PanoQoR™

Cryptographic Discovery & Inventory for Quantum Risk

PATERO
QUANTUM SECURE COMMUNICATIONS

We find encryption. We classify it. We score your risk.

Key Capabilities

Starting your transition to PQC with a partial inventory could cause disruption later. We inventory all five pillars.

CBOM (USING TECHNOLOGIES LISTED BELOW)

Reporting	All cryptographic components (keys, algorithms, protocols, certificates) are in use within the organization.
Identifies	• Detailed certificates with root and trust chain information • Crypto inventory and readiness • Cryptographic algorithms by device • Cryptographic algorithms by application • Cryptographic algorithms by operating system • Crypto algorithms by IP address

PANOQOR™

Cryptographic Discovery & Inventory for Quantum Risk

PATERO
QUANTUM SECURE COMMUNICATIONS

Identification of Encryption Protocols	**SYMMETRIC ENCRYPTION:** • AES (Advanced Encryption Standard). • DES (Data Encryption Standard) and 3DES (Triple DES). • RC4 and RC5 (although deprecated, they should still be identified). • Blowfish and Twofish. **ASYMMETRIC ENCRYPTION:** • RSA (Rivest-Shamir-Adleman). • ECC (Elliptic Curve Cryptography). • DSA (Digital Signature Algorithm). **HYBRID ENCRYPTION:** • Protocols like TLS (Transport Layer Security), which use a combination of symmetric and asymmetric encryption. • IPSec and SSL (Secure Sockets Layer).

Discovery and Classification of Cryptographic Keys	**Key Types:** The software identifies the following cryptographic key types: • Symmetric keys. • Public and private keys in asymmetric encryption. • Session keys used in TLS/SSL communications. • Key pairs used in digital certificates. **Key Storage:** Identify where cryptographic keys are stored (hardware, software, cloud), including: • HSM (Hardware Security Modules). • Keystores and software vaults. • Embedded keys in code or configuration files. **Key Strength:** Identifies key lengths (e.g., 2048-bit RSA, 256-bit AES) to ensure compliance with industry best practices. **Expired or Weak Keys:** The software flags keys that have expired or use deprecated encryption standards. **Endpoints:** identifies cryptographic material in use by discrete endpoints and enables the organization to determine the risk by endpoints. **IP Address:** identifies cryptographic material associated with IP addresses enables management of internal and 3rd party data in motion risks **Application:** identifies cryptographic material associated with applications to enable effective risk management **CI/CD Pipelines:** identifies cryptographic material embedded into development objects to include embedded secrets.
Certificate Discovery and Management	• SSL/TLS Certificates: Discovers certificates across all internal and external endpoints, including: • Self-signed certificates. • Certificates issued by Certificate Authorities (CA). • Wildcard and SAN (Subject Alternative Name) certificates. • Certificate Validity: Track expiration dates and provide alerts for expiring certificates. • Certificate Algorithm: Identify the algorithms used in certificate signing, such as RSA and ECDSA (Elliptic Curve Digital Signature Algorithm). • Certificate Trust Chain: Verify the trust chain of certificates to ensure they are correctly signed by trusted CAs.
Health and Risk Analysis	• Weak and Deprecated Algorithms: Flag algorithms considered insecure by modern standards (e.g., DES, MD5, SHA-1). • Key Rotation and Lifetimes: Identify and report on key usage lifecycles and enable enforcement of automated key rotation policies. • Encryption Coverage Gaps: Highlight areas of the IT environment where encryption is either weak or not being used. • Vulnerability Alerts: Detect vulnerable configurations such as weak key exchange methods (e.g., Diffie-Hellman 512-bit), exposed keys, or misconfigured certificates

EXTERNAL SCANNER

Solution Architecture	External (either Software As A Service, Private Cloud, Customer Provided environment), internally hosted as a docker image or consultant managed.
Technology	IP Scanning, Modified application vulnerability scanner, Agent (if required)
Scan configuration	Domain-enable a broad based scan across established domains (includes detected sub-domains) IP Range-enable a targeted scan across selected IP address ranges
Evaluation & Scoring	Scored against the following standards: • NIST Quantum cryptography • OWASP CBOM standards • Custom
Crypto evaluated against standard and quantum policies	YES
Evaluates and scores ciphers at endpoints	YES
Traditional Encryption Protocols	AES, RSA, ECC, TLS, IPSec, SSH, PGP, S/MIME, SSL, 3DES, Blowfish, DES
PQC Protocols	Kyber, Dilithium, FALCON, SPHINCS+
Cryptographic Keys	• Symmetric Keys • Private/Public Key Pairs • Session Keys • Expired Keys • Weak Key Lengths
Certificate types	• SSL/TLS certificates • CA-issued certificates • Self-signed certificates • Expired certificates, • Certificate algorithms (e.g., RSA, ECDSA) • Trust chains

INTERNAL SCANNER

Solution Architecture	External (either Software As A Service, Private Cloud, Customer Provided environment), internally hosted as a docker image or consultant managed.

Technology	STANDARD: Agent, modified vulnerability scanner, modified application scanner (includes Database scanner) CUSTOM: Customer Agent
Scan configuration	IP Address, Domain (to include subdomains) • Domain-enabled: a broad based scan across established domains (includes detected sub-domains) • IP Range-enabled: a targeted scan across selected IP address ranges • Targeted individual scans (machine name/host name)
Scanning Agent – scans and inventories machines for certificates and crypto	• Binary files • Java files • Java key stores • MS CAPI store certs • Compressed files • Dormant/isolated/hidden • PEM, CER, DER, P12 files
Certificate types	• SSL/TLS certificates • CA-issued certificates • Self-signed certificates • Expired certificates, • Certificate algorithms (e.g., RSA, ECDSA) • Trust chains
Active Certificate Scanner	Active TLS/SSL (automated) Other cert types (machine scanning agent) Vendor agnostic External + internal facing Public or private trust
Compliance and Audit	Internal policy: cert expiry times, cert signing authority, authorized algorithms, authorized libraries External regulations: PCI DSS (3.5, 4.1, 6.5), HIPAA, GDPR (Clause 83), PSD2 (Article 35), NIST (800-175, 22, 133, 131, 78, 56), ISO 27002 (Ctrl domain 12, 13, 14), ISO 24759, ISACA, CSA

INTERNAL SCANNER (CONT.)

Encryption Standards and Protocol Support	• Protocols: The software scans and catalogs encryption used in key protocols: • SSL/TLS for web communications. • IPSec for VPN connections. • SSH for secure remote connections. • S/MIME or PGP for encrypted email. • File-level Encryption: Full-disk encryption (e.g., BitLocker, FileVault), or file based encryption (e.g., GPG, OpenPGP). • Legacy Protocols: The software should detect deprecated or insecure encryption protocols (e.g., SSL 3.0, TLS 1.0, WEP in Wi-Fi networks).
Traffic Inspection	Analyze network traffic to detect the use of encryption, even in communications between internal systems, and verify secure encryption practices (e.g., TLS 1.2/1.3).
Cloud Environments	Track encrypted data stored in cloud services, including where encryption keys are managed (customer vs. cloud provider).
Traditional Encryption Protocols	AES, RSA, ECC, TLS, IPSec, SSH, PGP, S/MIME, SSL, 3DES, Blowfish, DES
PQC Protocols	Kyber, Dilithium, FALCON, SPHINCS+
Cryptographic Keys	• Symmetric Keys • Private/Public Key Pairs • Session Keys • Expired Keys • Weak Key Lengths
Certificate types	• SSL/TLS certificates • CA-issued certificates • Self-signed certificates • Expired certificates, • Certificate algorithms (e.g., RSA, ECDSA) • Trust chains

ASSET SCANNER

Solution Architecture	External (either Software As A Service, Private Cloud, Customer Provided environment), internally hosted as a docker image or consultant managed.
Technology	STANDARD: Agent, IP scanning, API feeds from common CI/CD pipelines CUSTOM: Customer Agent

Scan configuration	Domain (to include subdomains), IP addresses
IT Assets Scan	Endpoints • Laptops/Desktops • Servers • Routers • Switches • Firewalls • Storage Devices • Printers/Scanners
Software Assets	• OS • Applications • Cloud Services • Security software • Virtual Machines
IoT Assets	• Phone OS • Cameras • Smart Devices • Connected keychains or location trackers • HVAC • Medical devices • Environmental Sensors • Gateways • Point-of-sale (POS) systems. • Smart projectors and multimedia systems
IIoT	• Programmable logic controllers (PLCs) • Industrial robots and autonomous systems. • Smart sensors (e.g., temperature, pressure, and motion sensors). • SCADA systems (Supervisory Control and Data Acquisition).

DATABASE SCANNER

Solution Architecture	External (either Software As A Service, Private Cloud, Customer Provided environment), internally hosted as a docker image or consultant managed.
Technology	STANDARD: Agent CUSTOM: Customer Agent
Scan configuration	Domain (to include subdomains), IP address, individual machine/hostname
Databases	**RELATIONAL** • MySQL • PostgreSQL • Microsoft SQL Server • Oracle Database • MariaDB • IBM Db2 **NOSQL** • MongoDB • Cassandra • Couchbase • Redis • Elasticsearch **CLOUD** • Amazon RDS • Google Cloud SQL • Azure SQL Database • Amazon DynamoDB • Google Firestore / Firebase **OBJECT** • Db4o • ObjectDB **TIME SERIES** • InfluxDB • Prometheus • TimescaleDB

CODE

Solution Architecture	External (either Software As A Service, Private Cloud, Customer Provided environment), internally hosted as a docker image or consultant managed. All data is gathered from third party sources via API.
Technology	Git, Bitbucket, Atlassian, IBM, others

APPLICATION INTEGRATIONS: SECURITY EVENT MONITORING

Splunk Enterprise Security	External (either Software As A Service, Private Cloud, Customer Provided environment), internally hosted as a docker image or consultant managed.	Rest API
IBM QRadar SIEM	Provides real-time visibility, threat detection, and compliance management across the IT infrastructure.	Rest API
LogRhythm NextGen SIEM	Offers comprehensive threat detection, response, and compliance management with integrated user and entity behavior analytics.	Rest API
ArcSight Enterprise Security Manager (ESM)	Delivers real-time data collection, normalization, and correlation for comprehensive threat detection and response.	Rest API
AlienVault Unified Security Management (USM)	Integrates essential security capabilities, including asset discovery, vulnerability assessment, and intrusion detection.	Rest API
Securonix SIEM	Utilizes machine learning for advanced threat detection and response, focusing on user and entity behavior analytics.	Rest API
Exabeam Fusion SIEM	Combines SIEM and XDR capabilities to provide comprehensive threat detection, investigation, and response.	Rest API
Microsoft Azure Sentinel	A cloud-native SIEM solution offering intelligent security analytics and threat intelligence across the enterprise.	Rest API
Elastic Security	Built on the Elastic Stack, it provides SIEM capabilities with real time threat detection and response.	Rest API

Fortinet FortiSIEM	Integrates network operations and security operations to provide comprehensive visibility and automated response.	Rest API
ManageEngine Log360	Offers log management and network security with real-time event correlation and compliance reporting.	Rest API
Graylog	An open-source log management platform providing real-time event analysis and monitoring.	Rest API
Datadog Security Monitoring	Provides real-time threat detection across applications, networks, and infrastructure.	Rest API
Zoho Desk	Offers multi-channel ticketing, automation, and a self-service portal.	Rest API
HubSpot Service Hub	Integrates with HubSpot's CRM, offering ticketing, automation, and customer feedback tools.	Rest API
AzureDesk	Offers ticket management, automation, and reporting features.	Rest API
SupportBee	Provides a simple ticketing system with collaboration features.	Rest API

APPLICATION INTEGRATIONS: TICKETING

Zendesk	A comprehensive help desk solution offering ticket management, automation, and multi-channel support.	Rest API
Freshdesk	Provides a user-friendly interface with features like ticketing, automation, and a knowledge base.	Rest API
Jira Service Management	Offers robust IT service management capabilities, including incident, problem, and change management.	Rest API
ServiceNow	A comprehensive IT service management platform with advanced automation and integration capabilities.	Rest API
Spiceworks Help Desk	A free, user-friendly help desk solution suitable for small to medium-sized businesses.	Rest API

APPLICATION INTEGRATIONS: VULNERABILITY SCANNER

Tenable (Nessus)	Offers comprehensive vulnerability assessment for networks, endpoints, and servers, with over 47,000 unique asset and application scans.	Rest API
Invicti	Provides in-depth scanning for websites and applications, including Dynamic Application Security Testing (DAST), Interactive Application Security Testing (IAST), and Software Composition Analysis (SCA).	Rest API
StackHawk	Designed for DevOps teams, it offers entry-level web application scanning with continuous integration and continuous deployment (CI/CD) integration.	Rest API
Nmap	An open-source tool for network discovery and security auditing, known for its efficiency in host discovery and port scanning.	Integrated application
ConnectSecure	Provides basic infrastructure scanning tailored for service providers, featuring multi-tenant scanning and automated alerts.	Rest API
Vulnerability Manager Plus	An entry-level endpoint and server scanner that detects vulnerabilities in devices, including end-of-life software and third-party applications.	Rest API
Burp Suite	A comprehensive platform for web application security testing, offering tools for scanning and manual testing.	Rest API
OpenVAS	An open-source vulnerability scanner suitable for large-scale scans, covering web applications, databases, operating systems, and networks.	Integrated application
Nikto2	An open-source tool focusing on web application security, capable of detecting over 6,700 potentially dangerous files and configurations.	Integrated application
Arachni	A free, open-source vulnerability scanner for web applications, supporting Linux, Windows, and macOS platforms.	Rest API

APPLICATION INTEGRATIONS: ASSET MANAGEMENT

ManageEngine AssetExplorer	A web-based ITAM solution that helps monitor and manage assets from procurement to disposal.	Rest API
ServiceNow IT Asset Management	Provides comprehensive asset tracking, compliance management, and lifecycle automation.	Rest API
Freshservice	Offers ITAM features integrated with IT service management, including asset discovery and tracking	Rest API
SolarWinds Service Desk	Combines IT service management with asset management capabilities for streamlined operations.	Rest API
Ivanti IT Asset Management Suite	Offers asset discovery, software license management, and compliance tracking.	Rest API
Spiceworks IT Asset Management	A free tool that provides network inventory and asset tracking features.	Integrated application

APPLICATION INTEGRATIONS: REPORTING INTEGRATIONS

Zoho Analytics	Offers comprehensive data integration and visualization capabilities, connecting with over 250 data sources.	Rest API
Tableau	Renowned for its robust data visualization features, allowing users to create interactive and shareable dashboards.	Rest API
Microsoft Power BI	Provides powerful analytics and visualization tools, integrating seamlessly with other Microsoft products.	Rest API
Looker Studio	A free tool by Google that transforms data into informative dashboards and reports, emphasizing collaboration.	Rest API
Whatagraph	Specializes in creating marketing reports, aggregating data from various platforms into visually appealing formats.	Rest API