Cryptographic Agility Management

DISA Briefing

Julien Probst – CCO & Head of Products

Vladimir Soukharev – VP Cryptography

Philip George – Executive Technical Strategist, InfoSec Global Federal

07 February 2024

Briefing | Agenda

- **InfoSec Global Company Summary**

- **AgileSec Platform | Cryptographic Management**
  - Cryptographic Discovery
  - Cryptographic Control

- **Product Demonstration**

- **Q&A**

ISG BRIEFING

Company Summary

INFOSEC GLOBAL

Company | Background

Global **Operations**	🇨🇭 **Switzerland** Zurich	🇨🇦 **Canada** Toronto	🇺🇸 **United States**	🇸🇬 **Singapore**

Strong **References**	**Finance**	**Enterprises**	**Government**	**Technology**	**OEM & IOT**

Strategic **Ecosystem**	merlin cyber	Microsoft	TANIUM	CROWDSTRIKE	SYNOPSYS
	aws	THALES	ENTRUST	accenture	VENAFI
	MARVELL	RUAG	IDQ	utimaco	SCION ELEVATING SECURE COMMUNICATION

Offering
Crypto Agility Management

Discover	AgileSec **Analytics**
Control	AgileSec **Management**

Validated

NIST

NCCoE
NATIONAL CYBERSECURITY
CENTER OF EXCELLENCE

FIPS VALIDATED 140-2

AICPA SOC
aicpa.org/soc4so
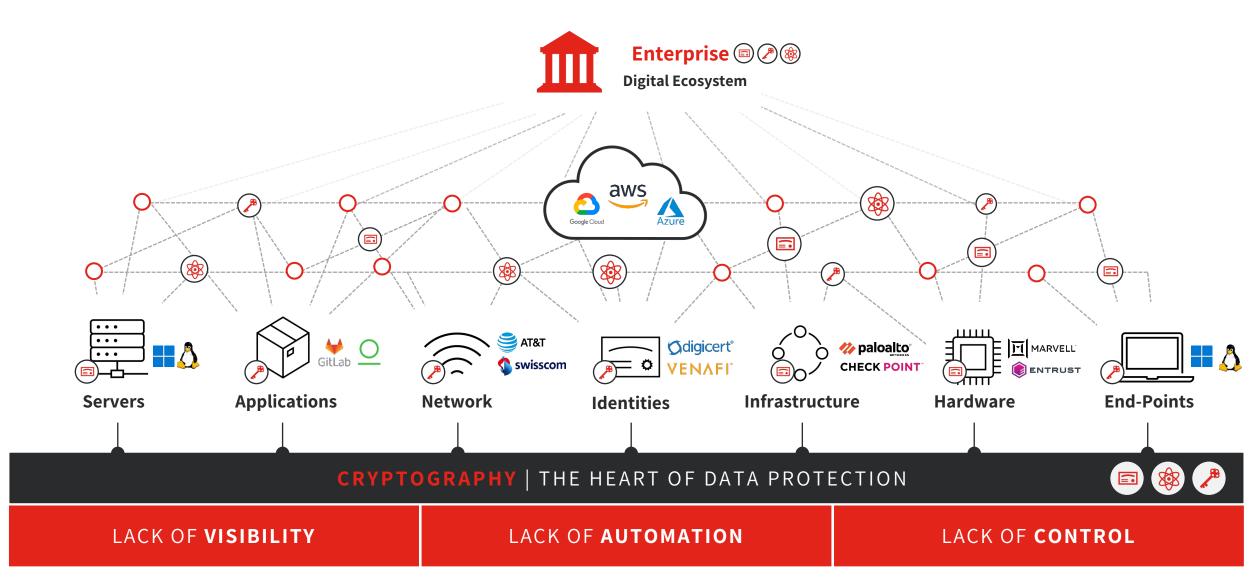
Quantum-Safe Canada

INFOSEC GLOBAL

Problem | Cryptography is Hidden Everywhere

Enterprise Digital Ecosystem

Servers Applications Network Identities Infrastructure Hardware End-Points

CRYPTOGRAPHY | THE HEART OF DATA PROTECTION

LACK OF **VISIBILITY**   LACK OF **AUTOMATION**   LACK OF **CONTROL**

INFOSEC GLOBAL

merlin cyber

5

ISG BRIEFING

The Platform

INFOSEC GLOBAL
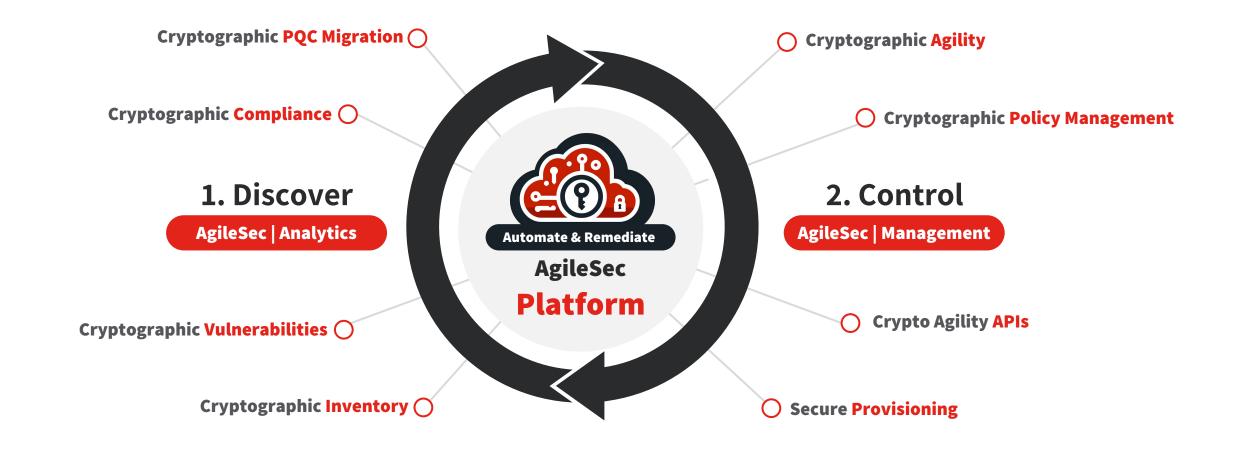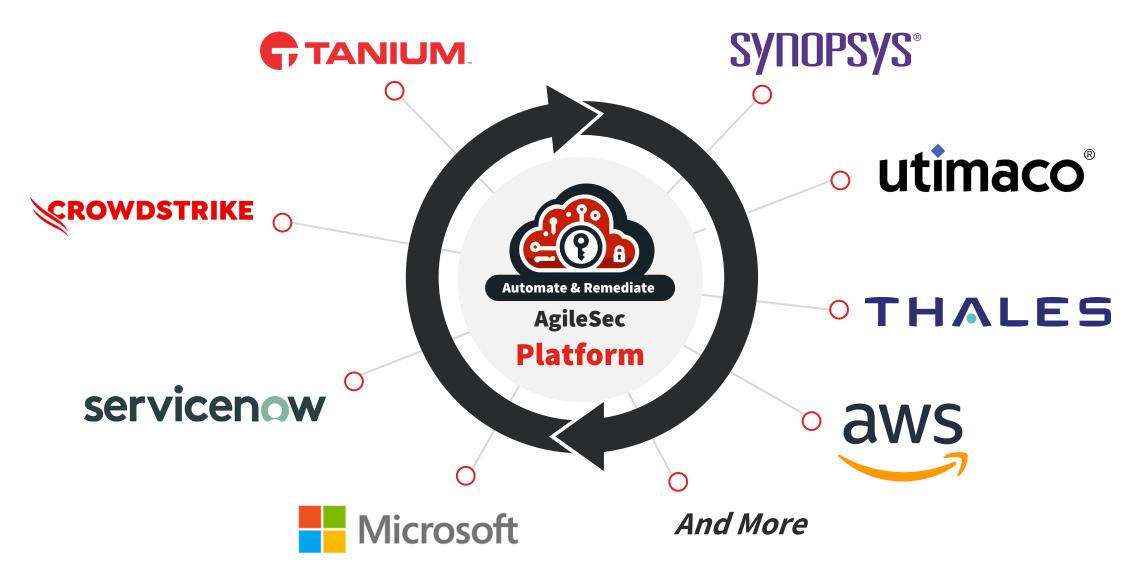
Vision | Part of the Ecosystem

TANIUM

SYNOPSYS®

utimaco®

CROWDSTRIKE

Automate & Remediate

AgileSec
Platform

THALES

servicenow

aws

Microsoft

And More

INFOSEC GLOBAL

merlin cyber

ISG BRIEFING

Cryptographic Discovery

AgileSec Analytics

INFOSEC GLOBAL

Discover | AgileSec Analytics

Discover
Cryptography Ecosystem

Hosts Environment

CI/CD Environment

Network Environment

HSM Environment

KMS Environment

Identities Environment

Other

Analyze
Cryptographic Compliance, Security & Correlation

INFOSEC GLOBAL

Cryptographic Discovery

Cryptographic Security Score

■ PQC Ready ■ Secure ■ Weak ■ Insecure

Hosts
Apps
Vaults
Others

75/100
Crypto Health

Algorithms   Protocols   Libraries   Keys   Certificates

Automate
Cryptographic Processes

Compliance

Response

CMDB

And More

Sample Integrations

Crowdstrike | ServiceNow | Artifactory | Gitlab | Github | Venafi | Thales CTM* | Azure Vault | Ansible | Entrust | Tanium | Windows | RedHat | Others
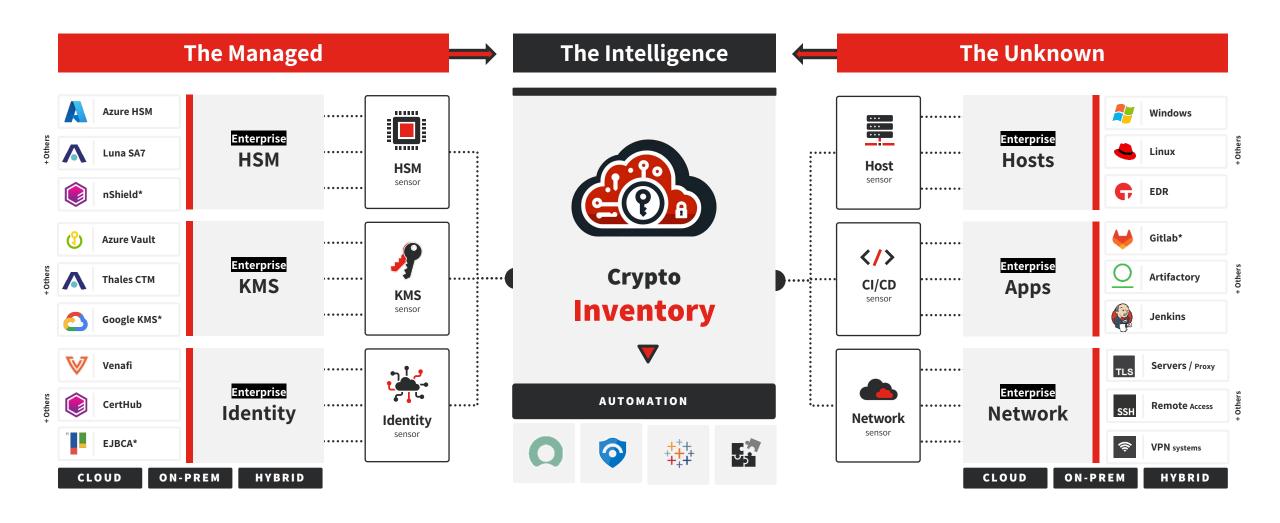
Which systems to include in a **cryptographic discovery**?

INFOSEC GLOBAL

Discover | Create Centralized Inventory

The Managed → **The Intelligence** ← **The Unknown**

The Managed

- Azure HSM
- Luna SA7
- nShield*
+ Others

Enterprise **HSM**

- Azure Vault
- Thales CTM
- Google KMS*
+ Others

Enterprise **KMS**

- Venafi
- CertHub
- EJBCA*
+ Others

Enterprise **Identity**

HSM sensor
KMS sensor
Identity sensor

CLOUD · ON-PREM · HYBRID

The Intelligence

Crypto **Inventory**

AUTOMATION

The Unknown

Host sensor
CI/CD sensor
Network sensor

Enterprise **Hosts**
- Windows
- Linux
- EDR
+ Others

Enterprise **Apps**
- Gitlab*
- Artifactory
- Jenkins
+ Others

Enterprise **Network**
- TLS Servers / Proxy
- SSH Remote Access
- VPN systems
+ Others

CLOUD · ON-PREM · HYBRID

INFOSEC GLOBAL

merlin cyber

13

How to **seamlessly** perform a cryptographic discovery in a **complex infrastructure**?

INFOSEC GLOBAL

Ecosystem | Integration

Complex Large-Scale Infrastructure

Option #1	Option #2	Option #3	Option #4
EDR Tools Integrated	**Native Host**	**Network**	**API Based**
Sensor	Sensor	Sensor	Sensors
CROWDSTRIKE TANIUM			

Cryptographic Inventory

CUSTOM DATA INGESTION & SENSORS

INFOSEC GLOBAL

merlin cyber
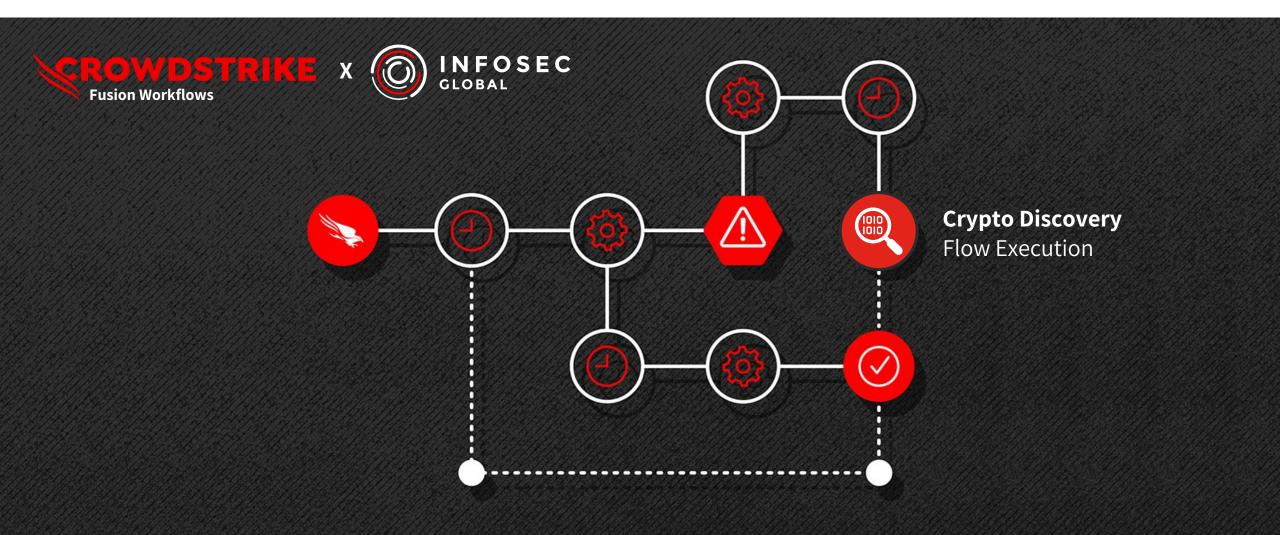
Integration | Crowdstrike

Crypto Discovery
Flow Execution
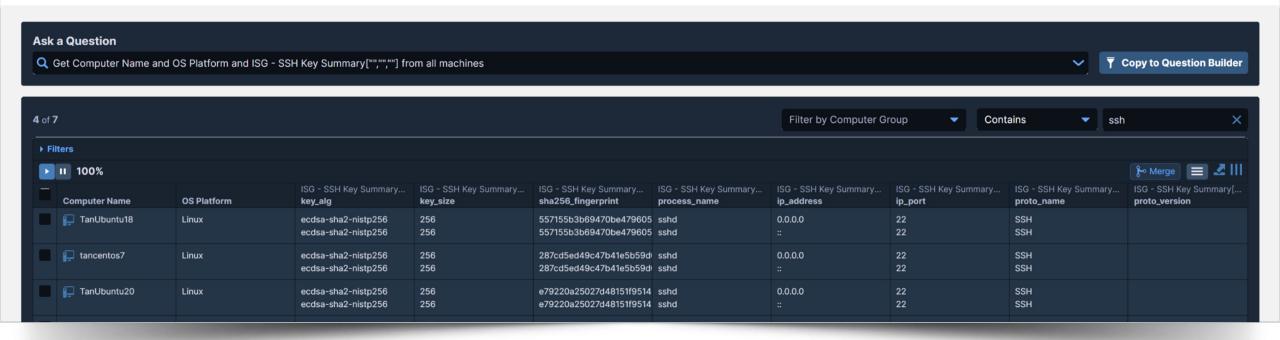
Integration | Tanium

Leverage ISG Scanning Capabilities as part of Tanium Questions

What cryptographic objects shall be **part** of an **inventory**?

INFOSEC GLOBAL

Inventory | Build Centralized Crypto Inventory (CBOM)

SSH Inventory
- Private SSH Keys
- Public SSH Keys

Keys Inventory
- Private Keys
- Public Keys

Keystores Inventory
- Private Key Stores

Locations
- File System
- Running Process
- Certificate Store
- Network Interface
- Repository

Certificates Inventory
- Root CA
- Intermediate CA
- SSL / TLS
- Personal Certificate
- S/MIME Encryption
- Digital Signing
- Time Stamping

Crypto Libs Inventory
- Classical Libraries
- PQC Ready Libraries

Algorithms Inventory
- Classical Algorithms
- Post-Quantum Algorithms

Ciphers Inventory
- Crypto Protocols
- Cipher Suites

INFOSEC GLOBAL

merlin cyber
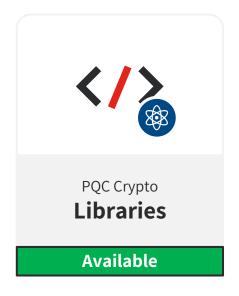
Inventory | PQC Cryptography

PQC Crypto **Libraries**	PQC Crypto **Certificates**	PQC Crypto **Keys**	PQC Crypto **Protocols**	PQC Crypto **Algorithms**
Available	**Draft**	**Draft**	**Draft**	**Available**
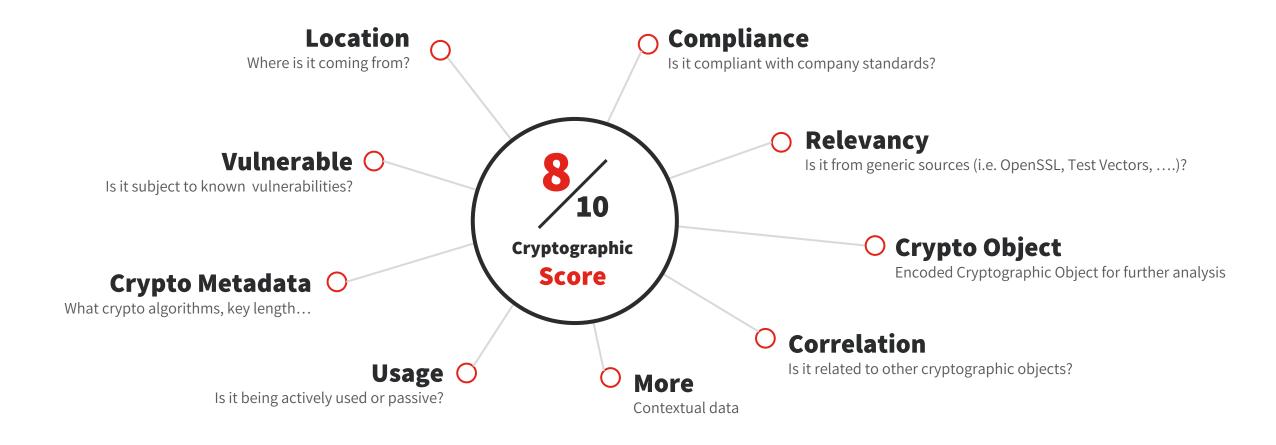
How to **navigate** and **prioritize** cryptographic findings?

INFOSEC GLOBAL

Prioritize | Cryptographic Score

Location
Where is it coming from?

Compliance
Is it compliant with company standards?

Relevancy
Is it from generic sources (i.e. OpenSSL, Test Vectors, ….)?

Vulnerable
Is it subject to known vulnerabilities?

8/10
Cryptographic **Score**

Crypto Object
Encoded Cryptographic Object for further analysis

Crypto Metadata
What crypto algorithms, key length…

Correlation
Is it related to other cryptographic objects?

Usage
Is it being actively used or passive?

More
Contextual data

1	2	3	4
Cryptographic Score **Does it Matter?**	Cryptographic Score **Is it a Risk?**	Cryptographic Score **Is it Priority?**	Cryptographic Score **What to Do?**

How to identify **misuse** and **relations** between cryptographic objects?

INFOSEC GLOBAL

Correlation | Cryptographic Dependencies

Finding // Instance

Server: **SV001** ☑

Finding // Instance

Server: **SV443** ☑

Finding // Instance

Server: **SV443** ⚠

Finding // Instance

Server: **SV021** ☑

Object
Root CA

Cryptographic
Correlation

Object
Private Key

IP: **10.0.0.120** ☑

Finding // Instance

Repo: **App001** ✕

Finding // Instance

Finding // Instance

HSM: **HM22** ☑

Repo: **App001** ⚠

Finding // Instance

INFOSEC GLOBAL

merlin cyber

24

How to report cryptographic vulnerabilities and compliance gaps ?

INFOSEC
GLOBAL

Vulnerability | Cryptographic Reporting

Cryptographic Dashboards

ISG PROFILE | CNSA 1.0 | CNSA 2.0 | CUSTOM

Cryptographic Severity

- Vulnerable
- Legacy
- Compliant
- PQC Ready

Evolution Monitoring

Time →

Cryptographic Policy

Cryptographic Policy	Source Type	Score
Broken Signature in Corporate Certificate	Host	High
Small Key Factor in Public SSH Key	Network	High
Leaked Private Key	CI/CD	High
30 days Expiring Corporate Certificate	Network	Medium
Duplicated RSA Private Keys	Host	Medium
[Custom] Missing Assignment	KMS	Medium
Post-Quantum X509 Certificate	Network	Low

INFOSEC GLOBAL

merlin cyber

26

How to report cryptographic **post-quantum priority**?

INFOSEC GLOBAL

Vulnerability | Cryptographic Reporting

| Now | 2,000 Logical Qubits | 4,000 Logical Qubits | 6,000 Logical Qubits | 12,000 Logical Qubits | 20,000 Logical Qubits |

| | ECC 256 broken | ECC 521 broken | RSA 2048 broken | RSA 3072 broken | RSA 8192 broken |

● Quantum Vulnerable   ● At Risk   ● Quantum Safe

INFOSEC GLOBAL

merlin cyber

Automate | Cryptographic Management Processes

AgileSec Analytics → CRYPTO VULNERABILITIES → ServiceNow Cryptographic Vulnerabilities → REMEDIATION → **Vulnerability Resolution**

Cryptographic Vulnerabilities

Third-Party Vulnerability Entries | ID | Search

Actions on selected rows...

All

ID	Summary	Risk score	Risk rating	Severity	Vulnerable items	Source
isg.certstore.certificate.self_signed_ce...	A certificate present in certstore is se...	74	2 - High	1 - Critical	20	ISG
isg.filesystem.certificate.certificate_b...	A certificate present in filesystem is b...	71	2 - High	1 - Critical	4	ISG
isg.certstore.certificate.expiring_certi...	A certificate present in certstore is ex...	54	3 - Medium	2 - High	2	ISG
isg.filesystem.private.key.weak_key_size	A private key present in filesystem is s...	74	2 - High	1 - Critical	15	ISG
isg.filesystem.end-entity.certificate.ex...	A end-entity certificate present in file...	54	3 - Medium	2 - High	5	ISG
isg.filesystem.cryptographic.library.lib...	A cryptographic library present in files...	54	3 - Medium	2 - High	10	ISG
isg.filesystem.public.key.weak_key_size	A public key present in filesystem is sm...	71	2 - High	1 - Critical	4	ISG
isg.filesystem.certificate.certificate_w...	A certificate present in filesystem is u...	71	2 - High	1 - Critical	9	ISG
isg.network.end-entity.certificate.expir...	A end-entity certificate present in netw...	54	3 - Medium	2 - High	4	ISG
isg.artifact.public.key.weak_key_size	A public key present in artifact is smal...	71	2 - High	1 - Critical	2	ISG
isg.filesystem.private.key.clear_text_ke...	A private key present in filesystem is s...	57	3 - Medium	2 - High	53	ISG
isg.artifact.private.key.clear_text_key_...	A private key present in artifact is sto...	54	3 - Medium	2 - High	3	ISG
isg.artifact.private.key.weak_key_size	A private key present in artifact is sma...	0	5 - None	1 - Critical	0	ISG
isg.filesystem.ca.certificate.certificat	A ca certificate present in filesystem i	74	2 - High	1 - Critical	25	ISG

INFOSEC GLOBAL

merlin cyber

30

Deployment | Flexibility, Scalability, Interoperability

Control | AgileSec Management

Control
Cryptographic Policy in Use

Manage
Cryptographic Policies, Algorithms, Keys and Settings

Integrate
Cryptographic Systems

Applications
AgileSec API

Network
AgileSec VPN

Custom
AgileSec API

INFOSEC GLOBAL

Cryptographic Management

Classical NIST | Policy

Key Agreement
DH-3072

Digital Signature
DH-3072

Symmetric Encryption
AES-128

Upgrading

Post-Quantum | Policy

Key Encapsulation Mechanism
KYBER-768

Digital Signature
SPHINCS+256

Key Agreement
AES-128

Key Management

Crypto Providers

Cloud Infrastructure

And More

Sample Integrations

| SYNOPSYS TRoot | Luna SA7 | Bouncycastle | OS OpenSSL | Future | StrongSwan | Wireguard | IDQ QKD |

Control | Integration

Integrations Systems

| Applications | Embedded | Services | Others |

Cryptographic Agility SDK

Agile Crypto API

Library Wrappers

Crypto Services

AgileSec Agility Core

Crypto Policy

Standard Providers
- ISG Classical
- OpenSSL

FIPS Providers
- ISG FIPS

PQC Providers
- ISG PQC
- LibOQS

Hybrid Providers
- ISG Hybrid

Hardware Providers
- HSM
- TEE
- PKCS#11

Sovereign Providers
- Custom

Bring your Own Providers
- Provider API

AgileSec Management

CONTROL

INFOSEC GLOBAL

merlin cyber

* In process

35

ISG BRIEFING

Closing

AgileSec Platform

INFOSEC GLOBAL

Q&A Session

Julien Probst
Chief Customer Officer & Head of Products

julien.probst@infosecglobal.com

Vladimir Soukharev
VP Cryptography

vladimir.soukharev@infosecglobal.com

Philip George
Executive Technical Strategist

pgeorge@isgfederal.com

Additional Information

Dave Diegtel

ddiegtel@merlincyber.com

www.infosecglobal.com | www.isgfederal.com

INFOSEC GLOBAL

merlin cyber