doyen Cyber

Chronos™

Innovative Security Solutions to **Combat Quantum Threats**

Strengthen Your Encryption | Secure Critical Assets | Ensure Compliance with Standards

@2024 Doyen Cyber. All Rights Reserved

Chronos™

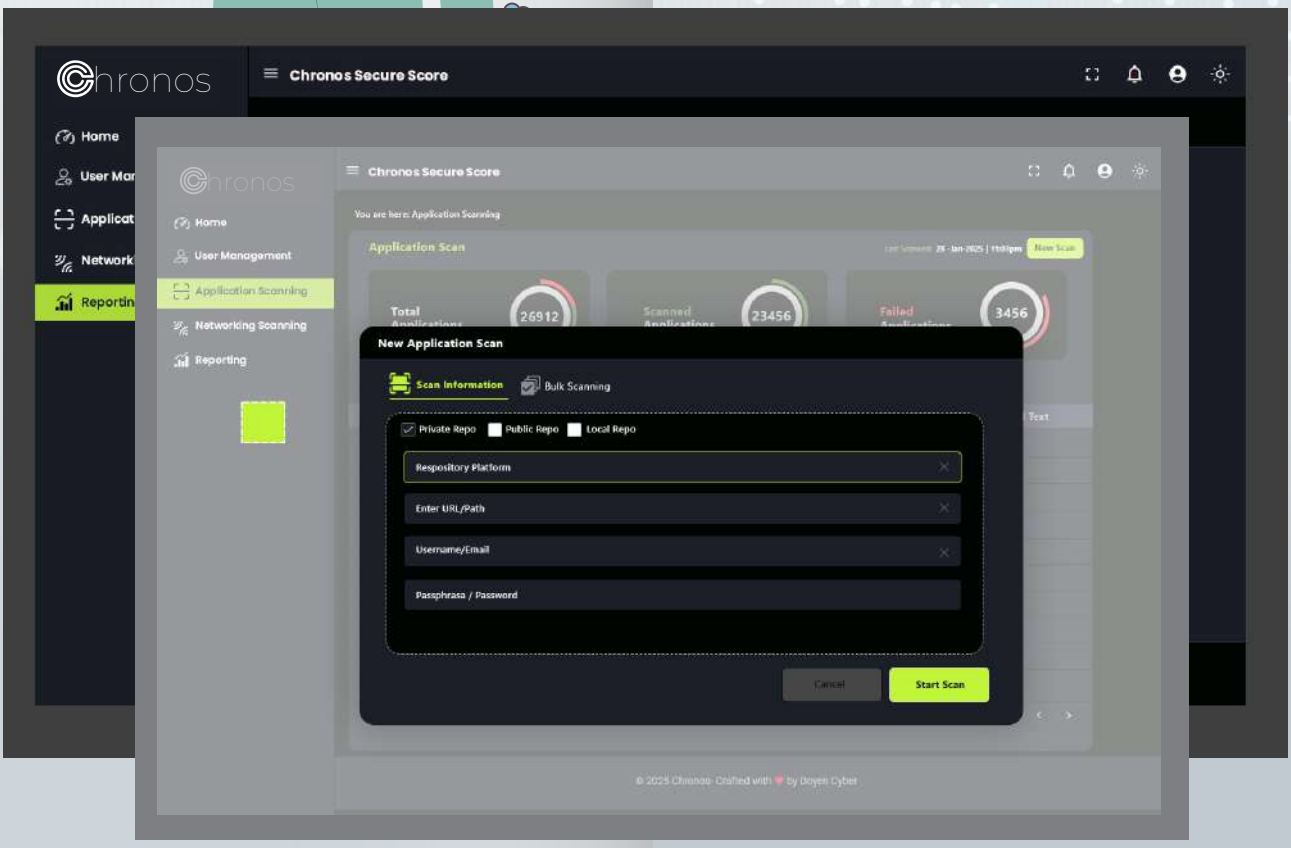
Future-Proofing Cryptography in the Quantum Era

Quantum computing is advancing rapidly, posing risks to traditional cryptography

Our solution helps discover and assess cryptographic implementations vulnerable to quantum threats.

Key Features / Why Chronos?

- **Cryptographic Discovery**
  Identify outdated or quantum-vulnerable cryptographic algorithms across applications and networks.
- **Automated Assessment Tool**
  Evaluate cryptographic usage within your repositories and network infrastructure.
- **Comprehensive Reporting**
  Get current statistics on cryptographic risks, along with actionable recommendations.
- **Quantum Security Dashboard**
  Visualize your organization's Quantum Resilience Score and track readiness over time.
- **Strategic Recommendations**
  Step-by-step guidance on transitioning to quantum-safe encryption, with quick wins to enhance security now.



@2024 Doyen Cyber. All Rights Reserved

Why it **matters?**

Quantum Computers Will Break RSA & ECC Encryption

Traditional cryptographic algorithms like RSA, ECC (Elliptic Curve Cryptography), and DSA rely on mathematical problems that are extremely difficult for classical computers to solve. However, quantum computers, using Shor's Algorithm, will be able to factor large prime numbers and solve discrete logarithm problems exponentially faster. This means:

- RSA-2048 encryption, which would take a classical computer billions of years to break, could be cracked by a sufficiently powerful quantum computer in mere hours or days.
- ECC, widely used in secure communications and digital signatures, will also be rendered obsolete.
- Any organization relying on these cryptographic standards today is at risk of future decryption attacks.

Chronos™

Future-Proofing Cryptography in the Quantum Era

Organizations Must Act Now to Safeguard Sensitive Data

The transition to post-quantum cryptography (PQC) is not instantaneous. It requires:

- Identifying vulnerable cryptographic systems in your infrastructure.
- Upgrading to quantum-resistant algorithms like those recommended by NIST's Post-Quantum Cryptography Standardization (e.g., CRYSTALS-Kyber, CRYSTALS-Dilithium).
- Implementing hybrid encryption models to maintain security during the transition

Cybercriminals Are Already Using "Harvest Now, Decrypt Later" (HNDL) Attacks

Even though large-scale quantum computers are not yet available, nation-state actors and cybercriminals are already collecting encrypted data today—with the intention of decrypting it later when quantum technology matures. This means:

- Sensitive financial, healthcare, and government data being intercepted today could be decrypted soon.
- Data with long-term confidentiality requirements (e.g., intellectual property, classified information, trade secrets) is especially at risk.
- Failure to prepare now means organizations could face a massive security breach once quantum computers reach the necessary scale.

@2024 Doyen Cyber. All Rights Reserved

Benefits of **Chronos:**

Innovative Security Solutions to **Combat Quantum Threats**

Compliance & Regulatory Readiness

- Align with evolving security stan dards, including NIST's Post-Quantum Cryptography Guidelines, GDPR, and industry-specific frame works.
- Avoid non-compliance penalties by ensuring cryptographic protocols are future proof.

Streamlined Migration to Quantum-Safe Encryption

- Receive actionable recommendations and quick-win strategies to transition to quantum-resistant cryptography.
- Reduce complexity by automating cryp-tographic assessments instead of relying on manual audits.

Data-Driven Decision Making

- Generate detailed reports with current encryption statistics and security gaps.
- Utilize a Quantum Security Score Dashboard to assess organizational readiness and track improvements over time.

Stay Ahead of Cyber Threats

- Combat "Harvest Now, Decrypt Later" threats by proactively securing sensitive data.
- Gain visibility into cryptographic weaknesses before attackers can exploit them.

Identify & Mitigate Security Risks

- Discover outdated or quantum-vulnerable cryptographic algorithms across applications and networks before they become exploitable.
- Prevent exposure to future quantum attacks by ensuring encryption compliance with post-quantum cryptography (PQC) stan dards

Cost Savings & Risk Reduction

- Prevent costly data breaches resulting from broken encryption.
- Reduce operational overhead by identifying and addressing cryp tographic vulnerabilities early rather than reacting to an incident.

Strengthen Customer & Partner Trust

- Demonstrate commitment to cutting-edge security practices and long-term data protection.
- Build trust with clients and stake holders by proactively addressing quantum computing risks.

@2024 Doyen Cyber. All Rights Reserved

Chronos™

A quantum cryptographic discovery tool not only protects sensitive data but also enhances customer trust, strengthens compliance, and improvesbusiness longevity—turning security from a cost into a competitive advantage.

@2024 Doyen Cyber. All Rights Reserved

doyencyber

"We believe in a safer digital world for all and strive to make cybersecurity accessible to everyone."

At Doyen Cyber, we are committed to tackling cyber poverty and driving innovation across the tech industry, with a particular focus on cybersecurity, quantum computing, and AI. Our mission is clear: to democratize access to essential cybersecurity tools and knowledge, empowering communities and fostering a safer digital world.

Central to our vision is our dedication to advancing the presence of women in cybersecurity. As a member of Women in Cybersecurity (WiCyS), I recognize the pivotal role diversity plays in technology and the invaluable contributions of women leaders in this field. We are passionate about providing mentorship opportunities to cultivate the next generation of cybersecurity trailblazers

Chronos™

Contact us: +27793249261 | Email Id: noorim@doyencyber.com

@2024 Doyen Cyber. All Rights Reserved