

INGRAM^{MICRO} SECURITY

Ingram Micro Cyber Security Portfolio



Cyber Security Services



Ingram Micro Cyber Security Portfolio

Services



Technical
Assessment



Consultancy
Service



Managed
Security Service

Trainings



General Training



Certification
Training



Specialized
Training

Vendors



Cyber Security Value Added Service - Global Offer

Basic Technical Services

Public Discovery

Web App Assessment

Vulnerability Assessment

Penetration Testing

Web Malware detection

PCI DSS ASV Scan

Source code review

Data Leakage Prevention

Configuration review

Consultancy Services

Governance & Strategy

Policies & Procedures

Compliance Assessment

Risk Assessment

Multi-Vendor Security Architecture

Access Control Assessment

Managed Security Services

Regular Assessment

SOCaaS

Security Monitoring

Incident Response

Digital Forensics

Threat Intelligence

Training Services

Cyber Security Awareness (Executive, Users, IT)

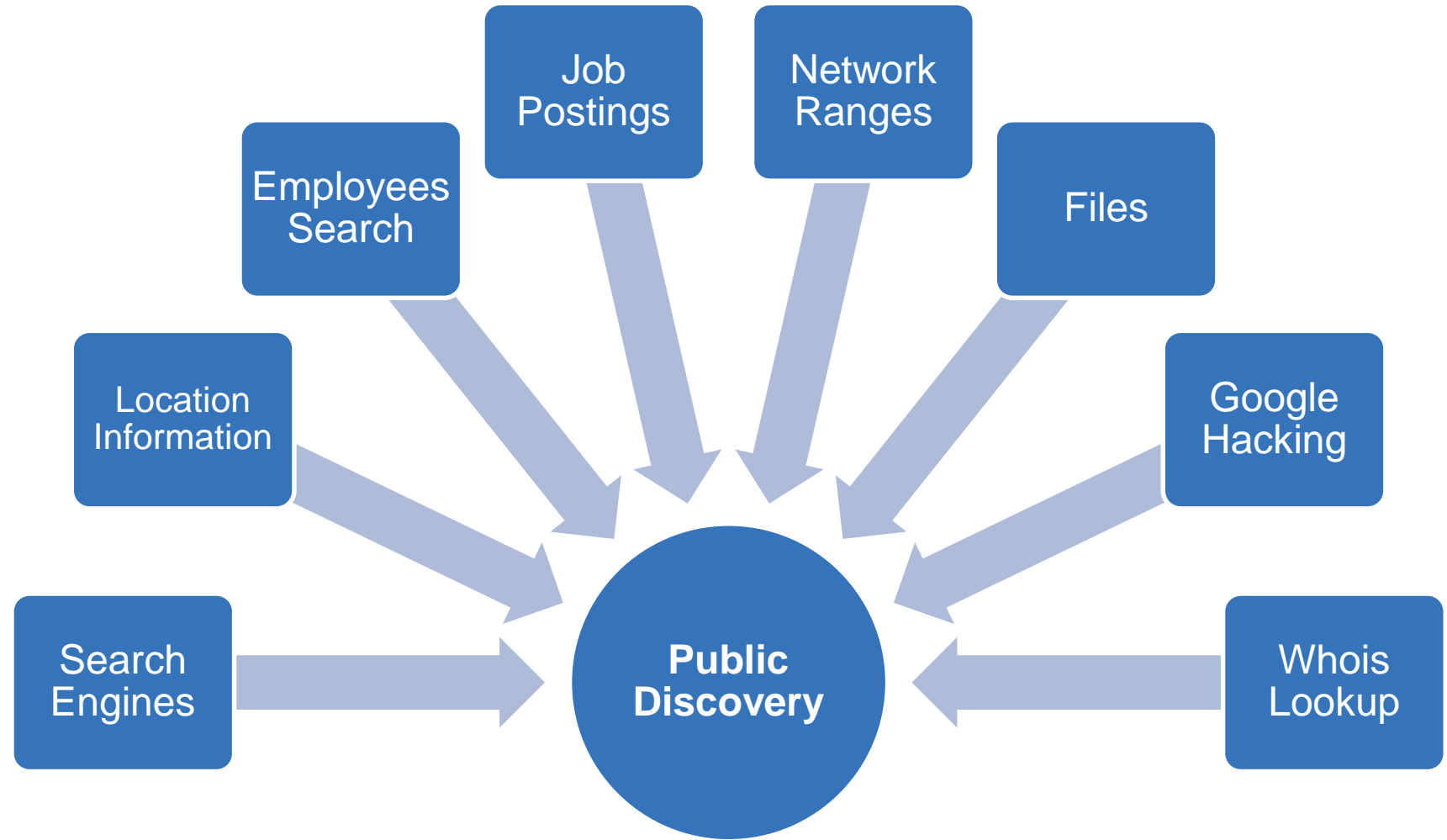
Certification Training (CISSP, Security+, Network+, etc.)

Specialized training (Secure coding, Forensics examination)

Cyber Security Services – Public Discovery Report

Description:

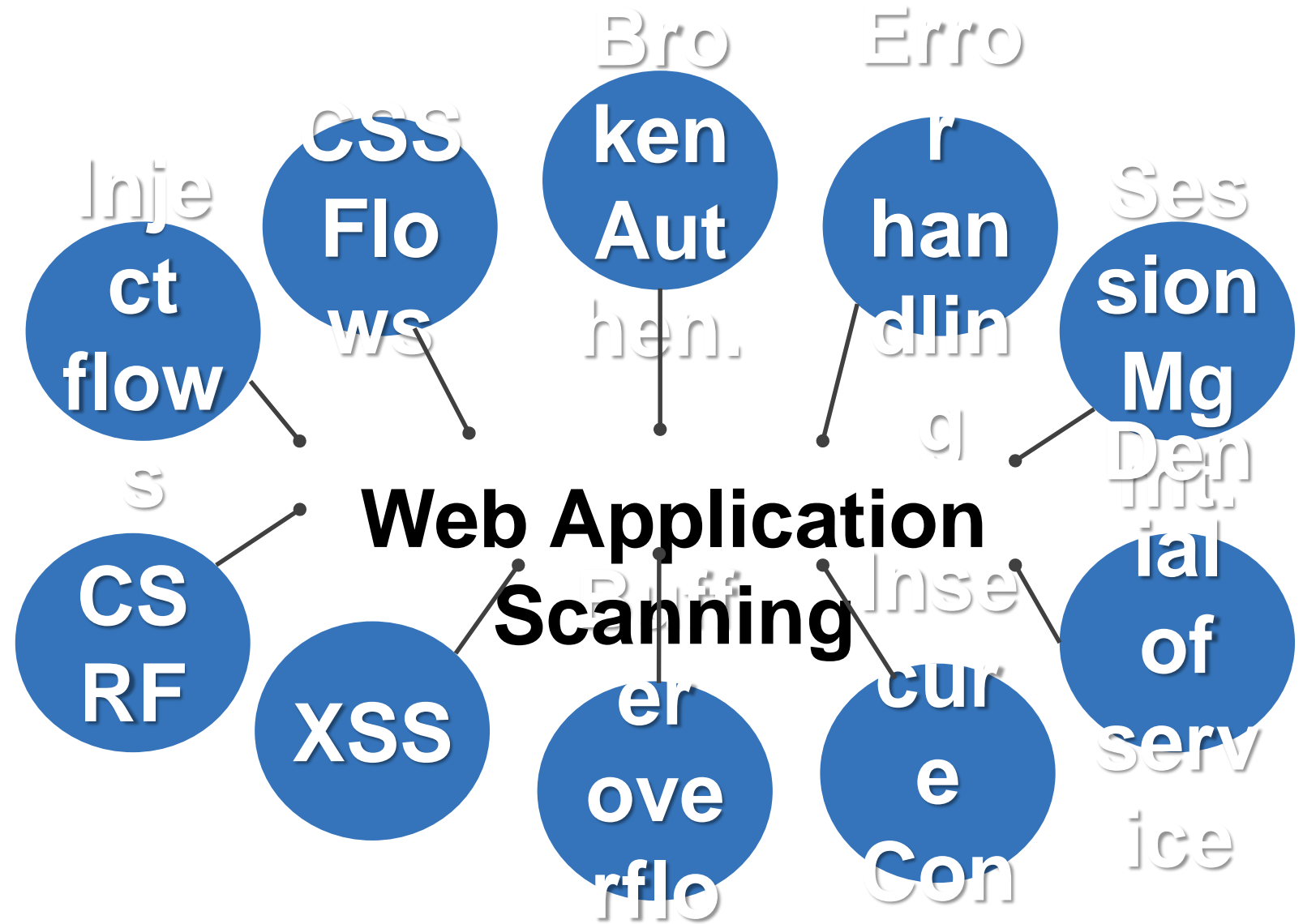
- **Free of charge.**
- **Passive i.e. no interaction with client systems.**
- **Aims to identify**



Cyber Security Services – Web Application Scanning

Description:

- Available in external and internal format.
- Aims to test web related vulnerabilities for public facing web



Cyber Security Services – Vulnerability Assessment

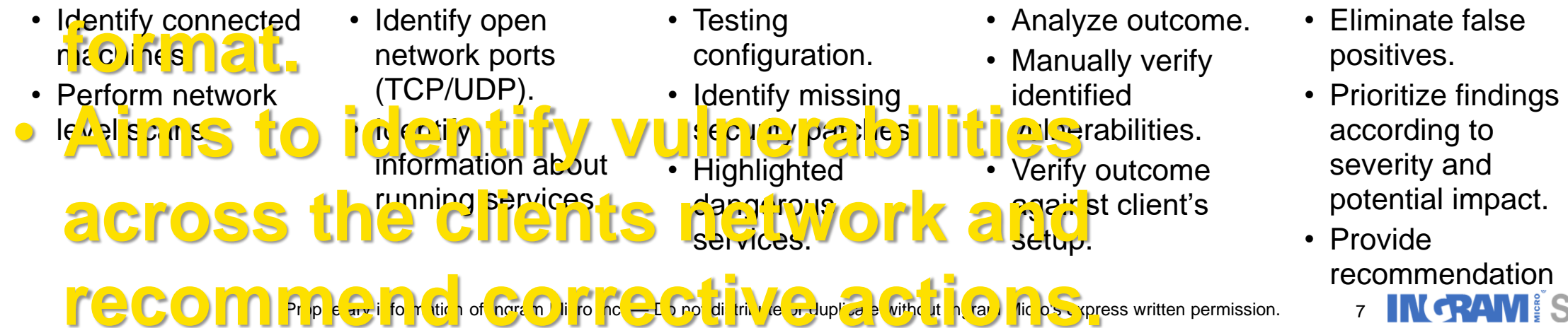
Description:

- Similar to Web Vulnerability Scanning, however it covers all servers, network devices, applications, and end points.

Time to deliver:

- **Two business day.**

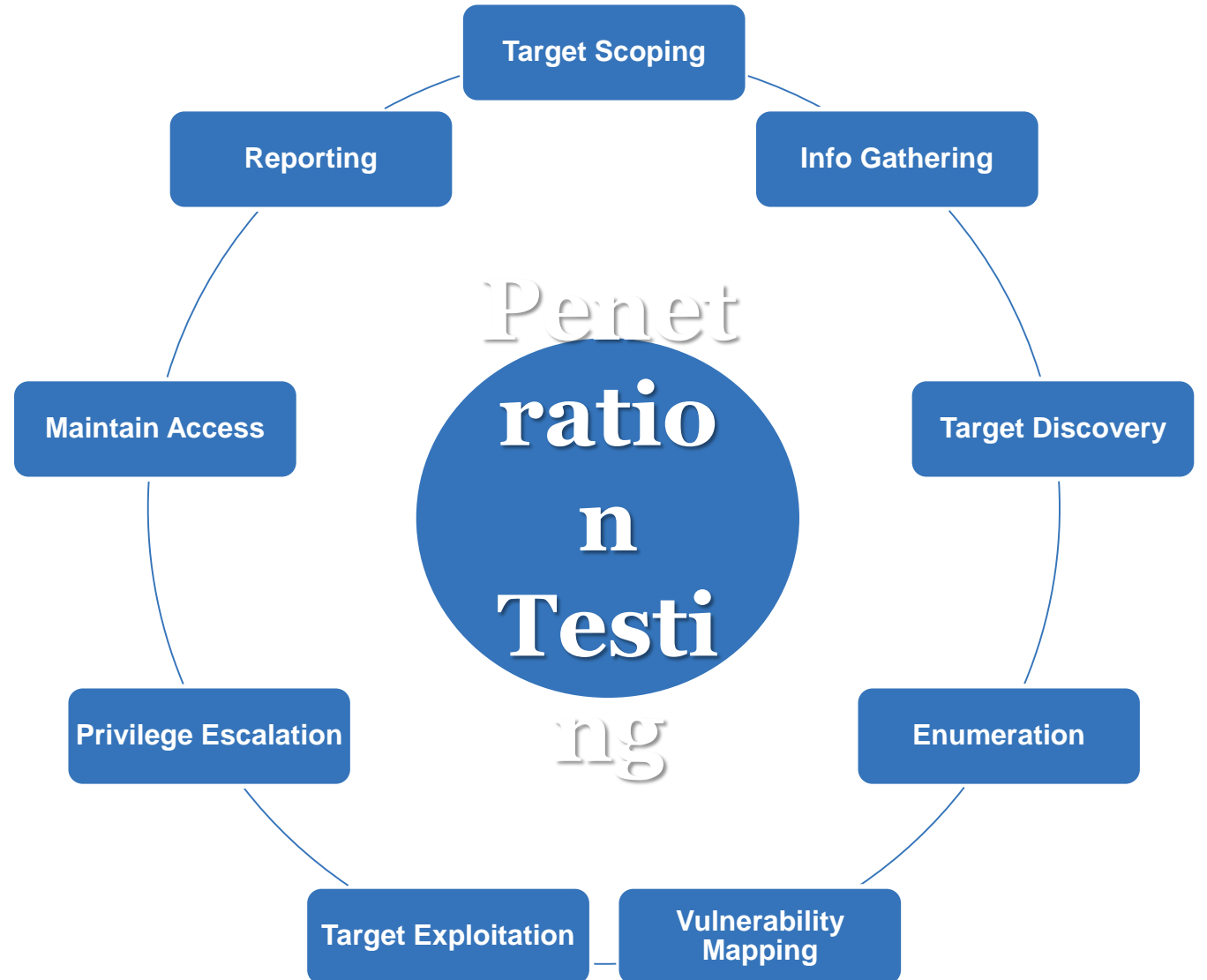
- **Available in external and internal format.**



Cyber Security Services - Penetration Testing

Description:

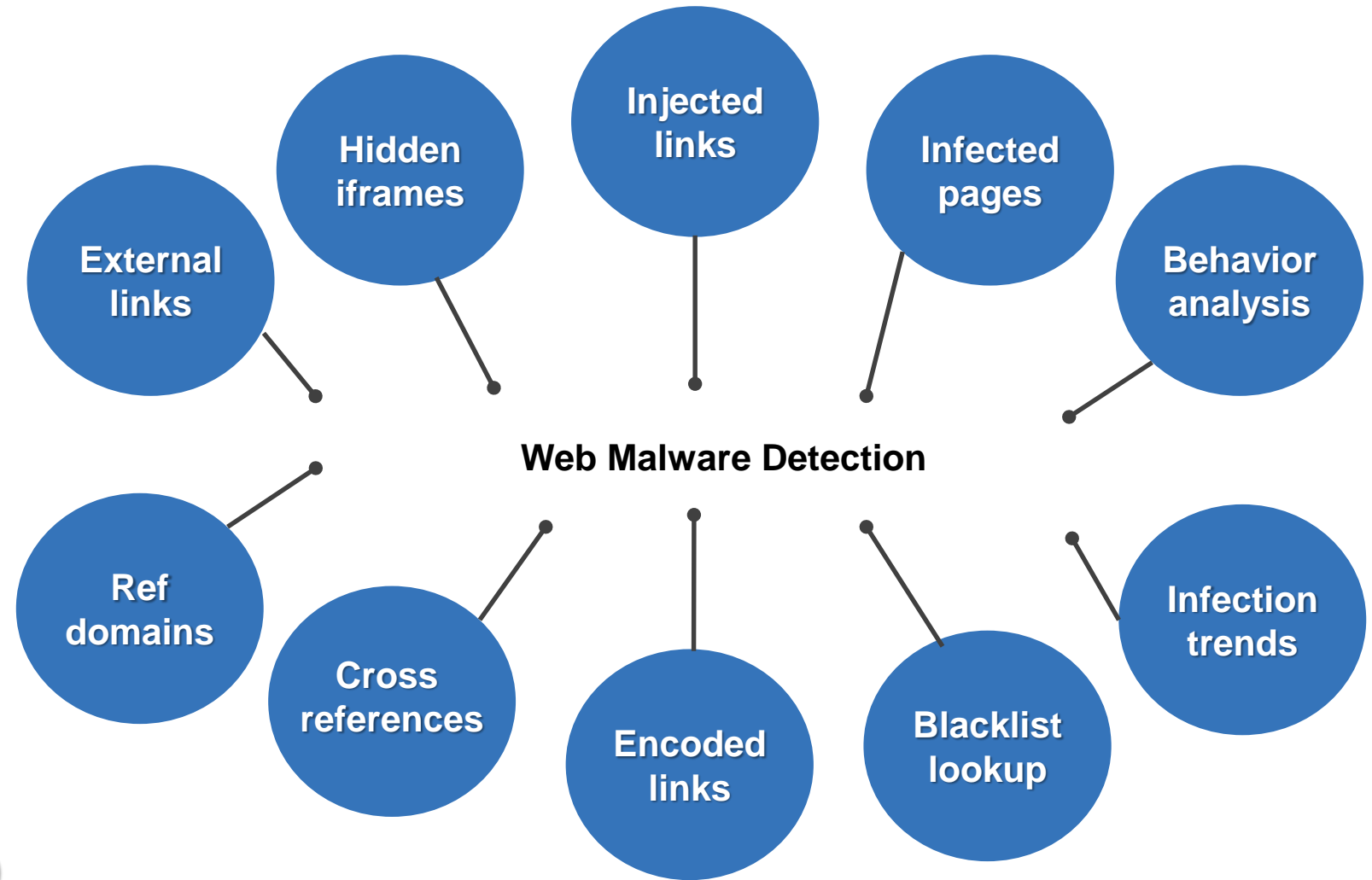
- Available in external and internal format.
- Black box penetration testing is available as well.
- Aims to identify vulnerabilities in the network



Cyber Security Services – Web Malware Detection

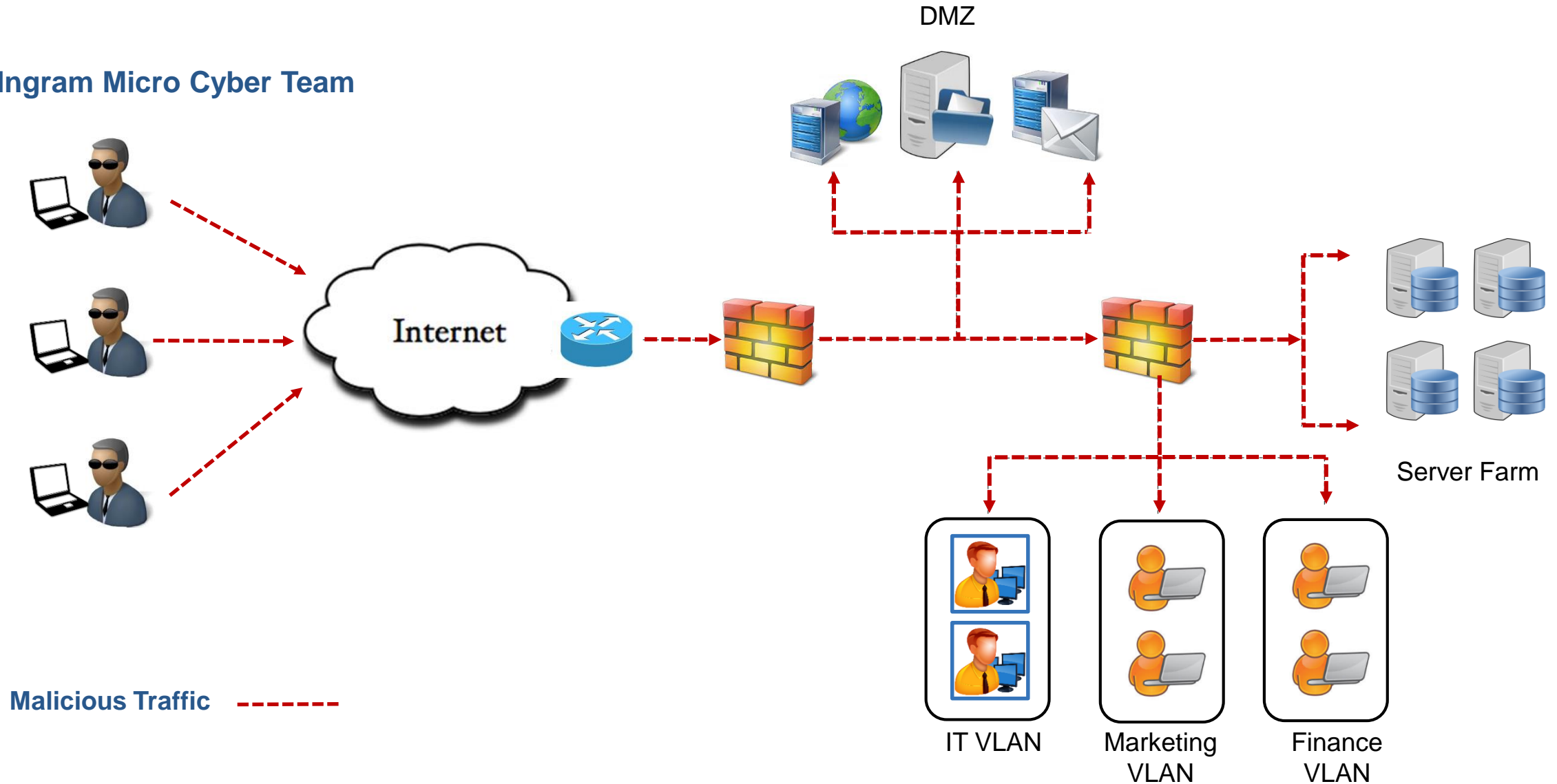
Description:

- Available in external and internal format.
- Aims to identify malwares in customer web site(s).

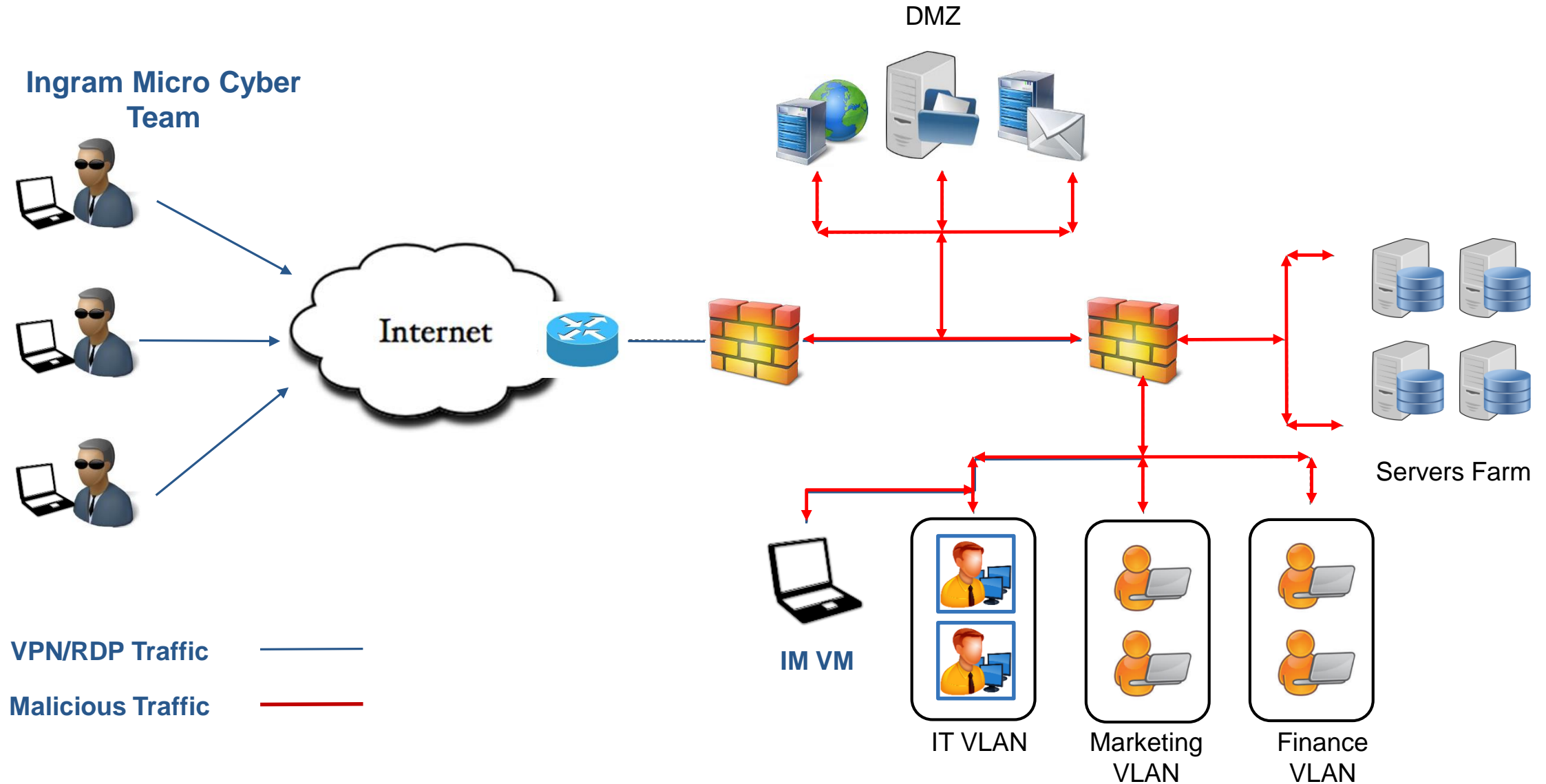


How Do We Deliver Our Services – External Format

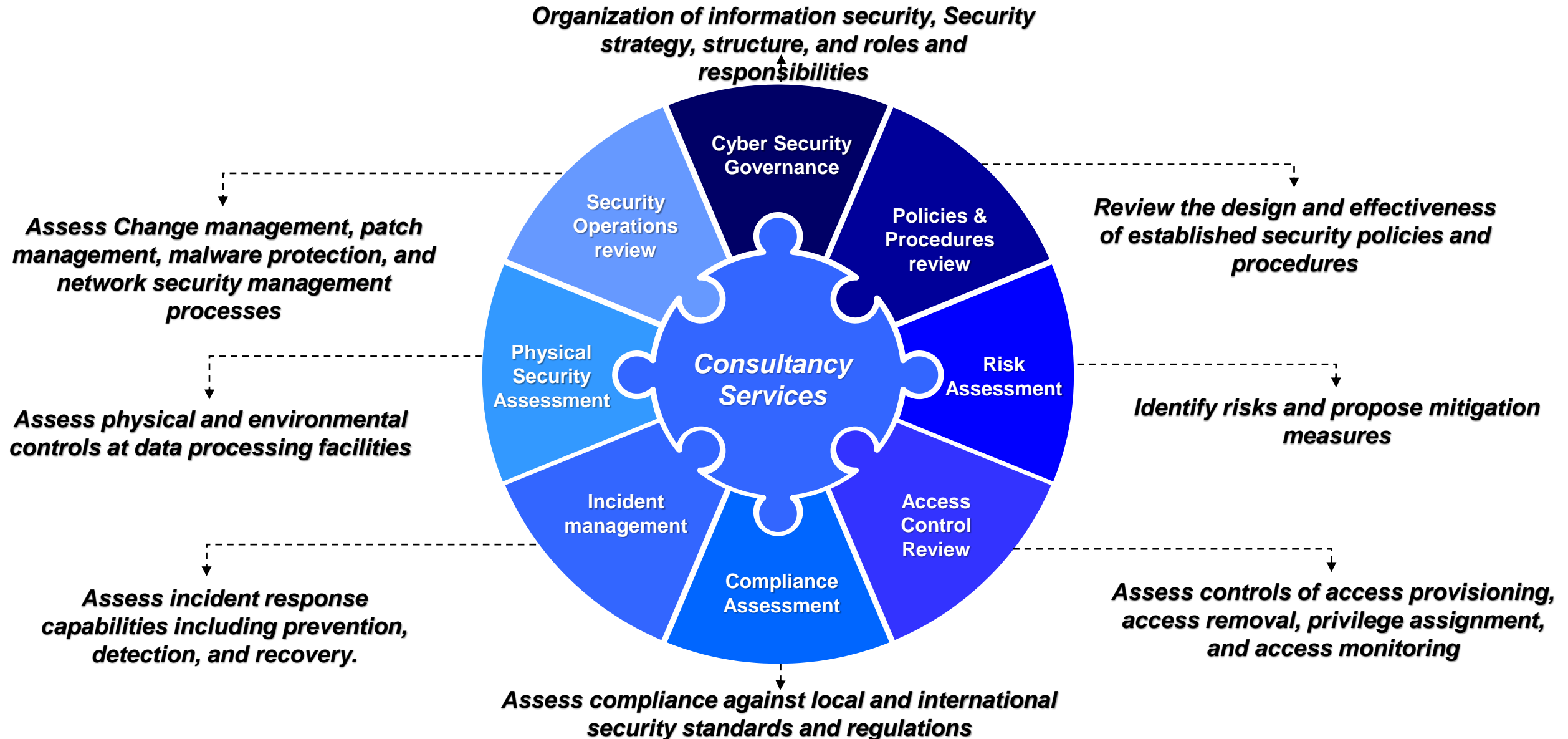
Ingram Micro Cyber Team



How Do We Deliver Our Services – Internal Format



Consultancy Services



Key Questions to Ask?



Are you already compromised? Do you know how good are your security defences? Do you know what would you do if you are compromised today?



Did you have a security incident and crisis management plan? Do you know the roles of your management aware of their roles and responsibilities regarding cyber security?



Does your organization have the required skills to manage Cyber Security? Do you have the right processes to manage your security? Are they effective? Are they designed as per best practices?



Do you have the right processes to manage Cyber Security? Do you have the right processes to manage your security? Are they effective? Are they designed as per best practices?



Sample Statement Of Services

PDR SoS

VA SoS

PT SoS



Sample Reports

Sample PDR Reports

IP Addresses, Open ports, and Running Services

We identified the following IP addresses, ports and services relevant to your organisation:

IP	PORT	Service
78.100.53.180	443	Apache Tomcat/Coyote JSP engine/version: 1.1
83.138.131.130	80	
	443	Mozilla/5 HTTPAPI httpdVersion: 2.0
12.130.158.179	80	Apache httpd
	443	Apache httpd
213.130.132.216	80	Apache httpd
199.7.200.45	80	
	443	Apache httpd
78.100.53.160	80	IronPort AsyncOS etc
87.120.190.82	13	Postfix smtpd
	443	nginx
	243	imap

Technology Stack

We identified the following technologies running on your machine:

Name
Operating System name
Web server name
Server side technology used
Client side technology used
Web Application Firewall

Login Pages

The following login web pages were accessible from the internet:

Address
https://78.100.53.180:443/

Vulnerable Services

We found the following potentially harmful/vulnerable services enabled on your web servers:

Hostname	Service Name & Version	Vulnerability
booking.qatarairways.com	Ticket, TLSv1.1	
ebswebad.qatarairways.com	Sslv, Sslv3, Tls1.1	The POODLE attack
qr.qatarairways.com	Tls1.1, TLSv1.1	
qr.qatarairways.com	Tls1.1, TLSv1.1	
career.qatarairways.com	Tls1.1, TLSv1.1	

Email Accounts & Security Status

Email ID	Dark Web Status
agrawal@qatarairways.com	Cafe
joh.jayaraman@qatarairways.com	Cafe
siriyah@qatarairways.com	Breachmail
gopal.singh@qatarairways.com	Cafe
akshdeep.kumar@qatarairways.com	Cafe
paul.gupta@qatarairways.com	Breachmail
a.hussain@qatarairways.com	Cafe
amrutha.pillai@qatarairways.com	Cafe
aradhya.duggan@qatarairways.com	Cafe
rashmi.sharma@qatarairways.com	Breachmail
abhishek.vijaya@qatarairways.com	Cafe
nandini.kumar@qatarairways.com	Cafe
prakash.mishra@qatarairways.com	Cafe

Sample VA Reports

INGRAM

INTEGRITY

IP	Host Name
x.1.0.x	MYVIS
x.1.0.x	VSCNWN2031
x.1.0.x	VCOHR
x.1.0.x	NEWPCS
x.1.0.x	
x.1.0.x	
x.1.0.x	
x.1.0.x	

INTEGRITY

Reconnaissance

Reconnaissance starts with internet search engines and information gathering about organization as a whole. Next, public web sites that exist for information look-up and data mining as well as public registries and authoritative bodies are consulted and specific information is gathered and cataloged. Powerful interconnection of organizational Domain Name System (DNS) servers and the DNS servers themselves are probed for configuration concerns. Port scanning, fingerprinting, and network mapping techniques are utilized to build a system and network profile, and a complete target list is compiled from all the information gathered during the phase.

Vulnerability Identification

Each host and all associated listening service to be targeted for the test are probed, singularly and in tandem with the other hosts to locate potential vulnerabilities. Using a large working knowledge of exploit techniques, public information, and results of private vulnerability research, the Ingram Micro SOC consultants catalog all the potential attack vectors.

Vulnerability Exploitation

All vulnerabilities found are manually investigated and researched, and an attempt is made to exploit. In exploiting vulnerabilities, Ingram Micro SOC has made an attempt to either gain unauthorized access to the target system or extract sensitive data from it. An exploit is considered successful if we were able to achieve either of those objectives.

Scanning Results & Recommended Action

Vulnerability Scoring

Common Vulnerability Scoring System (CVSS) is where appropriate; vulnerabilities are assigned a score ranging from 0 to 10, based on the Common Vulnerability Scoring System, version 2 (CVSSv2). CVSSv2 is the emerging security-industry standard for scoring the severity of vulnerabilities and provides a consistent algorithm for assessing the severity of a vulnerability. Ingram Micro SOC uses the CVSSv2 Base Score, which is comprised of six factors, as follows:

Base Metric Group

Access Vector

Confidentiality Impact

Access Complexity

Availability Impact

Authentication

Integrity Impact

Results

For the purpose of this test, Ingram Micro granted unauthorized access to a target system list, but not limited to the following, were:

- Ability to run commands on the target
- Legit bypass
- Successful credential theft
- Successful privileges

A summary of any system or device compromised below. Also documented are the additional attack vector upon the successful results.

Penetration Testing				
High	Medium	Low	Information	
1	2	0		0

Recommendations

It is highly recommended that ABC should various remediation recommendations it should also consider performing a test.

The critical areas that require immediate

3

Sample PT Reports

N.I.R.A.M			
#	Severity	Vulnerability	Remediation Action
1	H	Obsolete Web Server Detection	According to its version, the remote web server is obsolete and no longer maintained by its vendor or provider. Upgrade to a newer version or switch to another server. CVSS Base Score: 7.5 CVSSBase/N/A/C/L/Au/N/C/P/A/P#
2	M	Web Server Uses Plain Text Authentication Forms	Main user is CVSS 6 CVSS2
3	L	Multiple Ethernet Driver Frame Padding Information Disclosure	The ethernet is not medium buffer ethernet, so the ethernet is not medium buffer ethernet. CVSS 6 CVSS2
4	L	Device Type	Basic device

N.I.R.A.M			
#	Severity	Vulnerability	Remediation Action
1	H	Remote Could Allow Remote Code Execution	http://www.microsoft.com/technet/security/bulletin/MS08-038.aspx CVSS Base Score: 10.0 CVSSBase/N/A/C/L/Au/N/C/C/C/A/C
3	M	Microsoft Windows SMB Shares Unprivileged Access	Share access should be given on need to know basis. CVSS Base Score: 7.5 CVSSBase/N/A/C/L/Au/N/C/P/A/P
4	M	Microsoft Windows SMB Guest Account Local User Access	In the group policy change the setting for 'Network access: Sharing and security model for local accounts' from 'Guest only - local users authenticate as Guest' to 'Classic - local users authenticate as themselves'. CVSS Base Score: 5.0 CVSSBase/N/A/C/L/Au/N/C/P/A/N/A/N
5	L	Domain user Enumeration is possible	Disable null session on server
6	L	IS server is installed with default web page	Its recommended to disable all unnecessary ports

N.I.R.A.M			
#	Severity	Vulnerability	Remediation Action
1	H	Vulnerability in DNS Resolution Could Allow Remote Code Execution	Update Windows Patches Immediately. http://www.microsoft.com/technet/security/Bulletin/MS11-030.mspx CVSS Base Score: 10.0 CVSSBase/N/A/C/L/Au/N/C/C/C/A/C
2	M	LDAP NULL BASE Search Access	If the remote LDAP server supports a version of the LDAP protocol before v0, consider whether to disable NULL BASE queries on your LDAP server. CVSS Base Score: 5.0 CVSSBase/N/A/C/L/Au/N/C/P/A/N/A/N
3	L	Microsoft Windows SMB NULL Session	Disable null session on server



Cyber Security Trainings



Training Suite



FOUNDATIONAL TRAINING

1. Fundamentals of Information Security
2. CyberSAFE: Securing Assets for the End User

RISK MANAGEMENT

1. Fundamentals of a Formal ISRA
2. NIST SP 800-30
3. OCTAVE
4. ISO 27005

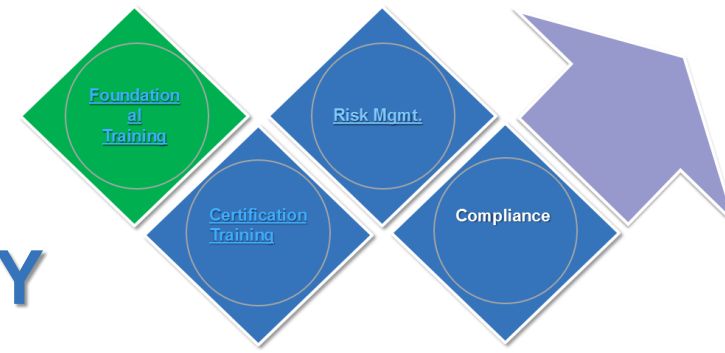
CERTIFICATION TRAINING

1. Cyber Security First Responder
2. CompTIA® N+
3. CompTIA® S+
4. CASP
5. CISSP

COMPLIANCE

1. PCI DSS and Payment Card Security
2. ISO 27001

Training Suite: Foundational Training



1. FUNDAMENTALS OF INFORMATION SECURITY

Key Takeaways:

- Basic tenets of information security
- Why Information Security matters
- How to implement basic security practices
- Case study and Hands-on workshop

Who Will Benefit:

- Technology users with a basic understanding of technical concepts

Course Duration: 1 day

2. CYBERSAFE: SECURING ASSETS FOR THE END USER

Key Takeaways:

- The need for information security
- Securing end-point devices such as laptops, desktops, mobile devices, etc.
- Secure use of the internet

Who Will Benefit:

- Basic users of desktops, laptops, tablets, mobile devices for activities including web browsing and email

Course Duration: ½ day

Training Suite: Certification Training



1. CYBER SECURITY FIRST RESPONDER (CFR)

Key Takeaways:

- A comprehensive approach to security
- Correct incident response mechanism

Who Will Benefit:

- Cyber Security Professionals who monitor and detect security incidents

Course Duration: 5 days

2. CompTIA® ADVANCED SECURITY PRACTITIONER (CASP)

Key Takeaways:

- Enterprise security, risk management and incident response,
- Research and analysis
- integration of computing, communications and business disciplines
- Technical integration of enterprise components

Who Will Benefit:

- IT professionals with strong knowledge of security

Course Duration: 5 days

Training Suite: Certification Training



3. CompTIA® SECURITY PLUS (S+)

Key Takeaways:

- Implementation, management, monitoring and troubleshooting of security as it spans across infrastructure, applications and operations

Who Will Benefit:

- Technology professionals who wish to further their IT career by acquiring foundational knowledge of security

Course Duration: 5 days

4. CompTIA® NETWORK PLUS (N+)

Key Takeaways:

- Configuration, management, and troubleshooting of common wired and wireless network devices

administration and/or support.

Course Duration: 5 days

Who Will Benefit:

- Entry-level technology professionals who wish to increase their knowledge of networking and acquire the skills to required for a career in network

Training Suite: Certification Training



5. CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL (CISSP)

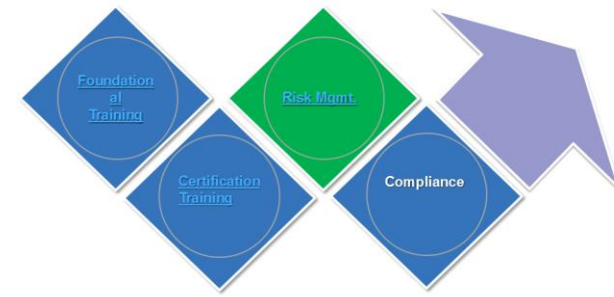
Key Takeaways:

- Identification and reinforcement of the 8 domains of Course Duration: 5 days the (ISC)2 CISSP CBK

Who Will Benefit:

- Advanced technology/information security professionals including auditors, security consultants, risk managers, network security engineers

Training Suite: Risk Management



1. FORMAL INFORMATION SECURITY RISK ASSESSMENT

Key Takeaways:

- The role of information security risk assessment in securing an enterprise
- How to do a formal information security risk assessment
- Case study and Hands-on Workshop

Who Will Benefit:

- Information risk professionals, information assurance professionals, auditors, pen-testers, incident responders, etc.

Course Duration: 5 days

2. RISK ASSESSMENT AS PER NIST SP 800-30

Key Takeaways:

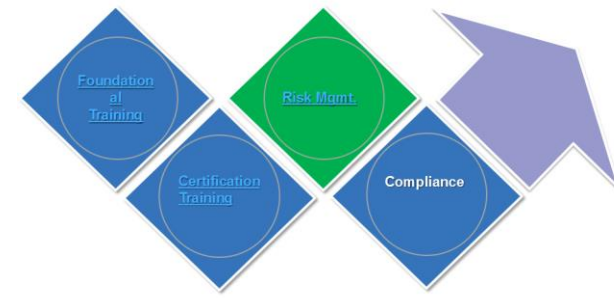
- Fundamentals of information security risk assessment
- How to do a formal information security risk assessment as per the NIST SP 800-30 methodology
- Case study and Hands-on Workshop

Who Will Benefit:

- Information risk professionals, information assurance professionals, auditors, pen-testers, incident responders, etc.

Course Duration: 5 days

Training Suite: Risk Management



3. RISK ASSESSMENT AS PER ISO 27005

Key Takeaways:

- Fundamentals of information security risk assessment
- How to do a formal information security risk assessment as per the ISO 27005 methodology
- Case study and Hands-on Workshop

Who Will Benefit:

- Information risk professionals, information assurance professionals, auditors, pen-testers, incident responders, etc.

Course Duration: 2 days

4. RISK ASSESSMENT AS PER OCTAVE

Key Takeaways:

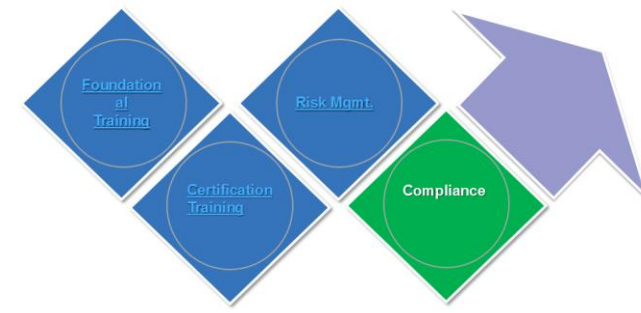
- Fundamentals of information security risk assessment
- How to do a formal information security risk assessment as per the OCTAVE methodology
- Case study and Hands-on Workshop

Who Will Benefit:

- Information risk professionals, information assurance professionals, auditors, pen-testers, incident responders, etc.

Course Duration: 2 days

Training Suite: Compliance



1. PCI DSS

Key Takeaways:

- Fundamentals of payment card security
- The 12 PCI DSS Requirements
- Common challenges in implementation
- Critical success factors
- Case Study and Hands-on workshop

Who Will Benefit:

- Information risk professionals, information assurance professionals, auditors, individuals who process card information

Course Duration: 2 days

2. ISO 27001

Key Takeaways:

- Fundamentals of an ISMS
- ISO 27001 Controls
- Common challenges in implementation
- Critical success factors
- Case study and Hands-on Workshop

Who Will Benefit:

- Information risk professionals, information assurance professionals, auditors, individuals who process card information

Course Duration: 2 days

Ingram Micro - Global Leader in Technology & Supply Chain Services

**\$50
Billion**

In revenue

200,000 Customers & 2,000 Vendors

500 Million

units shipped per year

19.6M+

Sq. Ft across

125 logistic centers

& **35** Service centers

Operations in

52 Countries with

32,000 + associates covering

6 continents

Top **10** Global Supplier

Handling

1 of 3

mobile devices in U.S.

1/3

of the Top Telcos

Only distributor with
certification

ISO 37001:2016

Ingram Micro Strategy – Accelerating Digital Transformation



Cyber Security



Physical Security



IoT



AI & Machine Learning

Will drive Growth in



Data Center



Enterprise Network



Enterprise Software

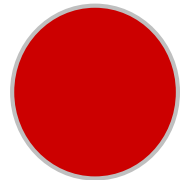


Cloud Technology

INGRAM MICRO[®] **SECURITY**

Expert *People* Dedicated to You

EMEA Security Next Centers Of Excellence (COEs)



COE covering Western Europe
in Netherlands (Utrecht)



COE covering Central + East
Europe in Belgrade

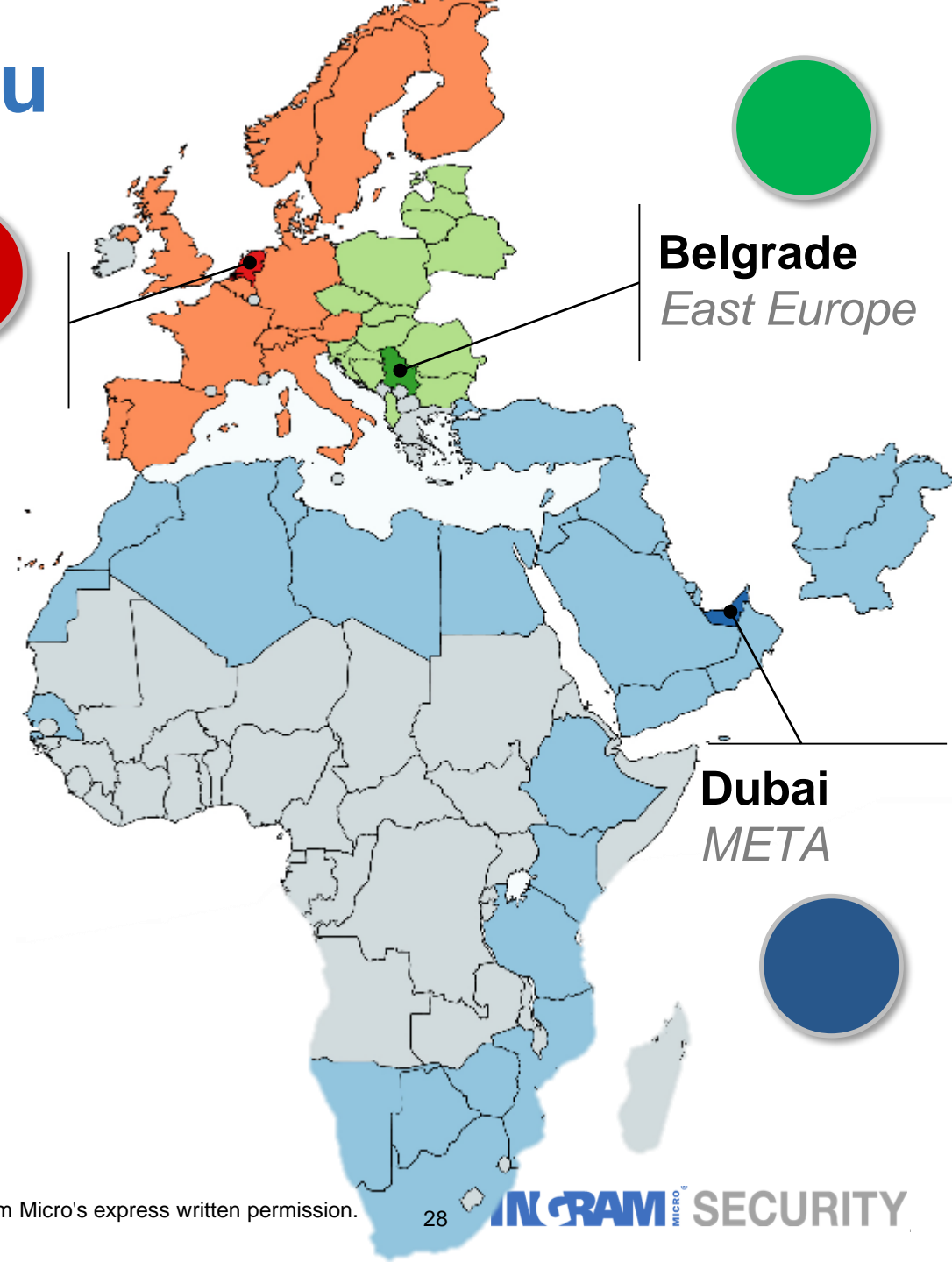


COE covering META (Dubai)

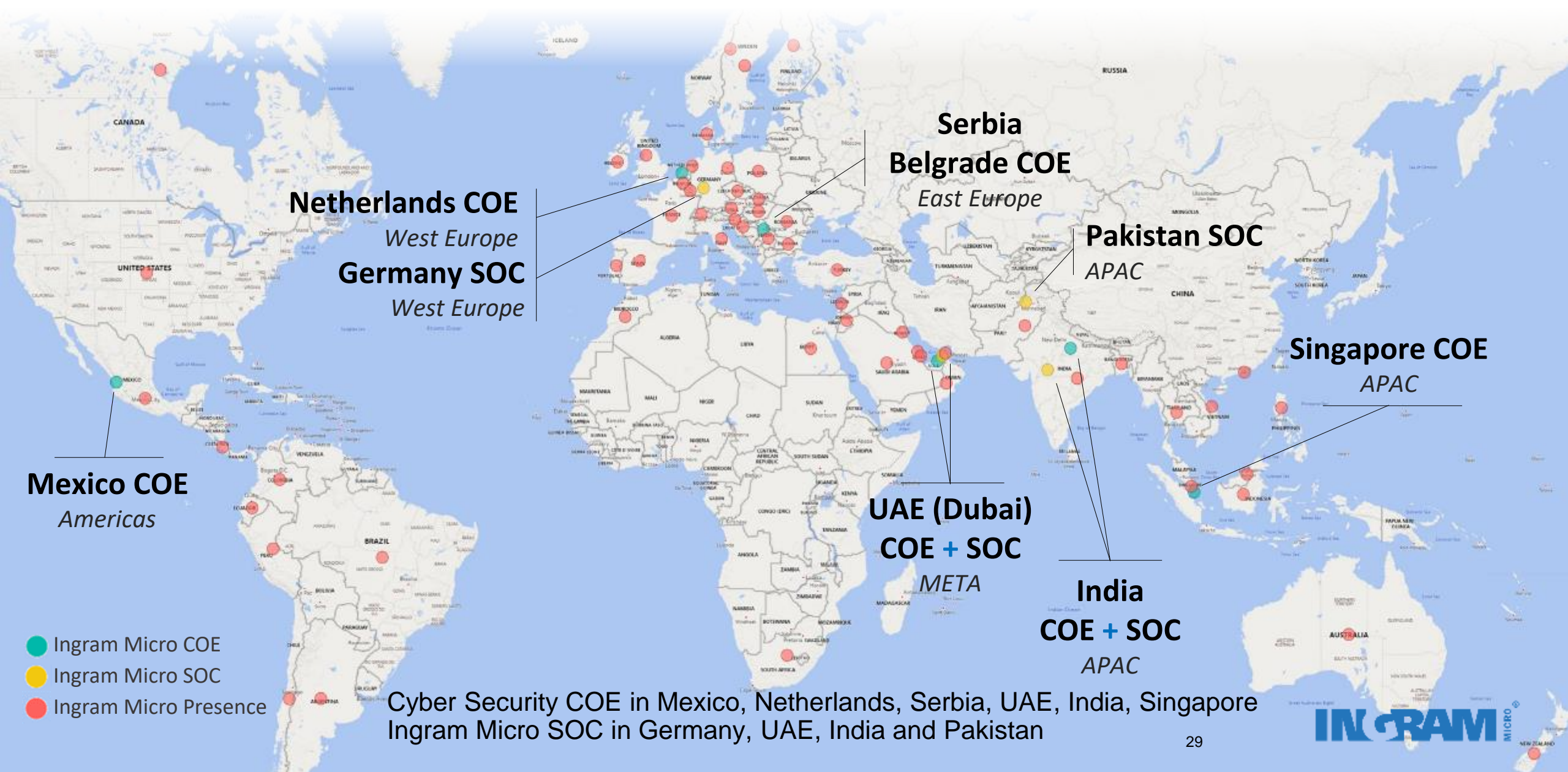
Netherlands
West Europe

Belgrade
East Europe

Dubai
META



Global Team of Security Experts Ready to Serve



Security *n*EXT Proven Partner GTM *Process*



Security *n*EXT Solutions for Cyber Security Leaders

Ingram Micro gives you the advantage of the best people, processes and technology to take your Cyber Security practice to the next level

PEOPLE

CYBER SECURITY TRAININGS



**Foundational
Trainings**



**Advanced Cyber
Security Trainings**



**Privacy Training
(GDPR)**

PROCESS

CYBER SECURITY SERVICES



**Technical
Assessments**



Consulting Services





**Managed Security
Services**

TECHNOLOGY

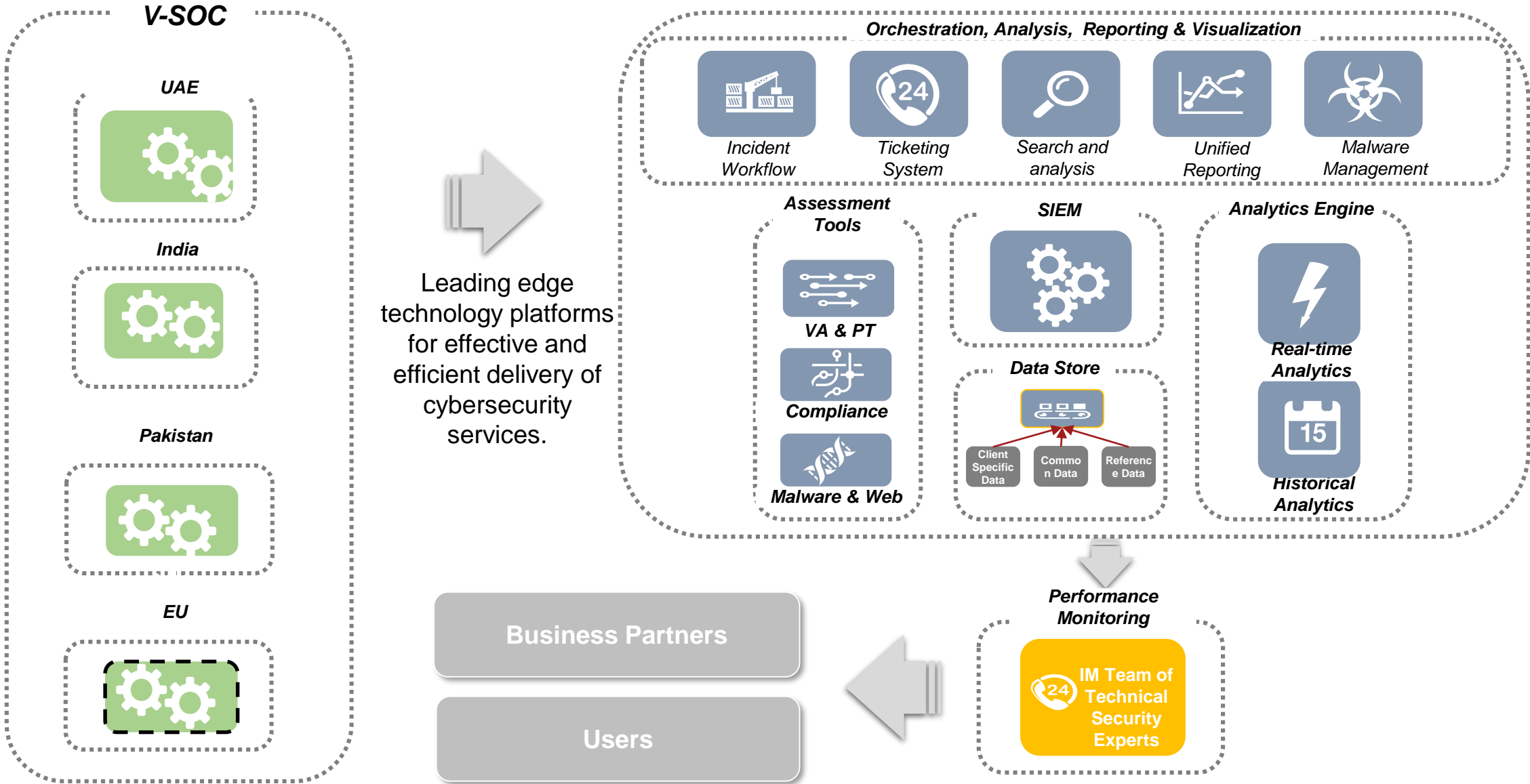
CYBER SECURITY VENDORS



Security *n*EXT Trainings Portfolio Built for Partners

FOUNDATIONAL TRAININGS	CERTIFICATION TRAININGS	RISK AND COMPLIANCE	EMERGENT TECHNOLOGIES	PRIVACY (GDPR)
Fundamentals of Cyber Security	CISSP	Risk Assessment as per NIST SP 800-30	IoT and Cyber Security	CIPP/Europe 
CyberSAFE	CompTIA Security+	Risk Assessment as per OCTAVE	Blockchain and Cyber Security	CIPM 
Fundamentals of Information Risk	CompTIA Network+	PCI DSS and Payment Card Security	Artificial Intelligence and Cyber Security	Privacy Legislation in the UAE
	CASP	ISO 27001 Compliance		GDPR Foundations
	CyberSec First Responder	NESA, ISR, ADSIC compliance		GDPR Implementation

Security *n*EXT Ingram Micro Virtual Security Operation Center



Security *n*EXT Services Portfolio Built for Partners

Technical Assessments

DATA

- Public Discovery Scan
- Database Security Assessment
- Digital Forensics

APPLICATION

- Source Code Review
- Web App Assessment
- Web Malware Detection
- Mobile App Assessment

DEVICE

- Vulnerability Assessment
- Configuration Review

NETWORK

- Network Architecture Review
- Network Audit
- Penetration Testing (Black box & White box)

Consulting

GOVERNANCE

- Information/Cyber Security Strategy
- Information/Cyber Security Operating model
- Data Classification
- Information/Cyber Security Policies + Procedures

RISK

- Risk Assessment

COMPLIANCE

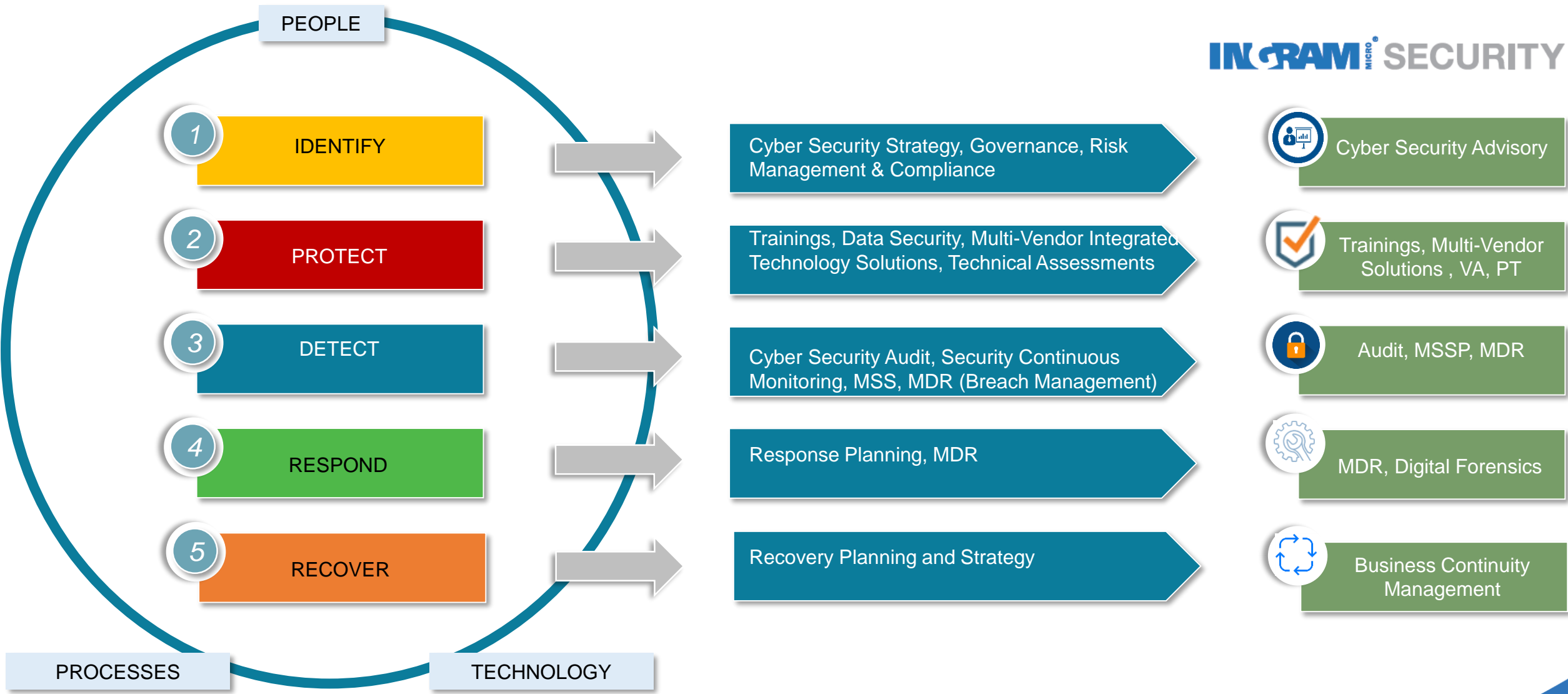
GDPR, ISO 27001, PCI DSS, NIST SP 800-30, NESAC, ISR, ADSIC, SAMA

- Information Security/Cyber/IT Audit
- Gap Assessment
- Remediation Support
- Certification Assistance

Managed Security Services

- Compliance Monitoring
- Log Management
- Intrusion Detection
- Incident Response
- Threat Intelligence
- Threat Hunting
- Fraud Monitoring
- Malware Protection
- Digital Forensics
- SOC Advisory

Security *n*EXT Solution Portfolio



INGRAM MICRO SECURITY

Security *n*EXT Tools & Own Products

1

Discovery Report

2

CyberGram - Ingram Micro Cyber Security Self Assessment Tool

3

Ingram Micro Virtual Lab

4

Security Awareness Tools: Trainings & Videos

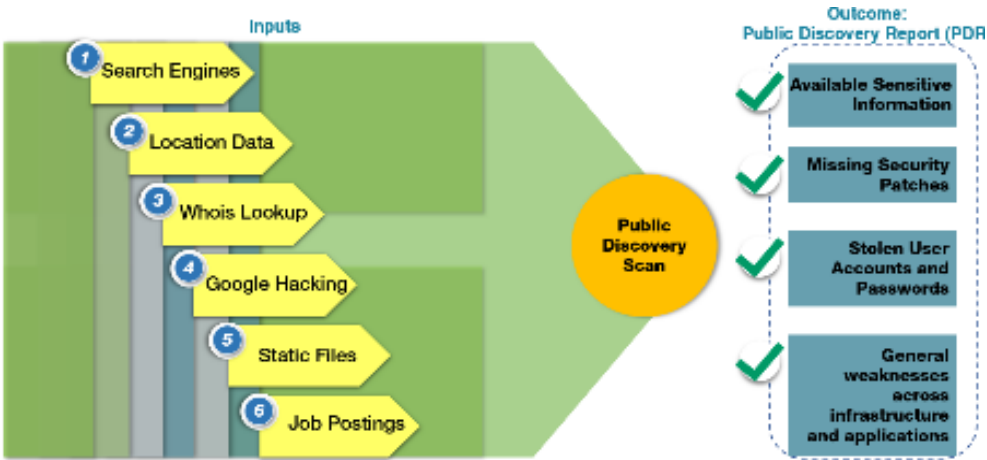
5

Security Bundles

6

Multi-Vendor Solution

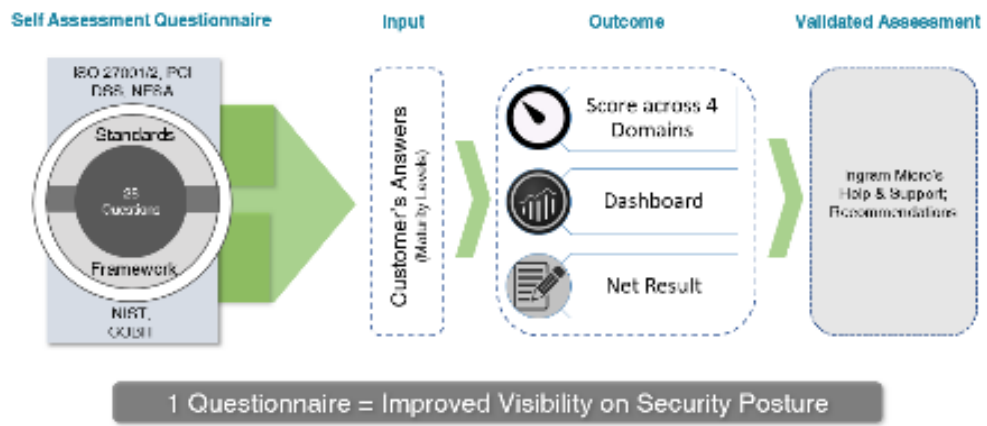
Security *n*EXT Technology Tools Built For You



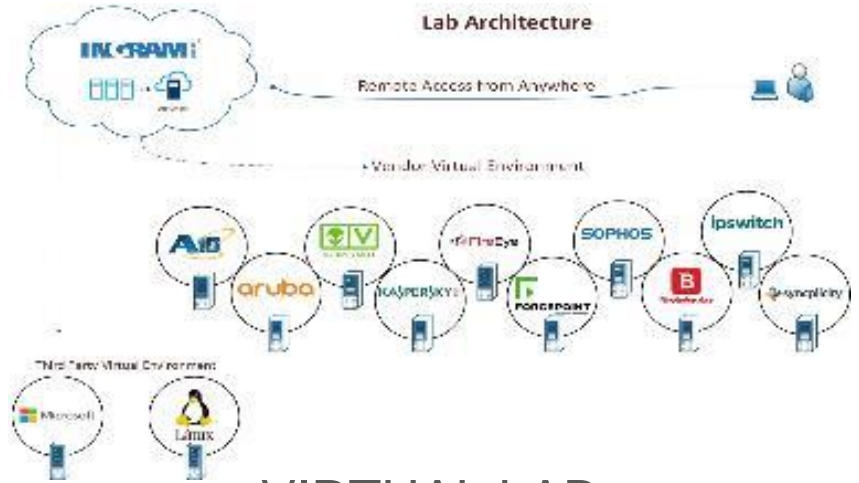
1 DISCOVERY REPORT



4 SECURITY AWARENESS TRAININGS



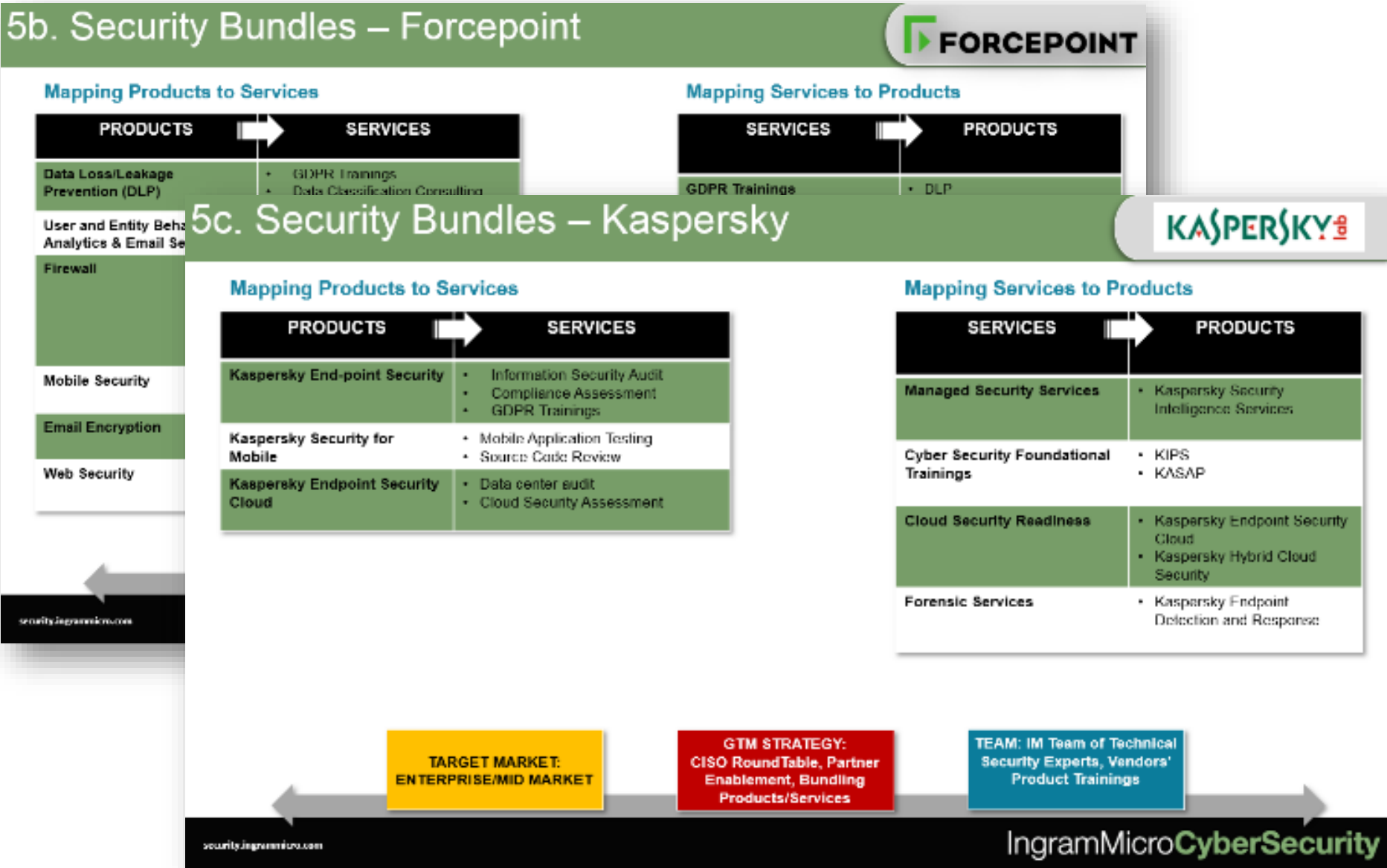
2 CYBERGRAM



3 VIRTUAL LAB

5. Security Bundles – Samples

- 1 Forcepoint
- 2 Kaspersky



6. Multi-Vendor Solutioning

