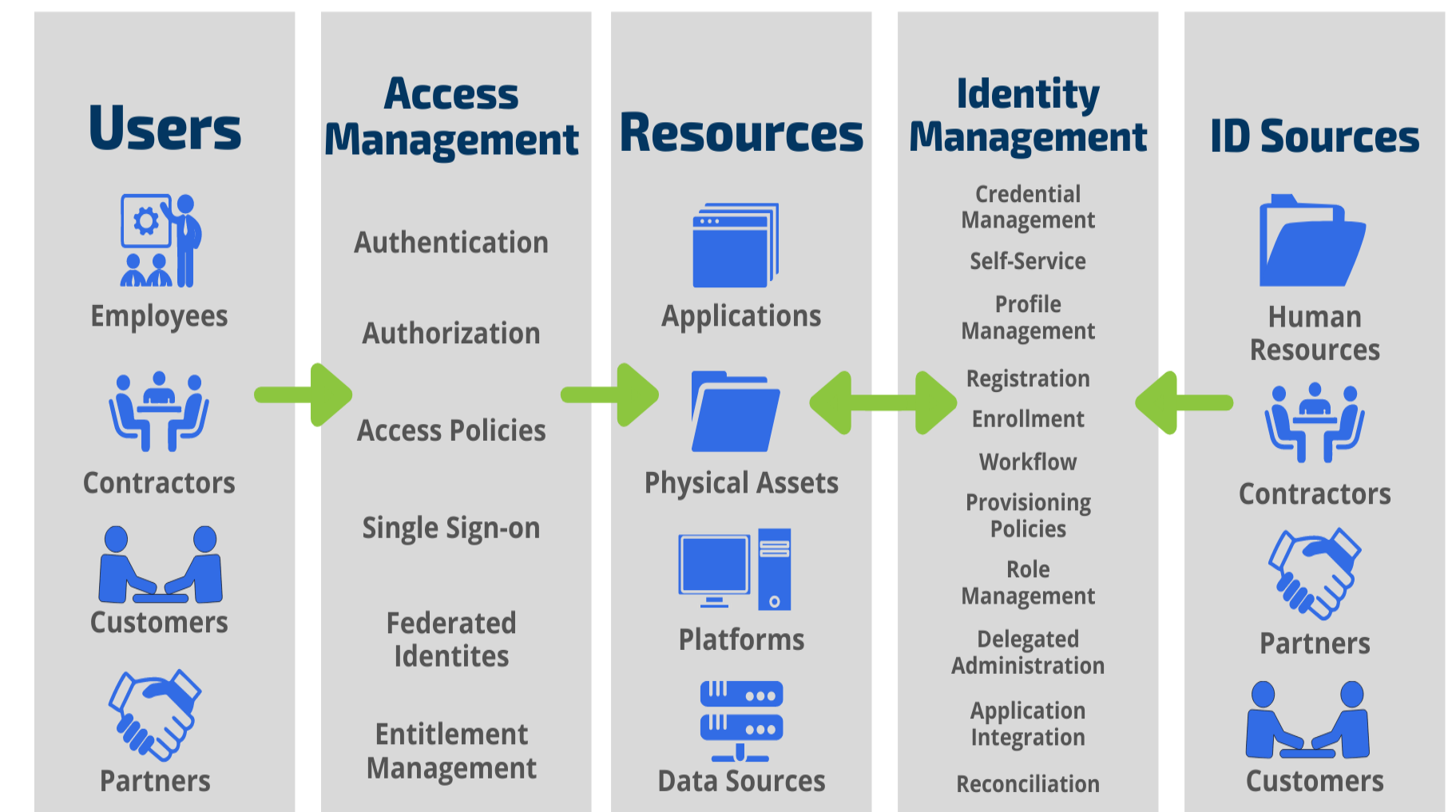
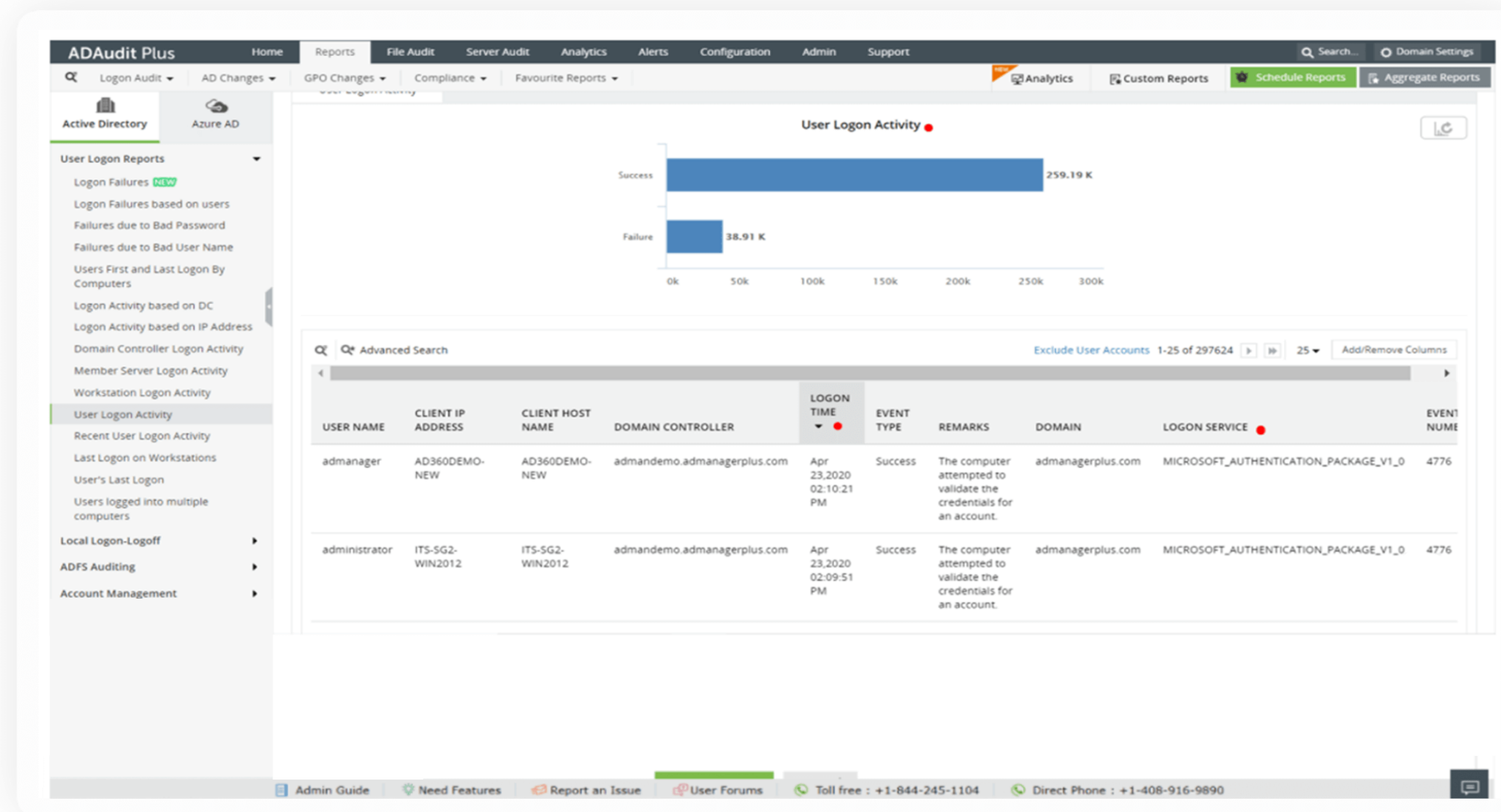
- Security and Risk Management
- Asset Management
- Cybersecurity Architecture and Engineering
- Secure Network Transmission and Data Communication
- **Identify and Access Management (IAM)**
- Security Data Assessment and Testing
- BACKUP and DISASTER RECOVERY
- Data Security Operation
- Other



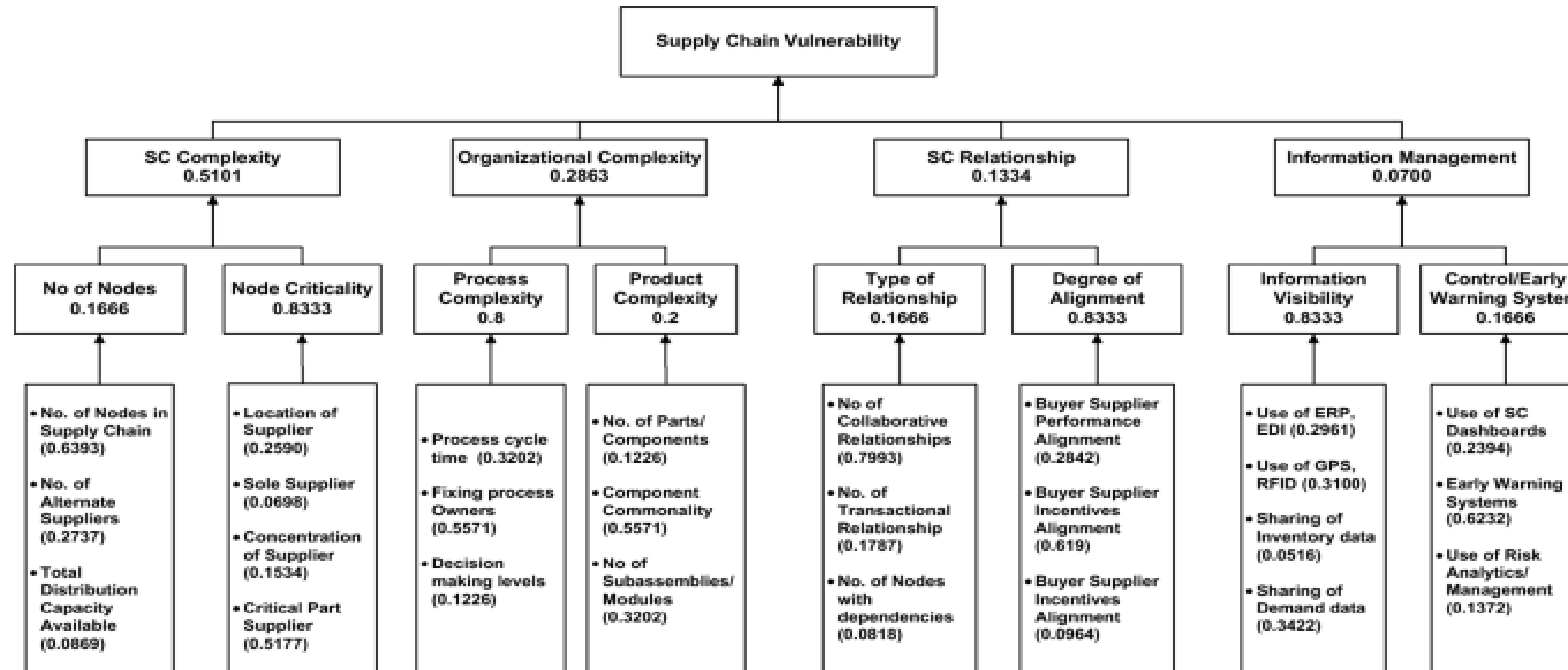
<5> IDENTIFY AND ACCESS MANAGEMENT (IAM)

- Our team shall

- <Item 5.1> To plan the management of authorization mechanism
 - Required security team to design and communicate our mechanism with specific team, then provide the plan how to perform the authorization in working progress.
- <Item 5.2> To implement the authentication system
 - To adopt the well-known platform of "ManagedEngine". It enables to centralize your user access from multiplied platform into one.
 - Required the data security team and system engineer to migrate the data from initial to the new platform, set-up the new policies and rules in configuration, or build-up the network connection etc.
 - The cost is changed subject to the number of users, hardware and circuit as required.



<6> SECURITY DATA ASSESSMENT AND TESTING



<Item 6.1> Design and validate Supply Chain Vulnerability assessment, test and audit strategies
(Focused on data communication with third parties of channels, suppliers and vendors etc.)

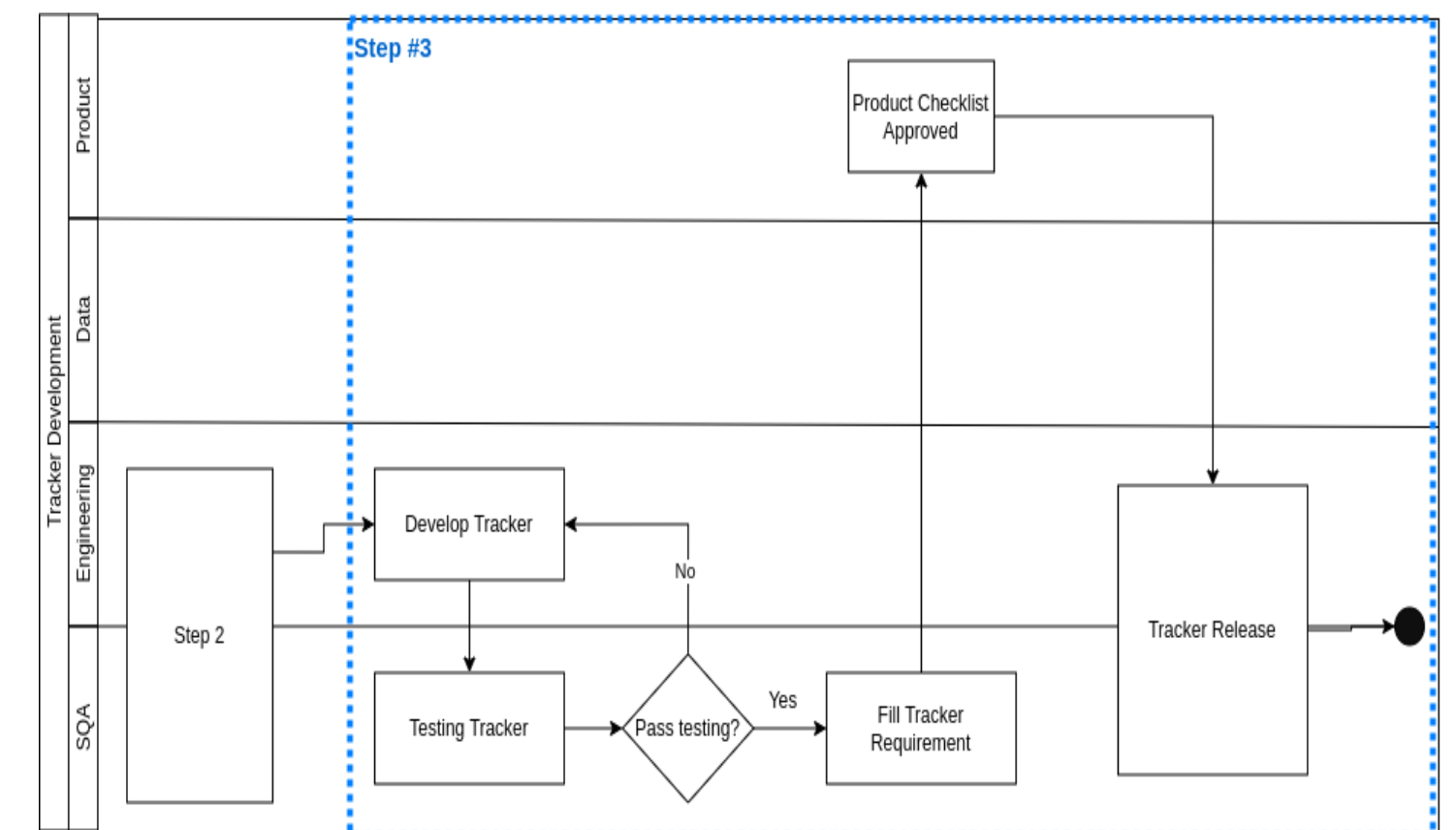
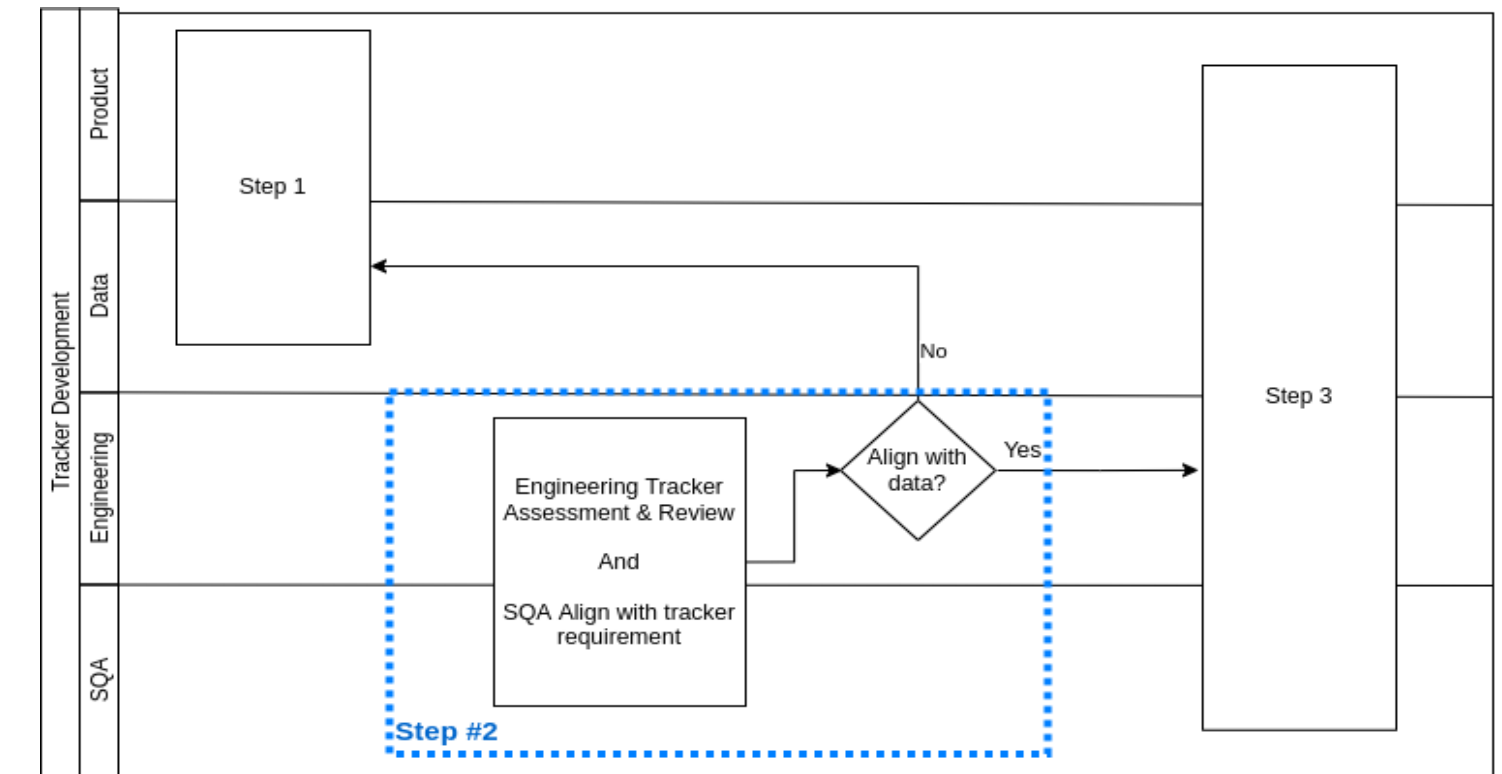
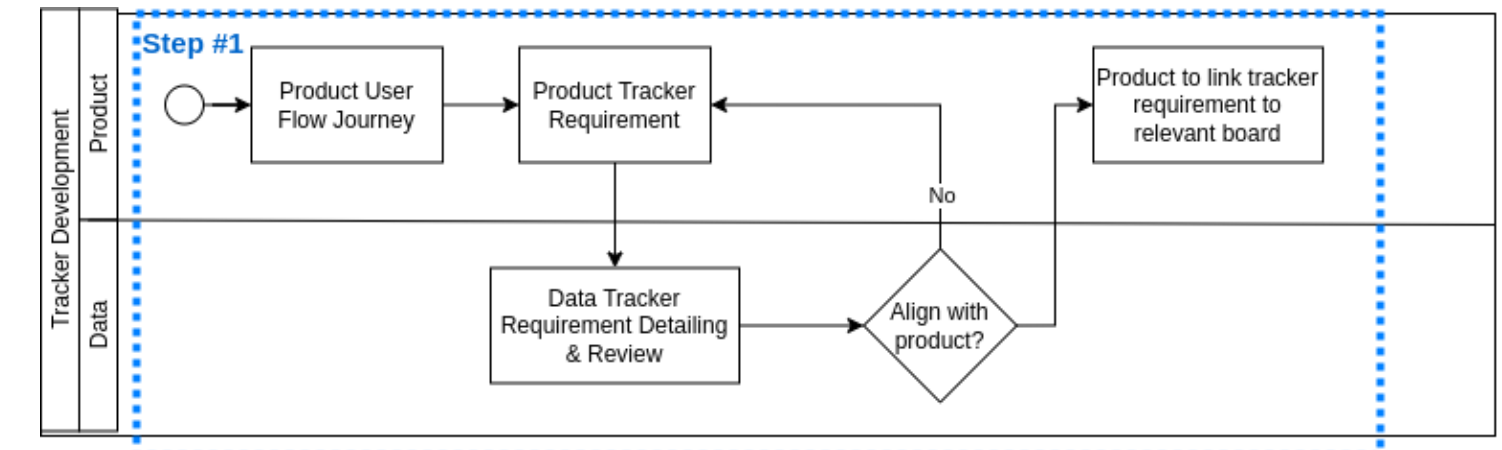
- Validate and improve security tool detection and response capabilities
- Prioritize efforts by correlating attacks to the findings of vulnerability management systems, Streamline security task management with IT and then track, monitor, and assure that security gaps are being closed
- Required dedicated China and Hong Kong Security team with professional security specialists cooperated with our networking team to conduct this assessment together.
- Remarks : The cost is changed subjected to the number of nodes and the network complexity of DMZ (Demilitarized Zone)

<6> SECURITY DATA ASSESSMENT AND TESTING



<Item 6.2> Data Track Safety (DTS) Assessment

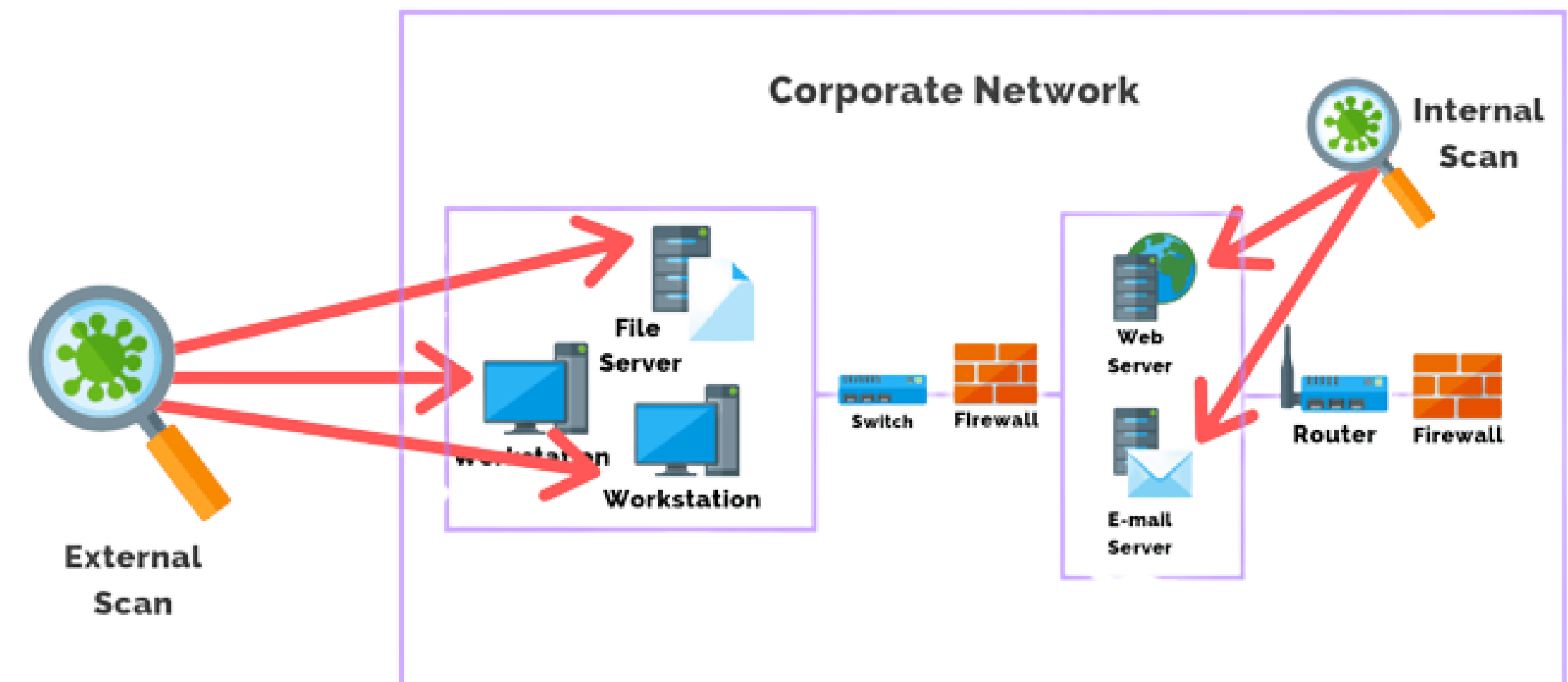
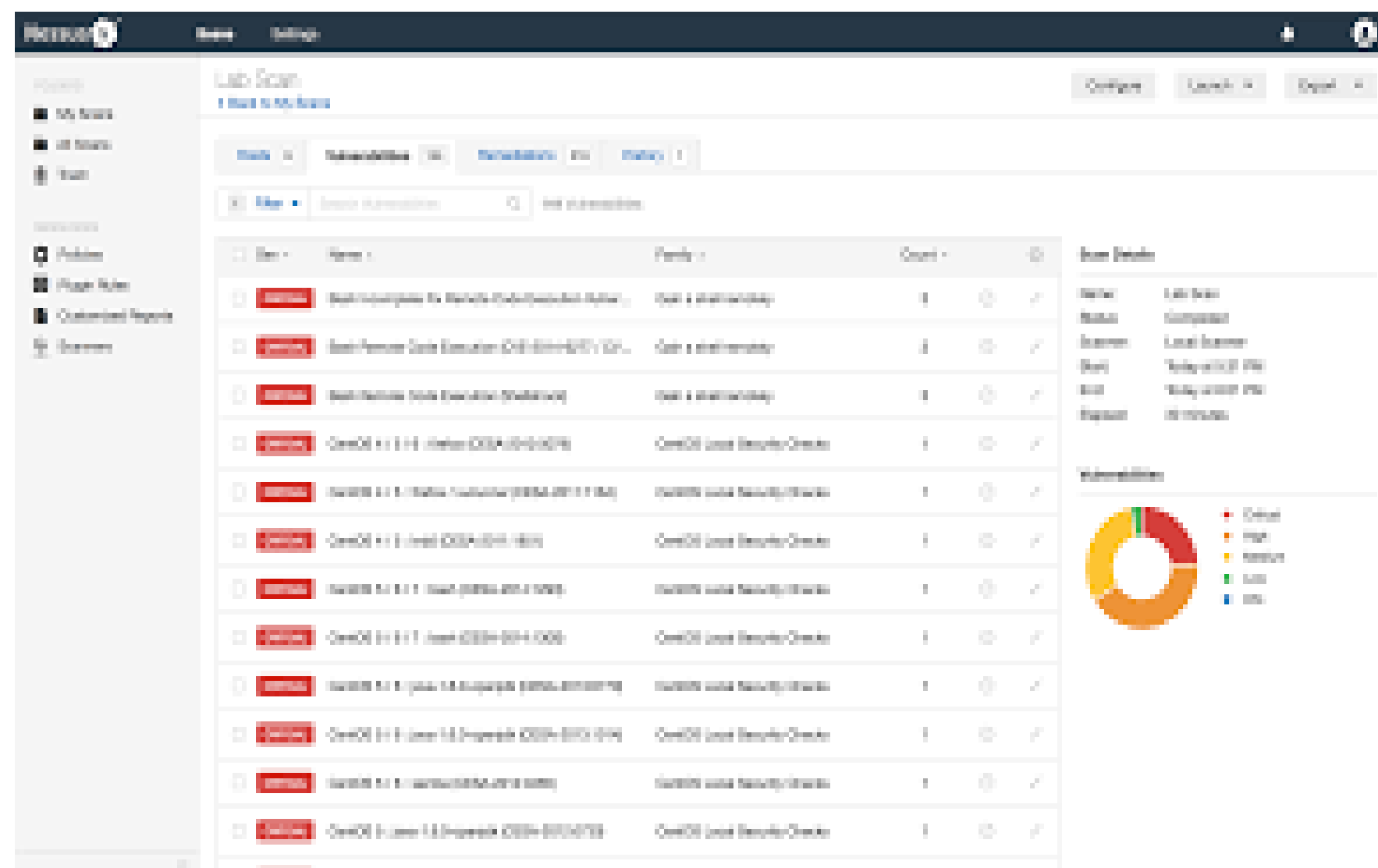
- It required data protection specialist, back-end and front-end engineers are accountable for the technical decision on the data tracking requirements
- It required another three main functions that are involved throughout this process, namely,
 - Product Manager, Data Analyst, Software Engineer
- The relevant work is shown on the right of workflow
- The cost is considered by data hosting at the place of local network only.



6> SECURITY DATA ASSESSMENT AND TESTING

<Item 6.3> Vulnerability Assessment (External and Internal)

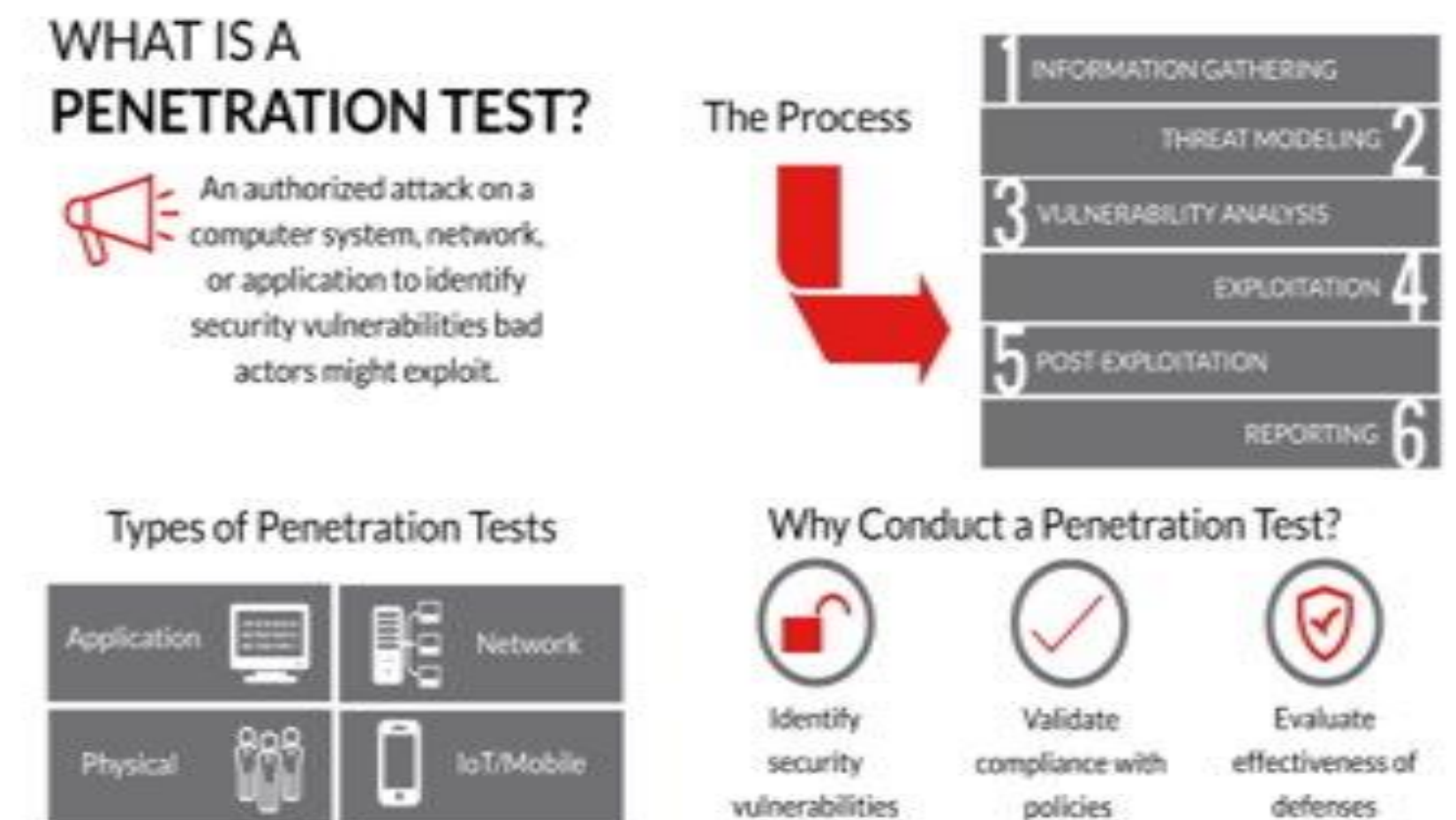
- Required dedicated security specialist to conduct the assessment until completion.
- Using CN platform for scanning with license of “啟明星辰” ,“Acunextix” and even “ Nexus” for assistance .
- Required our general assistants to consolidate the results from above platforms and lately revert to specialist’s review and analysis.
- If there is internal vulnerability Assessment, our engineer should conduct the site visit and perform the on-site assessment respectively
- If fail, we should suspend the test on another working days e.g.t Internet disconnection
- Remarks : The cost is changed by the number of IP and nodes in DMZ, the minimum charge is 150K(HK\$)



<6> SECURITY DATA ASSESSMENT AND TESTING

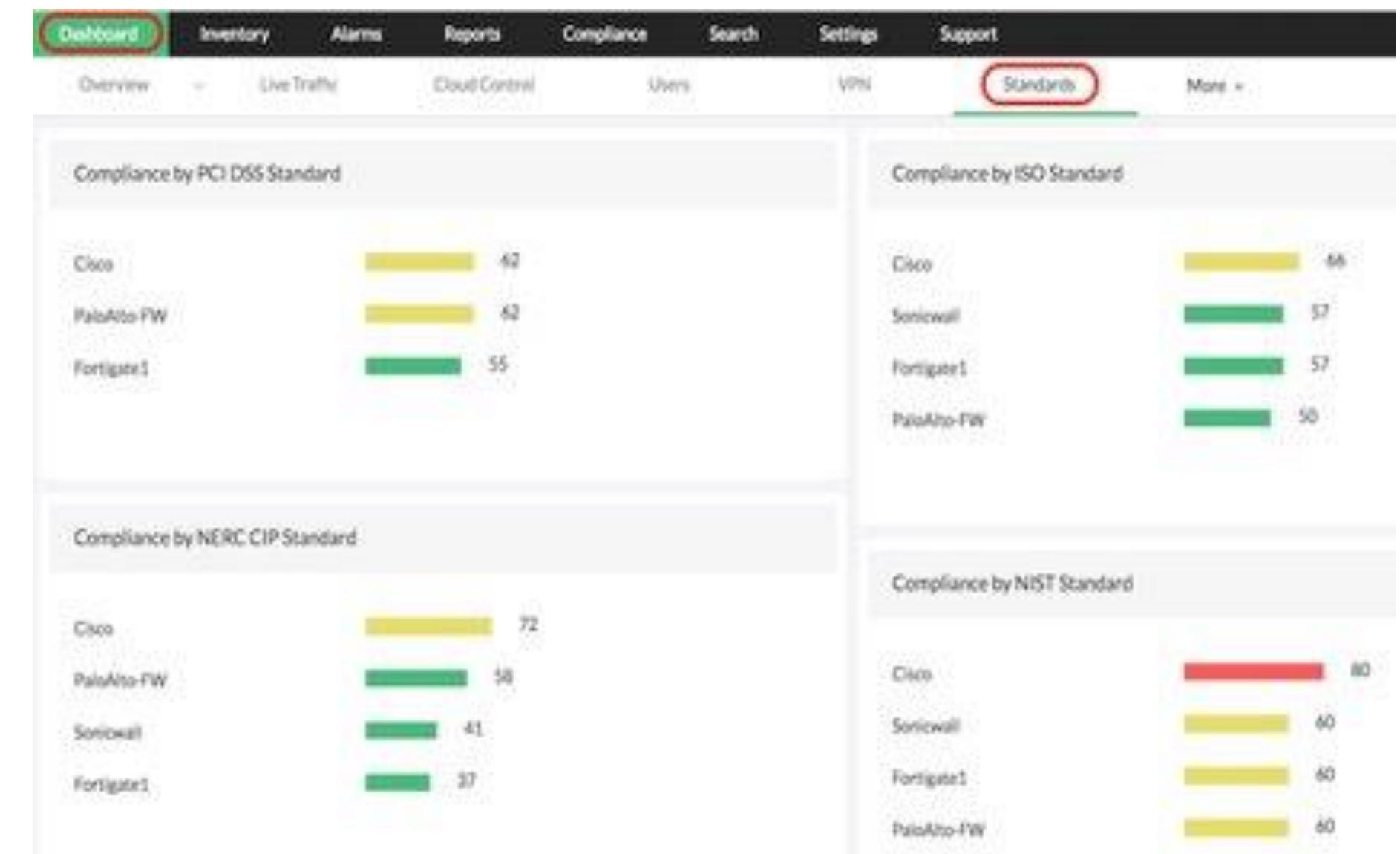
<Item 6.4> Manual Penetration Testing

- Physical Penetration Test (two Common Attack Vectors)
 - Social Engineering – is the art of manipulating people so they give up confidential information
 - Bypassing Security Cameras – can allow unauthorized physical access to sensitive areas
- Network Penetration Test (two Common Attack Vectors)
 - Phishing
 - A Distributed Denial Of Service Attack (DDOS)
 - A Man-in-the –Middle Attack (MitM)
- Mainly focused on manual P-test and consider automated platform liked "Acunetix "or "Pentera" for assistance if necessarily.
- To conduct this manual P-Test by our team, including Social Engineer, security data specialist, Red and Blue team etc.
- Remarks : The cost is changed by the number of IP and nodes in DMZ, the minimum charge is 150K(HK\$)



<Item 6.5> Log Reviews / Synthetic transactions / Code review and testing

- Our engineer is required to be manually reviewing logs or setting up log analysis tool/filter i.e. splunk
- Required Information security team and networking team to check and review the logs and even conduct the testing on site locations.
- Using the automated platform with licensed in ManageEngine for assistance

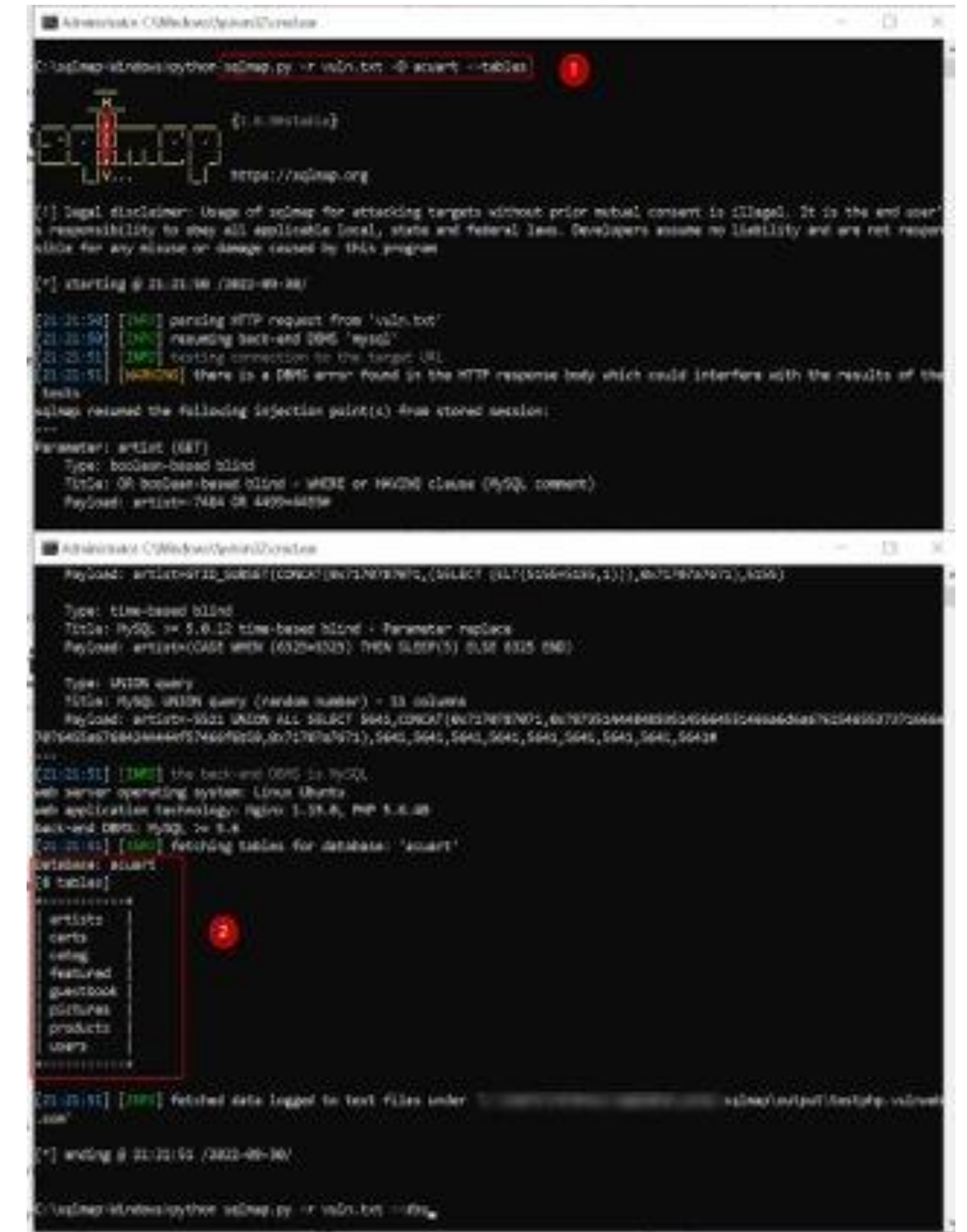


<6> SECURITY DATA ASSESSMENT AND TESTING

<Item 6.6> Misuse case testing

A process used by software testers as “ 啟明星辰 ” and “Acunetix” to evaluate the vulnerability of their software to known risks. Testers first enumerate the known misuse cases and then attempt to exploit those use case with manual and/ or automated attack techniques.

- It required Security engineer to simulate the misuse cases for attack and the blue team should be stand-by for recovery if any sudden occurs.

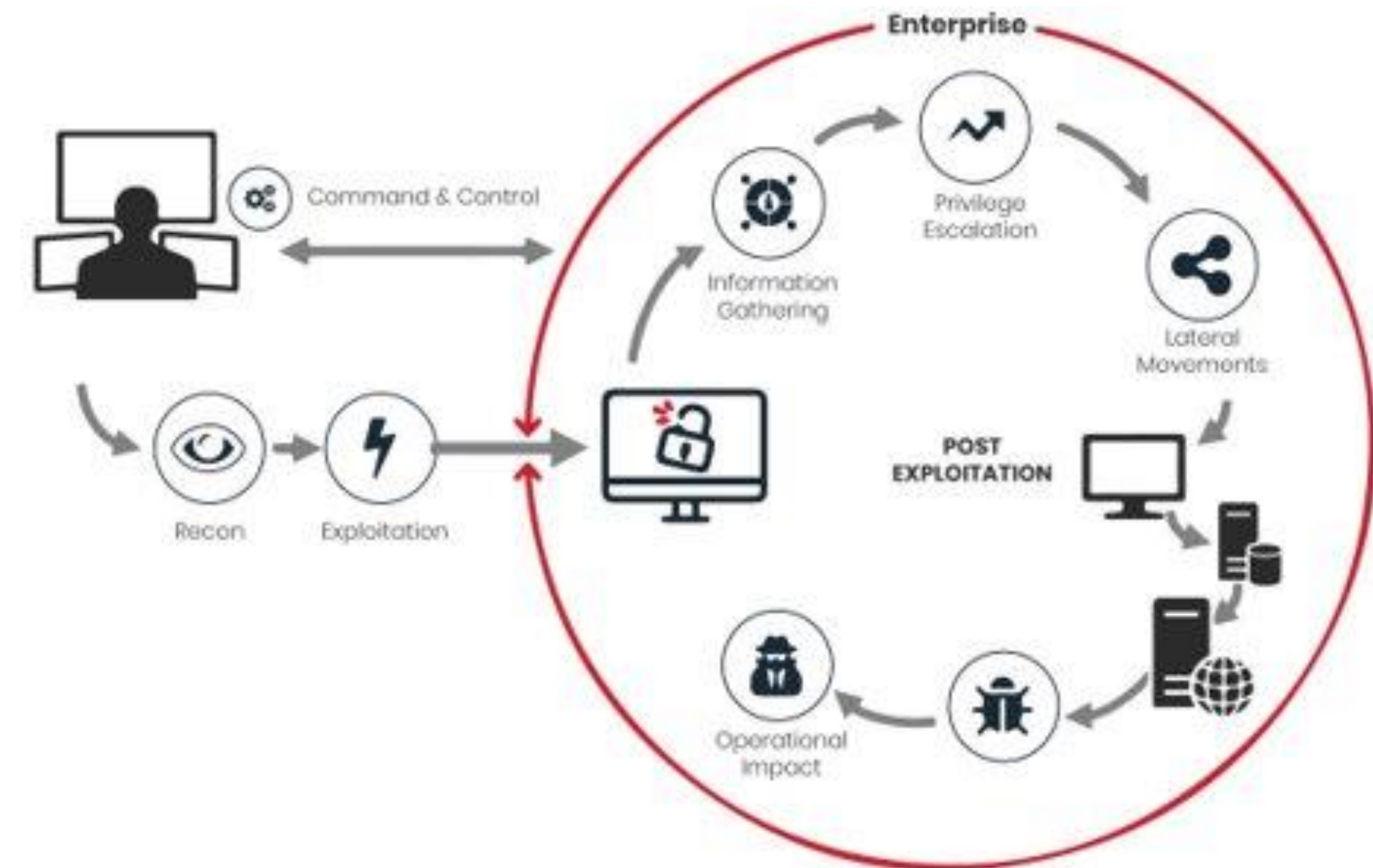


Product should meet a certain consumer demand, or it should be so compelling that consumers believe they need it.

<Item 6.7> Breach Attack Simulation

A process used by software testers as “ 啟明星辰” and “Acunetix” to evaluate the vulnerability of their software to known risks. Testers first enumerate the known misuse cases and then attempt to exploit those use case with manual and/ or automated attack techniques.

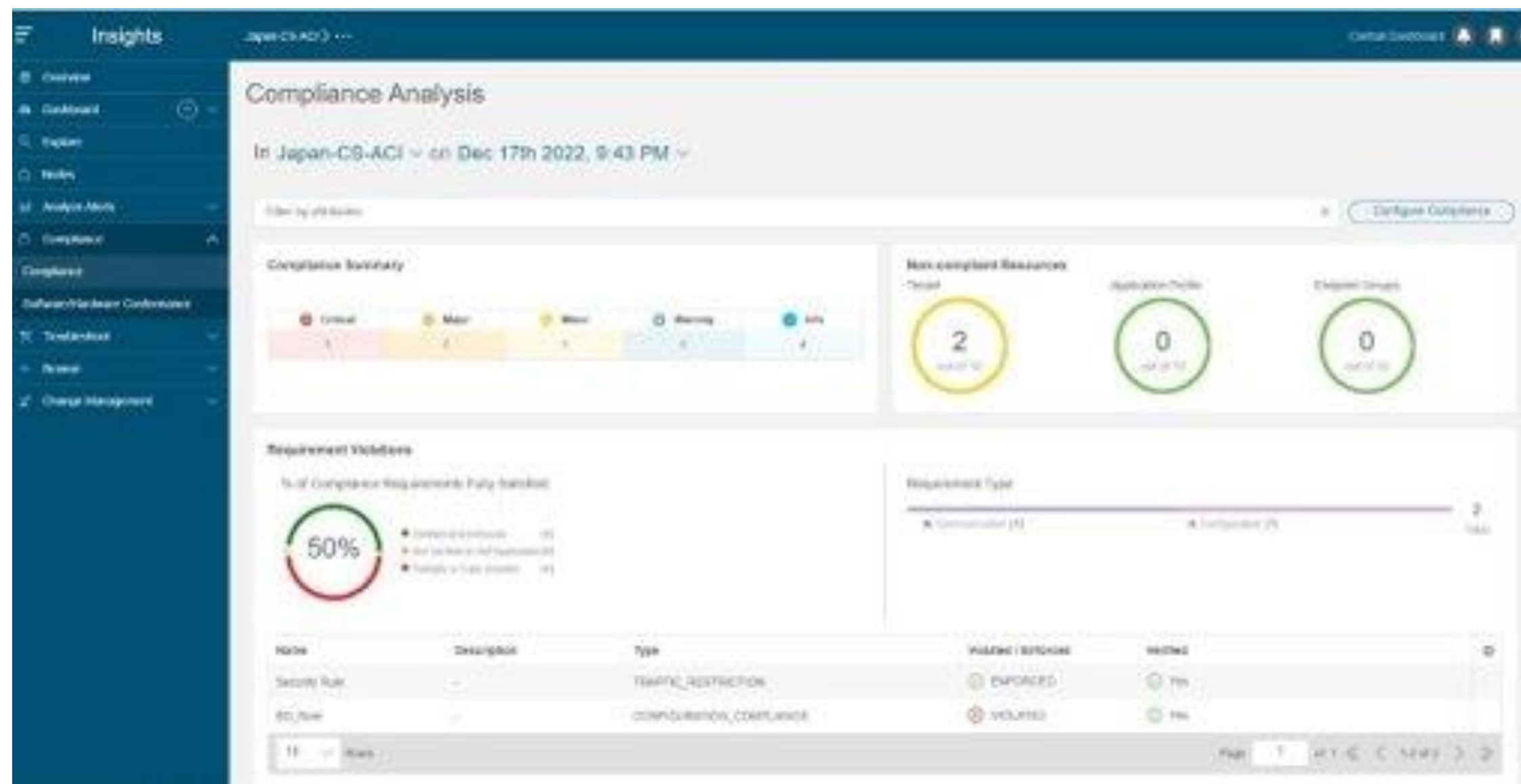
- It required Security engineer to simulate the misuse cases for attack and the blue team should be stand-by for recovery if any sudden occurs.
- Networking team should provide the back-up plan and reduce the impact on network from our breach attack simulation.



<6> SECURITY DATA ASSESSMENT AND TESTING

<Item 6.8> Compliance Checks

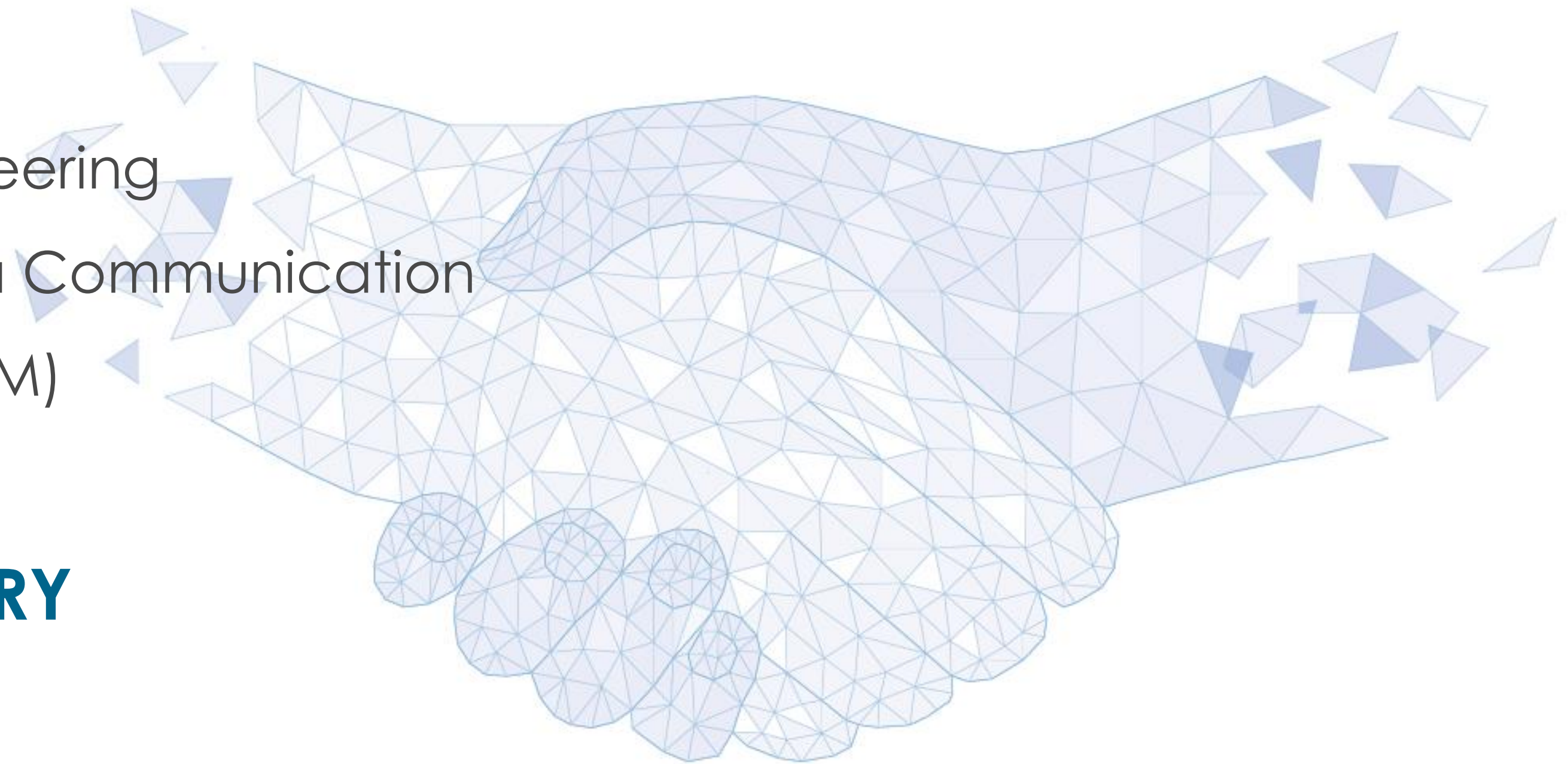
- A process used Required dedicated security specialist and networking team to conduct the assessment until completion.
- Using CN platform for assessment which are so called “啟明星辰”, “Acunextix” and even “Nexus” for assistance .



Product should meet a certain consumer demand, or it should be so compelling that consumers believe they need it.

Penetration Test (Pen Test)

- Security and Risk Management
- Asset Management
- Cybersecurity Architecture and Engineering
- Secure network Transmission and data Communication
- Identify and Access Management (IAM)
- Security Data Assessment and Testing
- **BACKUP and DISASTER RECOVERY**
- Data Security Operation
- Other



<7> Backup and disaster recovery(BDR)

<Item 7.1> Backup Verification Data Guidelines

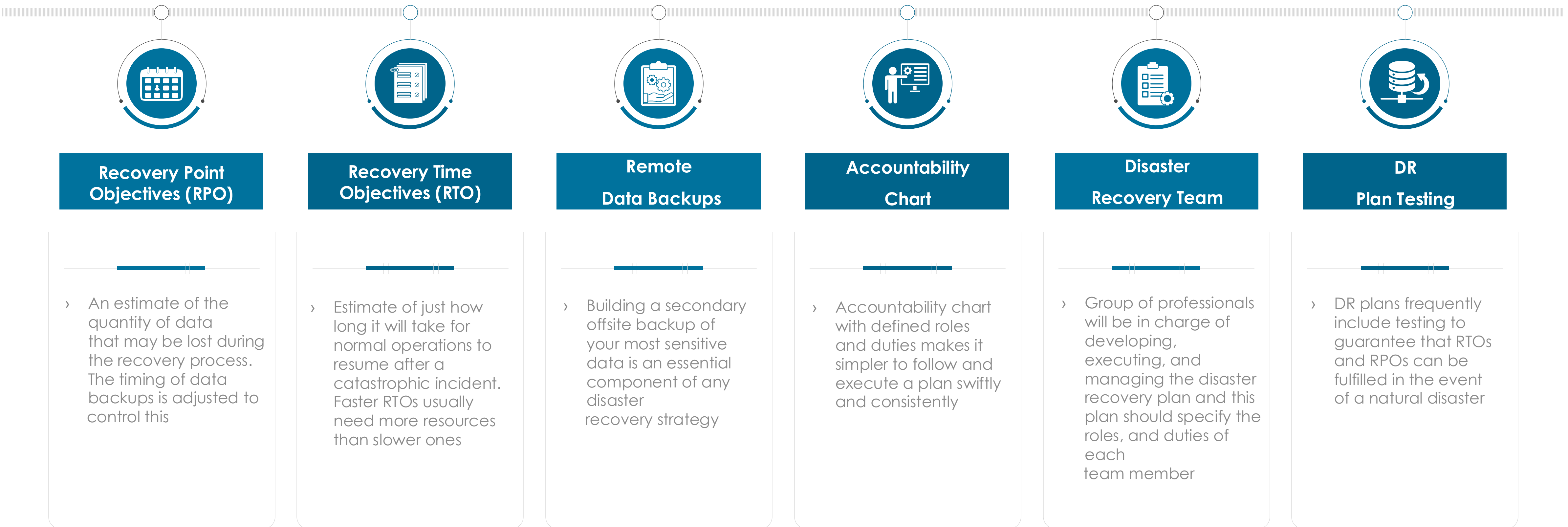
Under the standard of National Institute of standards and Technology, **NIST**

- Required experienced data specialist setup the scope of the back-up plan and disaster recovery guideline, and establish the procedure to verify that each daily backup is completed
- To provide the training for primary staff on the procedure and train secondary staff in case of absence or turnover so that it can avoid any knowledge gap
- Our team will constantly test backups, verify the procedures are working as planned and ensure that employees are adequately trained



<7> Backup and disaster recovery(BDR)

<Item 7.1 > Essential Elements of Disaster Recovery Plan



<7> BACKUP AND DISASTER RECOVERY(BDR)

<Item 7.2> Analyze test result and generate report
(including Remediation / Exception handling / Ethical disclosure)

Analysis of the Security Assessment Data

Required Information security team and security specialist to review and analyse the result, then subsequently conclude and appear their insights, remediation, exception handling and ethical in the comprehensive backup and disaster recovery report

- Consider what information provided to you is incomplete or might be a lie or half-truth.
- Look for patterns by grouping your initial findings by the affected resources, risk, issue category, etc.
- Identify for trends that highlight the existence of underlying problems that affect security.
- If examining scanner output, consider exploring the data using spreadsheets and pivot tables.
- Fill in the gaps in your understanding with follow-up scans, documentation requests, and interviews.
- Involve colleagues in your analysis to obtain other people's perspectives on the data and conclusions.



5 Reasons You Need a Backup and Disaster Recovery Partner

<Item 8.1>

Increase Data Security Awareness and Company with investigations, there are:

- 6Hrs x Training course and activities
- Invite 1 or 2 legal security practitioner and auditor for the presentation of how to handle the case relating security operation under investigation.



<8> DATA SECURITY OPERATION

<Item 8.2> Review Logging and monitoring activities, the cost is changed subjected to the scope of work, we shall provide

- <Item 8.2.1 > Intrusion Detection Systems (IDS) and Intrusion Prevention System (IPS)
 - These two platforms are primarily focused on identifying possible incidents, logging information and reporting, and analyses network traffic content to network traffic for patterns and recognize malicious attack patterns.
 - The cost included 2x installation of hardware and software with licenses, 2 x suggested basic hardware and 20 user accounts only.



<8> DATA SECURITY OPERATION

<Item 8.2>

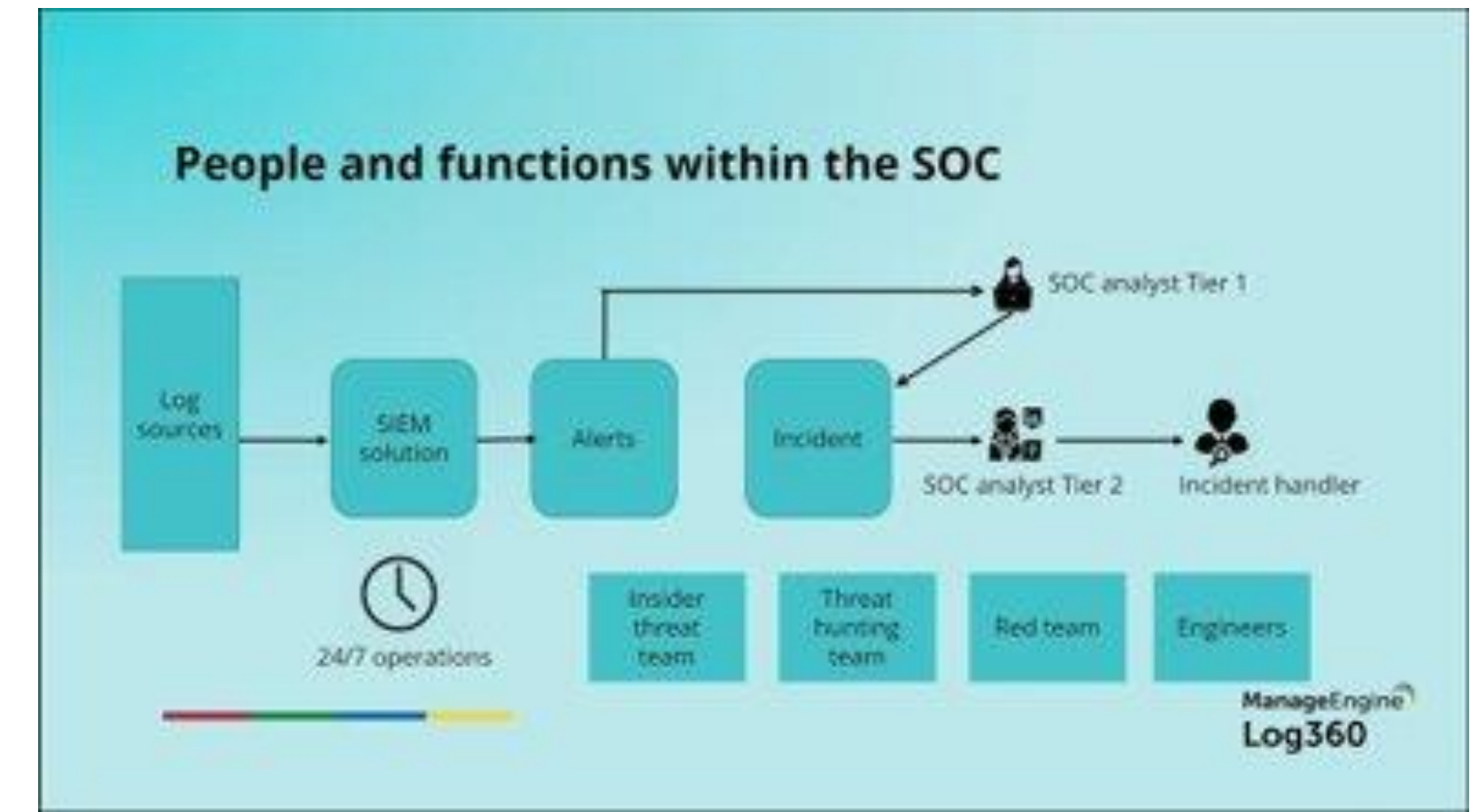
Review Logging and monitoring activities, the cost is changed subjected to the scope of work, we shall provide

<Item 8.2.2 > Security Information and Event Management, regular event notification and monitoring, log management and threat intelligence, we will

Dedicated our security specialist to design, plan and review the process for achieving your business goals into SIEM, Provide 50x User accounts for the platform ManageEngine

To streamline our service of security operation center, SOC in China, we can help to monitor network traffic and to push notification to dedicated person if any occurs for a year.

<Item 8.2.2 > User and Entity Behavior Analytics (UEBA)

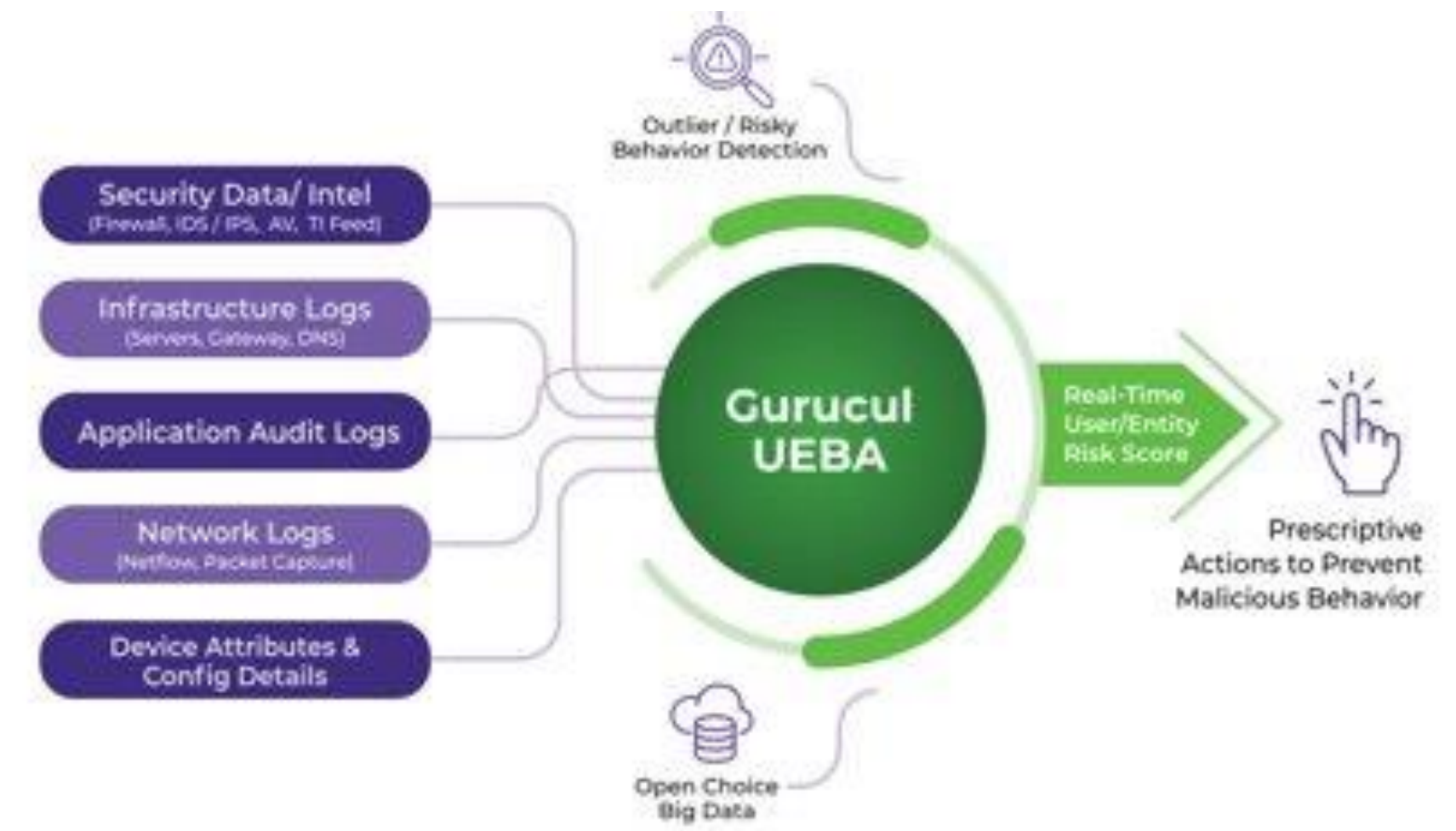


<Item 8.2>

Review Logging and monitoring activities, the cost is changed subjected to the scope of work, we shall provide

- <Item 8.2.3 > User and Entity Behavior Analytics (UEBA)

- Dedicated security coordinator conducted the questionnaire across all level users in department
- Our security specialist should analysis and summarize the result of questionnaire and correlating with the possible events incidents by people, since then will provide the conclusion of how to prevent data disaster by malicious behavior in future.



<8> Data Security Operation

<Item 8.3.1>

To operate the detective and preventative measurement

<Item 8.3.2 >

The implementation of Intrusion detection system and Intrusion Prevention System

<Item 8.4>

To evaluate the third-party security service whether be appropriated to business

Referred by <Item 8.3.1> <Item 8.3.2 > and <Item 8.4> ,
if the implementation should be worked and processed outside of Hong Kong, we may consider:

- To refer by the **cross-border data** transfers from the transfer mechanisms requirements set out in Article 38
- Training : Mandarin Speaking
- Our Support and delivery
- Hardware and software, network design and the cross boarder of internet connection etc.
- Others



Remarks : The price is varied and considered by the scope of work and the location in China

<8> Data Security Operation

<Item 8.4.> The implementation of Backup and disaster recovery (BDR)

- Our security and networking team will support your specific team to work together regarding the implementation of backup and disaster recovery as scheduled.
- Our security and networking team will review and check the result after completion.
- If any occurs, we may seek the professional data specialist for further assistance.



<Item 8.4.1> Increased the awareness of Personal Data Safety and protection and

<Item 8.4.2> Emergency Back-up and recovery management

- Our security team prepare and share relevant material to everyone
- To invite the speaker to present about the importance of personal data safety and protection
- Organizing some activities to increase their personal data awareness
- In terms of emergency Back-up and recovery management, we may
 - Design the plan with specific team and decision-maker under the budgets concerns.
 - Process and review the procedure where can facilitate a rapid and successful restoration of operation if any occurs
 - Conduct the testing and revision procedure
 - Conclude our insights and remediation into the guidelines of emergency back-up and recovery



< Item 8.4.3> Data Security Emergency and Recovery Training and Awareness

- Our security team prepare and share relevant material to everyone
- To invite the speaker to present about the importance of personal data safety and protection
- Organizing some activities to increase their personal data awareness
- Setup the high-alert notification in help-desk



<Item 9.1> Providing legal Security consulting service in Hong Kong and China

- To provide one year subscription plan of legal security consulting service (basic / standard and premium)
- To provide the legal advice with the communication by telephone, email or face to face.
- To explore any possible data breach the contract, industry practice or regulations.
- To review any data whether satisfy the requirement of regulation and compliance.
- Not included :
 - To give the legal advice once you are being a high target for cyber attacks if necessary
 - To provide cyber security law training for your employee



< Item 9.2 > Providing Data Protection Insurance (Standard or Tailored solutions)

Standard version

• First Party

- **Incident Response** – from an actual or suspected cyber event – often nil deductible
- **Business Interruption** – loss of net profit and continuing operating expenses
- **Data and System Recovery** – increased cost of work, data recovery costs, additional business interruption mitigation
- **Cyber Extortion** – extortion payments and negotiation

• Third Party

- **Privacy and Network Security Liability**– liability following data breach or failure of network security:
 - PCI DSS contractual fines and penalties
 - Consumer redress fund
 - Regulatory fines and penalties (where legally insurable) – GDPR



- **Media Liability** – liability following defamation or infringement online

Comprehensive Security Testing

Conduct thorough simulated hacker attacks to identify flaws and vulnerabilities in the information system

Legal and Compliant Operations

Meet the requirements of cybersecurity regulations and laws, such as information security level protection and the cybersecurity law, through penetration testing services.

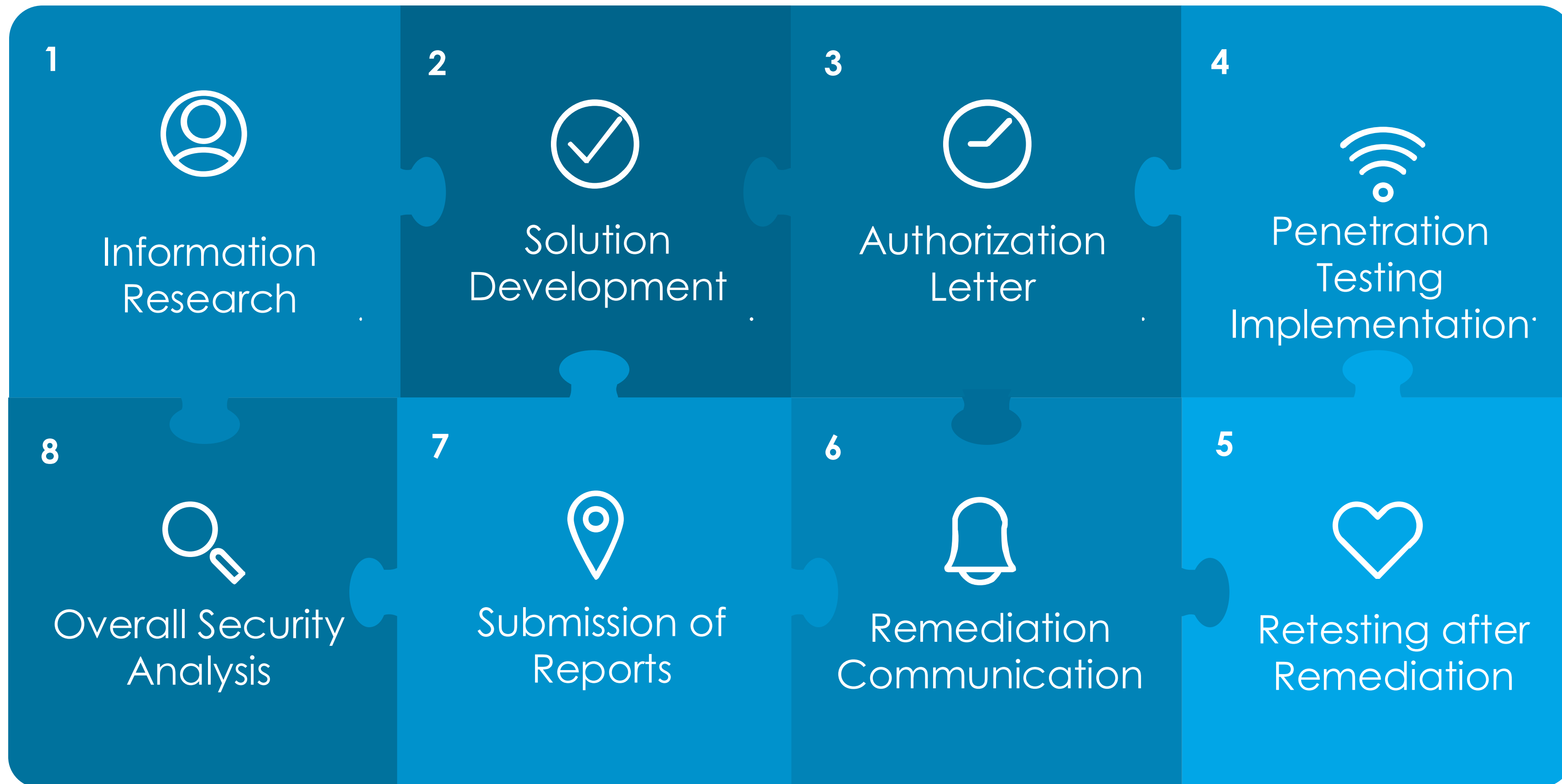


Enhanced Security Capabilities

Utilize the penetration testing report for training and educating personnel, providing detailed procedures and repair recommendations.

Reduce the risk of data breaches

Penetration tests can help organizations to reduce the risk of data breaches by identifying and remediating vulnerabilities that could be exploited by attackers.





✉ info@goipgroup.com

🌐 www.goipgroup.com



+60 3 2700 7929
VO6-06-06, Signature Office 2,
Lingkar SV, Sunway Velocity,
55100 Kuala Lumpur, Malaysia

HONG KONG

+852 2138 9388
Unit 03-06 27/F Metropolis Tower,
6-10 Metropolis Drive, Hung Hom

MALAYSIA

SINGAPORE

+65 6826 6288
8 Eu Tong Sen Street, #22-81,
The Central, Singapore 059818