INFOSEC GLOBAL FEDERAL

Keys-in-the-Wild

Request an Inventory Pilot

How Storm-0558 Leveraged Misplaced Trust to Strike “Espionage Gold”

The Cyber Safety Review Board’s report on the Summer 2023 Microsoft Exchange Online Intrusion noted that the actor group Storm-0558, “struck the espionage equivalent of gold.” accessing cloud email accounts of, “many of the most senior U.S. government officials managing our country’s relationship with the People’s Republic of China.”

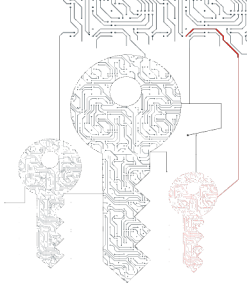
Pointing to the ubiquity of cloud systems, the CSRB further noted that the cloud is a “high-value target” for a range of advanced adversaries. But the question remains, was this a failure of the cloud or of a deeper problem with our ability to know and trust who has privileged access to our most sensitive systems?

Cryptographic assets, like signing keys or authentication tokens, are typically trusted because cryptography provides proof of their legitimacy. However, cryptographic keys by themselves do not equal trust. Storm-0558’s actions successfully demonstrated how damaging cryptographic keys can be when they exploited a Microsoft Services Account (MSA) key to issue their own authentication tokens. In the words of the CSRB a, “single key’s reach can be enormous, and in this case the stolen key had extraordinary power.” We call this a “Keys-in-the-Wild” problem, where unknown and invisible cryptographic keys can be leveraged by malicious actors to great effect.

If a Key Goes Missing in the Wild and No One is Looking, Can It Cause Damage? Yes.

Unfortunately, the “Keys-in-the-Wild” problem exists because there is little to no searching for unknown cryptographic assets. There are no cybersecurity controls, for example, that recommend scanning for keys-in-the-wild to find keys like the Storm-0558 key. Invisible, unprotected keys are the unknown, unknowns. One example of this visibility challenge extends into the use of Hardware Security Modules (HSMs). HSMs are a critical tool used to protect sensitive IT assets such as web servers or critical applications. Sometimes, existing cryptographic keys are transferred into HSMs. If the original key is not destroyed, as sometimes occurs by mistake, this may lead to duplicate pairs – one pair is safe in an HSM and the copy is outside the HSM, and the outside copy may be able to be exploited by a malicious adversary. This can be a very dangerous situation because the organization believes that the key pair is strongly protected and only exists inside an HSM when, in fact, that’s not the case and they are not scanning for duplicates to find the copy outside the HSM.

INFOSEC GLOBAL FEDERAL



Zero Trust Lessons from Storm-0558 to Avoid Keys-in-the-Wild

The Federal Zero Trust strategy mandates that agencies continuously validate every user and device seeking to access federal resources. This approach reduces cyber risk by assuming no implicit trust and requiring strict identity verification and access controls. When examined through the Zero Trust lens, the Storm-0558 intrusions give us a framework for identifying and eliminating Keys-in-the-Wild.

Credential Protection and Visibility

- **Zero Trust Principle:** Ensure that all credentials and cryptographic keys are protected and monitored for unauthorized access or exposure.
- **Lesson from Storm-0558:** The keys used by Storm-0558 may have been trusted, but obviously the espionage actor did not have authorization to use them and their access should have been detected. Unfortunately, it is not common practice to scan for cryptographic assets and as such, a key-in-the-wild can create a perfect and enormously powerful attack vector for authentication, digital signatures, or decryption. The failure to detect the presence of the Storm-0558 authentication key shows the need for effective secret scanning tools that can help identify keys in the wild in real time.
- *Agencies should deploy advanced secret scanning tools to continuously scan for exposed keys and credentials across all environments.*

Scope Validation and Access Control

- **Zero Trust Principle:** Implement strict scope validation and access controls to ensure that keys and credentials are used only within their intended contexts.
- **Lesson from Storm-0558:** The acquisition of the trusted MSA signing key enabled Storm-0558 to forge tokens and access email accounts without detection. This breach underscores the potential large scope of damage when trusted keys are used to validate unauthorized access requests.
- *Agencies should enforce rigorous validation checks to ensure keys are only used within their defined scopes and contexts.*

Continuous Cryptographic Monitoring

- **Zero Trust Principle:** Continuous monitoring and logging of all activities are critical to detect anomalies and unauthorized access attempts promptly.
- **Lesson from Storm-0558:** The undetected key leakage and difficulty in tracing the key's acquisition emphasize the need for robust, real-time monitoring and comprehensive logging. Continuous monitoring and auditing of cryptographic key usage is essential to detect and respond to unauthorized access attempts swiftly.
- *Agencies should employ advanced logging and monitoring tools to ensure full visibility into key usage and access patterns.*

Policy Enforcement and Continuous Compliance Monitoring

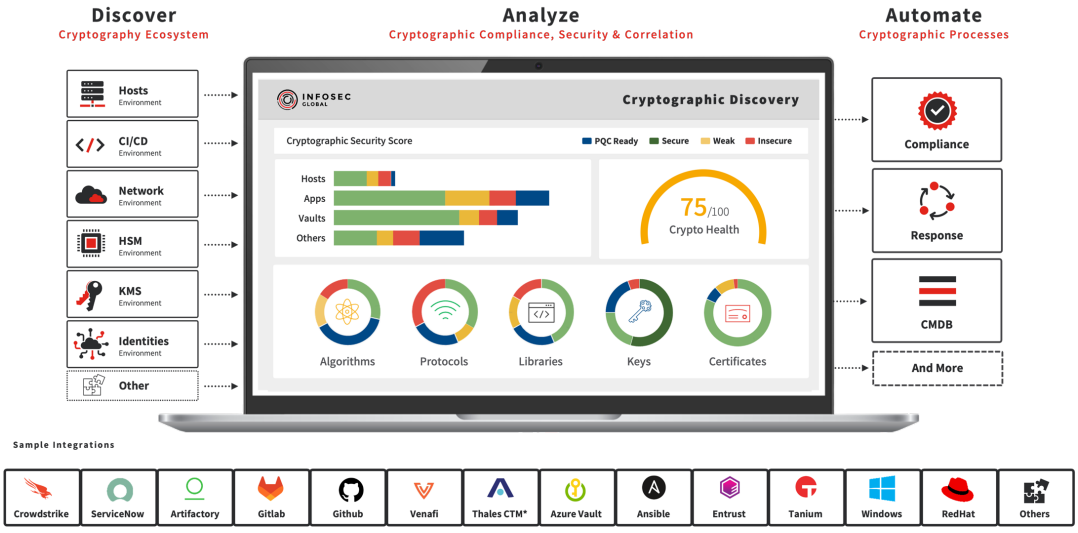
- **Zero Trust Principle:** Conduct continuous monitoring to ensure compliance with security policies and identify potential vulnerabilities.
- **Lesson from Storm-0558:** The incident underscores the need for regular, thorough audits to maintain compliance and enhance security measures.
- *Agencies should continuously monitor their key management and access control practices to ensure adherence to Zero Trust principles.*

Strong Key Management Practices

- **Zero Trust Principle:** Enforce least privilege principles for key management, including up-to-date encryption standards, and secure key storage.
- **Lesson from Storm-0558:** With no visibility into keys that were not stored securely, it was not possible to identify when they were misused.
- *Agencies should ensure secure key storage using up-to-date encryption standards while continuously monitoring for insecure keys that may be misused.*

InfoSec Global AgileSec™ Analytics Pilot for Federal Agencies

To combat the threat of Keys-in-the-Wild from being used by adversaries, InfoSec Global is piloting its AgileSec™ Analytics solution with Federal agency systems to discover, inventory, and analyze host devices in an agency's technology estate to identify keys that are not properly protected and potentially available to threat actors, whether insiders or external actors.

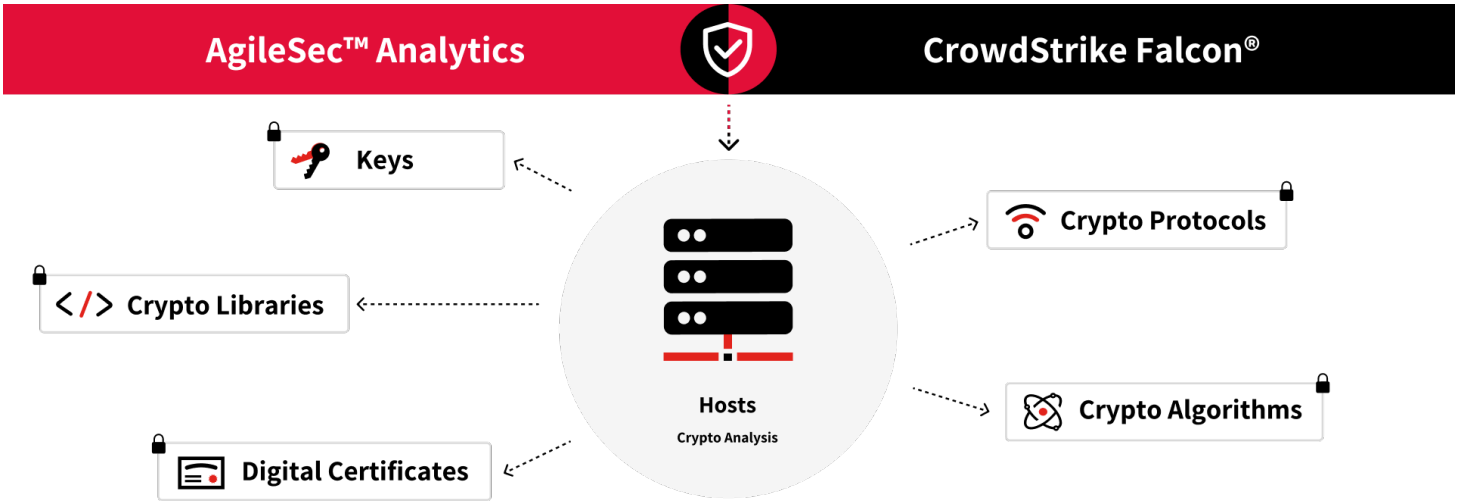


AgileSec Analytics is a cryptographic discovery and analysis solution that quickly, easily, and automatically generates an inventory of certificates, keys and cryptographic mechanisms found in software applications (source code and binary), libraries, hosts, and networks across the organization. It proactively hunts for hidden risks and vulnerabilities. AgileSec Analytics accelerates cryptographic compliance and postquantum readiness for enterprises, governments, and technology providers.

The cost of a pilot deployment is $50,000 for up to 250 host devices.

InfoSec Global and CrowdStrike Falcon

AgileSec™ Analytics integrates with the CrowdStrike Falcon® platform and leverages Falcon real-time response (RTR) to discover and retrieve cryptographic objects on hosts that are running the Falcon agent. With this context, AgileSec Analytics can identify cryptographic assets that pose a potential risk and enable the replacement of those assets to avoid any business disruption. With rich dashboards and customizable reports, AgileSec Analytics visualizes key metrics for cryptography security and compliance.



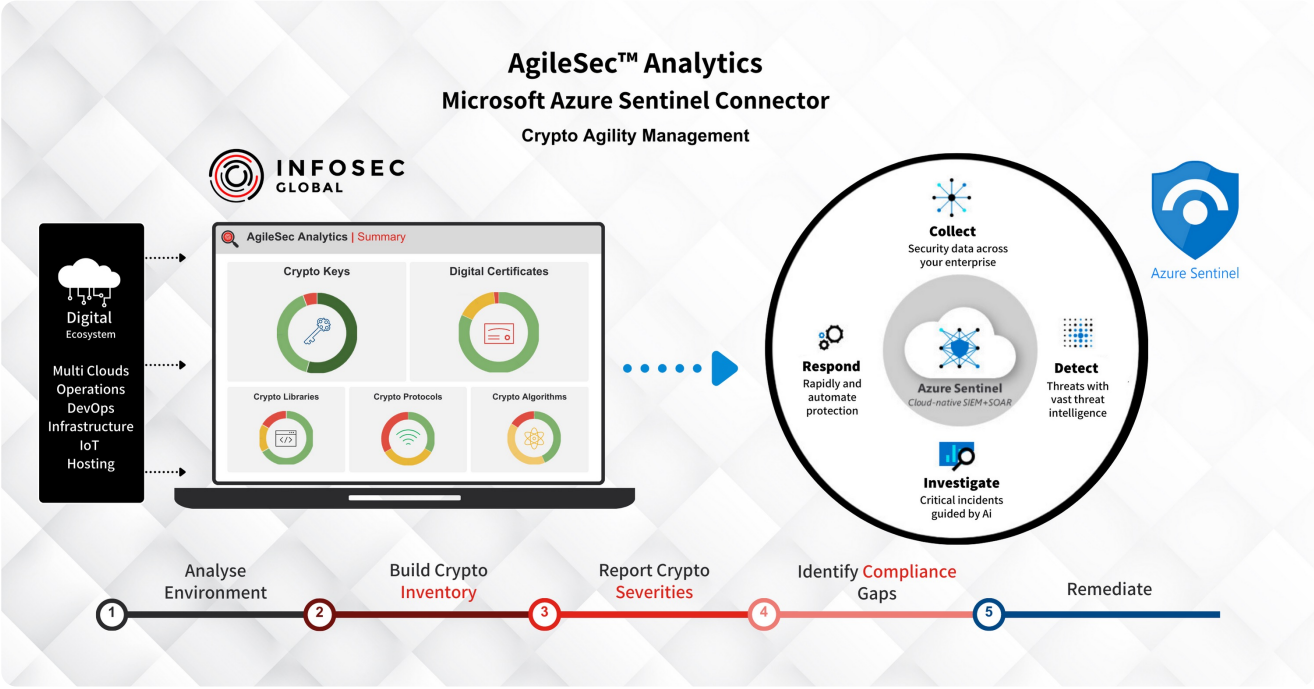
- **Complete Visibility:** Continuously scan and maintain inventory of cryptographic assets on hosts that are running the Falcon agent to minimize visibility gaps across your dispersed environment, preventing potential threat or compromise.
- **Rapid Remediation:** Enable replacement of non-compliant cryptographic assets across your devices.
- **Continuous Compliance:** Leverage rich dashboards and customizable reports to visualize key metrics and risks, helping ensure cryptography security and compliance.

For more information visit: https://marketplace.crowdstrike.com/listings/infosec-global-agilesec-analytics

INFOSEC GLOBAL FEDERAL

InfoSec Global and Microsoft Azure Key Vault Scanner

Microsoft Azure Key Vault serves as a robust safeguard for cryptographic keys and various sensitive secrets utilized by cloud applications and services. This versatile platform enables you to encrypt keys and small confidential information, such as passwords, all while ensuring these keys are securely stored within cloud-based hardware security modules (HSMs). It simplifies the administration of centralized application secrets, enables access, and use monitoring, improves performance, and reduces the latency of cloud applications. The AgileSec™ Analytics integration captures metadata about cryptographic objects in Azure Key Vault and executes comprehensive analytics to detect vulnerabilities.



- **Centralized Cryptographic Inventory:** Create a centralized inventory of certificates, secrets, and keys discovered within a digital ecosystem, including hosts, applications, network, key vaults, and others.
- **Identify Where Keys From Key Vault Are Used:** Correlate the data collected from multiple sources to automatically identify where the Keys that are present in Azure Key vault are used within a digital ecosystem.
- **Assess Vulnerabilities and Compliance Gaps:** Automatically identify cryptographic vulnerabilities, including weak or unprotected keys, and compliance gaps, such as usage of deprecated algorithms.
- **Post-Quantum Preparation:** Receive expert guidance regarding the management of cryptographic keys in preparation to migrate to post-quantum security.
- **Multi-Vault and Multi-Tenant Support:** Scan across multiple vaults and operate efficiently in multi-tenant Azure environments to generate consolidated, centralized visibility and analysis of cryptographic objects.
- **Dependency Insights:** Gain deep insights into how cryptographic material is used and identify the machines dependent on a specific key, facilitating smoother key rotation processes.

For more information visit: https://www.infosecglobal.com/posts/unveiling-infosec-global-microsoft-azure-service-integrations

Scanner InfoSec Global and Thales CipherTrust Manager

AgileSec™ Analytics enables organizations to discover cryptographic assets through integration with Thales CipherTrust Manager. This integration provides a comprehensive overview of cryptographic assets stored in HSMs, such as Thales' Luna HSM.

The Thales integration empowers organizations to effortlessly visualize keying material stored in HSMs, offering a sophisticated correlation of key usage across the entire ecosystem. This dynamic integration enhances security measures, streamlines key management processes, and ensures a unified approach to cryptographic control.

Moreover, AgileSec Analytics streamlines cryptographic discovery and key management processes by providing a centralized platform for discovering and correlating key information. This efficiency not only saves time and resources but also ensures a more proactive and strategic approach to cryptographic asset management. The seamless integration with Thales CipherTrust and Luna HSM delivers broad coverage and visibility, making it an indispensable asset for organizations seeking heightened security and efficiency in their cryptographic endeavors.

The integration of AgileSec Analytics with Thales encryption and key management products brings forth several compelling advantages:

- **Strengthened Security:** The integrated solution provides comprehensive visibility over an organization's cryptographic assets by seamlessly discovering and cataloging cryptographic assets in on-prem, cloud-native, or hybrid ecosystems. This heightened visibility reduces the risk of overlooking critical assets or potential vulnerabilities, thus fortifying overall security.
- **Streamlined Key Management:** Manual asset discovery and management methods are time-consuming and prone to human error. The integrated solution automates the entire process, thereby reducing administrative burdens and streamlining key management workflows, improving operational efficiency.
- **Enhanced Compliance:** Compliance with data protection regulations necessitates maintaining an accurate inventory of cryptographic assets. The integrated solution assists in meeting regulatory standards by providing an up-to-date record of keys and certificates, enabling smoother audits and compliance checks.

For more information visit: https://cpl.thalesgroup.com/encryption/enterprise-key-management

To find out more information about InfoSec Global's Keys-in-the-Wild pilot, please contact: **Troy Stark, Head of Sales, troy.stark@infosecglobal.com**

Sources

- https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdf
- https://msrc.microsoft.com/blog/2023/09/results-of-major-technical-investigations-for-storm-0558-key-acquisition/
- https://www.wiz.io/blog/key-takeaways-from-microsofts-latest-storm-0558-report
- https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf#:~:text=URL%3A%20https%3A%2F%2Fwww.whitehouse.gov%2Fwp
- https://www.cisa.gov/sites/default/files/2024-04/CSRB_Review_of_the_Summer_2023_MEO_Intrusion_Final_508c.pdf

INFOSEC GLOBAL FEDERAL

InfoSec Global Federal

InfoSec Global Federal is a cryptographic security company that specializes in providing next generation cryptographic discovery, agility, and management solutions from the silicon firmware up through end-point applications. Our secure software enables the management and agility of all cryptographic assets across a digital ecosystem, enabling government agencies to automate and orchestrate cryptography usage.

Notable Facts About InfoSec Global

- Technology validated by NIST as part of the NCCOE PQC Migration Initiative.
- Established track record in cryptographic agility management since 2014.
- Achieved **FIPS** and **SOC2** Compliance and Certifications.
- Co-Author of **SPHINCS+ (SLH-DSA)** a new PQC algorithm under standardization by **NIST**.
- Working with top-tier global customers in **finance**, **insurance**, and **technology** markets.
- Strong practical experience deploying **crypto-agility** & **crypto-discovery** in complex environments.
- Established strategic alliances with large **OEMs** and **Global** channel partners.
- Led by crypto legends (**'Father of SSL'**) and seasoned successful entrepreneurs.

Request an Inventory Pilot

Certifications

FIPS VALIDATED 140-2

AICPA SOC aicpa.org/soc4so

InfoSec Global USA (Federal)

8330 Boone Blvd
Floor 8
Tysons, VA 22182

InfoSec Global Canada

2225 Sheppard Avenue East
Suite 1402,
Toronto, Ontario
M2J 5C2 Canada

InfoSec Global Switzerland

Hardturmstrasse 103
8005 Zurich
Switzerland