Cybersecurity in the era of generative AI: IBM's Approach and Strategy

George Mavrovitis
IBM Security Technical Sales

Enterprises are embracing generative AI, but have concerns

Under pressure to adopt

64%

face significant pressure to accelerate generative AI initiatives

Concerned about new risks

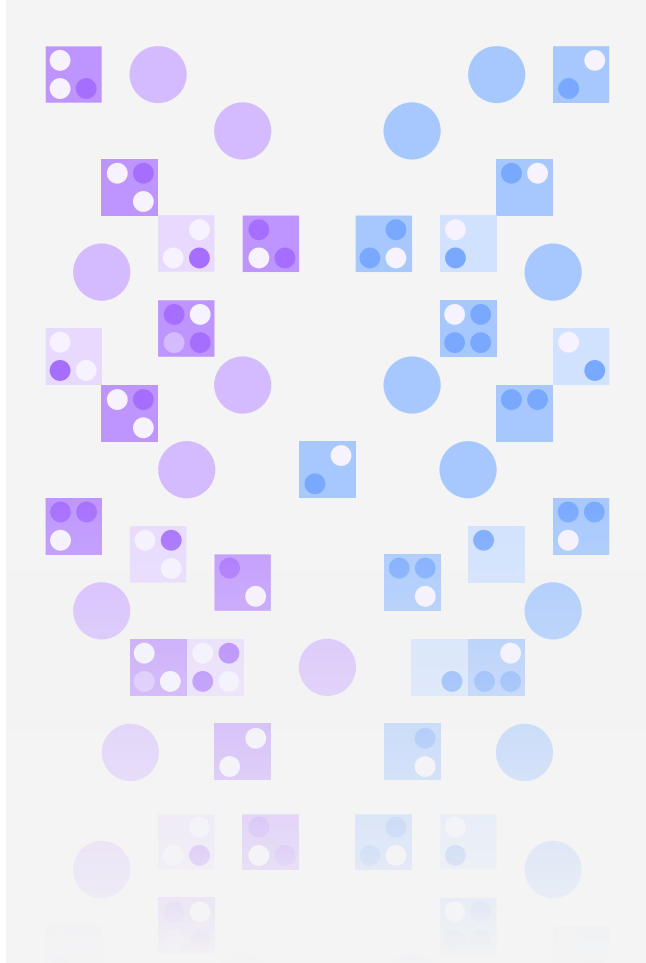
84%

see cybersecurity risk as the #1 roadblock to generative AI adoption

Investing in new defenses

64%

identified security as the #1 priority for generative AI use cases



Generative AI is the new burning platform to secure now

Source: “Enterprise generative AI: State of the market” 2023 IBM Institute of Business Value Study

Security operations need AI to improve efficiency

49%

SOC team members are only getting to **half of the alerts** that they're supposed to review within a typical workday[1]

80%

of organizations use at least **10 disparate solutions** to manage security hygiene[2]

2 out of 3

organizations' external attack surface has **expanded** in the last year[2]

51%

of organizations struggle to **detect and respond** to advanced threats[3]

52%

of security environments have become more **difficult to manage** over the last two years[3]

29%

of security operations processes are **immature** and need reengineering before they can be automated[2]

Source: 1. Global Security Operations Center Study Results, IBM, March 2023.
Source: 2. The State of Attack Surface Management 2022, Randori.
Source: 3. ESG: SOC Modernization and the Role of XDR, 2022.

Attackers will target AI

AI should be treated as a **new attack surface,** with new detection and response strategies required for model evasion, extraction, inference and poisoning

Prompt injection can drop defenses preventing generation of unwanted material, plus access to exploitable integrations and a wealth of sensitive training data

Malicious models can be uploaded to open repositories, with **hidden behavior** triggered long after they've been deployed

Attackers will utilize AI

Generative AI will **scale** cybercrime, and reduce barriers to entry to lower skilled attackers

Phishing will become more **targeted**, and generative video and audio techniques will necessitate new approaches to avoid business compromise

Attackers will **adapt** to defensive strategies faster, and improve detection evasion, vulnerability discovery, and malware customization

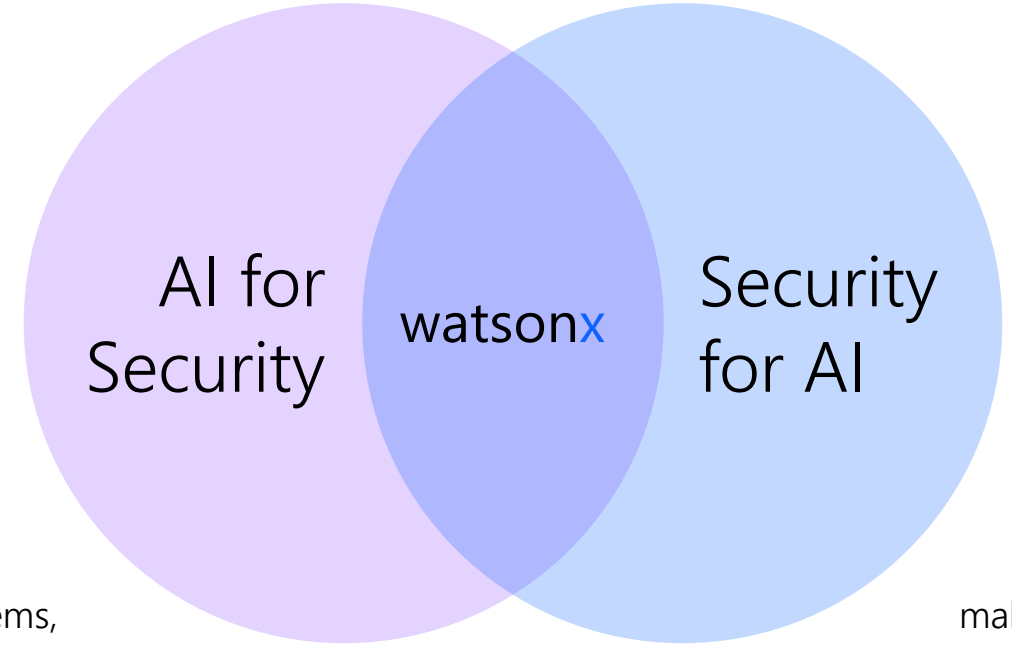
IBM's cybersecurity and AI strategy

Productivity gains from foundation models and generative AI will reduce human bottlenecks in security

AI will manage repetitive security tasks such as summarizing alerts and log analysis, freeing teams to tackle strategic problems

AI will generate security content (detections, workflows, policies) faster than humans, expediting implementation and adjusting to changing security threats in real-time

AI will learn and create active responses that optimize over time, with abilities to find all similar incidents, update all affected systems, and patch all vulnerable code



Protecting foundation models, generative AI, and their data sets is essential for enterprise-ready AI

Secure the underlying AI training data by protecting it from sensitive data theft, manipulation, and compliance violations

Secure the usage of AI models by detecting data or prompt leakage, and alerting on evasion, poisoning, extraction, or inference attacks (IBM Adversarial Robustness Toolkit)

Secure against new AI generated attacks such as personalized phishing, AI-generated malware, and fake identities by using behavioral defenses and multi-factor authentication

The AI and data Platform

watsonx

Scale and accelerate SOC solutions with AI

watsonx.ai

Train, validate, tune and deploy AI models

A next generation enterprise studio for AI builders to train, validate, tune, and deploy both traditional machine learning and new generative AI capabilities powered by foundation models. It enables you to build AI applications in a fraction of the time with a fraction of the data.

watsonx.data

Scale AI workloads, for all your data, anywhere

Fit-for-purpose data store optimized for governed data and AI workloads, supported by querying, governance and open data formats to access and share data.

watsonx.governance

Enable responsible, transparent and explainable data and AI workflows

End-to-end toolkit encompassing both data and AI governance to enable responsible, transparent, and explainable AI workflows.

Create the competitive edge for your Security Solutions

watsonx is having a radical impact on every aspect of security operations

People

Cyber Assistants

Using conversational AI to answer adhoc user questions or complex queries around security - reducing the skill requirements and bridging cyber talent gap

Onboarding and ramp-up

Reduce the time in onboarding new security professionals. SOC managers can understand complex threats more easily and CISOs can better understand security posture of their company

Customer support

Simplify onboarding and setting up of a SOC for a new customer and provide a self serve experience to users for any help or problem resolution

Process

Triage

Prioritizing incidents based on their potential consequences so that resources are utilized where they can have the greatest business impact.

Test Threat Detection

Use techniques such as synthetic data creation or generating phishing emails for Security testing and Red team/ blue team training.

Policies and Documentation

Summarize compliances, threats, vulnerabilities, detection guidance and maintain cohesive security policy documentation, best practices policies and procedures

Technologies

Customize Digital Playbooks

Input English language text and adapt and transform generic SOC configurations and digital playbooks, to match the specific requirements and IT ecosystem of each client.

Customized Summarization/ Reports

Producing incident summaries, customized reports and recommendations, considering each client's risk profile and security needs

Unlock insights, improve response

Assist Security Analyst by surfacing insights based on decisions made in the past for similar Security incidents, and provide response recommendation

watsonx

Content gen, Insight extraction, Retrieval-augmented generation

Tune the models to use existing knowledge base to generate contextual insights

Classification, Summarization, Content generation

Automate code generation and and reduce time taken for interpreting and summarizing information

Retrieval-augmented generation, Summarization, Insight extraction

Prompt tune relevant foundation model using past data and company-specific Security configurations

AI brings **speed** and **accuracy** so we can…

Proactively Protect, **Accurately** Detect and Respond **Faster**

… and **lower costs & complexity** of security operations

What’s next?

Improving the productivity of security analysts with multiple foundation models

40%

of a security analyst's time is spent on automatable tasks[1]

Automate Mundane Tasks

1 Virtual Cybersecurity Assistant

A question-answering chatbot feature grounded on cybersecurity-specific content, providing analysts with real-time insight into an environment's specific threat landscape by asking simple questions, e.g., "Where is malicious code running in the environment?".

2 Incident and Case Summarization

Automating alert analysis and summarization by translating complex attack syntax to human-readable explanations of exposure, including impacted assets and recommended mitigations.

3 Playbook Generation

Automatically generate workflow of recommended actions for incident response and remediation

using a decision support engine to compose automation rules and protection policies.

Elevate from Reactive to Proactive

4 Threat Hunting Acceleration

Automatically generate hunt queries from natural language that can be used to hunt for specific patterns of threats. Also use for chatbot Q&A of specific threat actors, techniques, and behaviors and cross correlate across seemingly unrelated events.

5 Predictive Threat Insights

Assess the possibility of a specific attack occurring, with 60-70% of attacks being "repeat offenders" (based on same code), this function will create a predictive capability that helps security teams strengthen their response readiness.

6 Detect Previously Unseen Threats

Identify anomalous behavior without needing to be trained on it using our continuously-learning AI foundation model that can detect and respond to previously unseen threats.

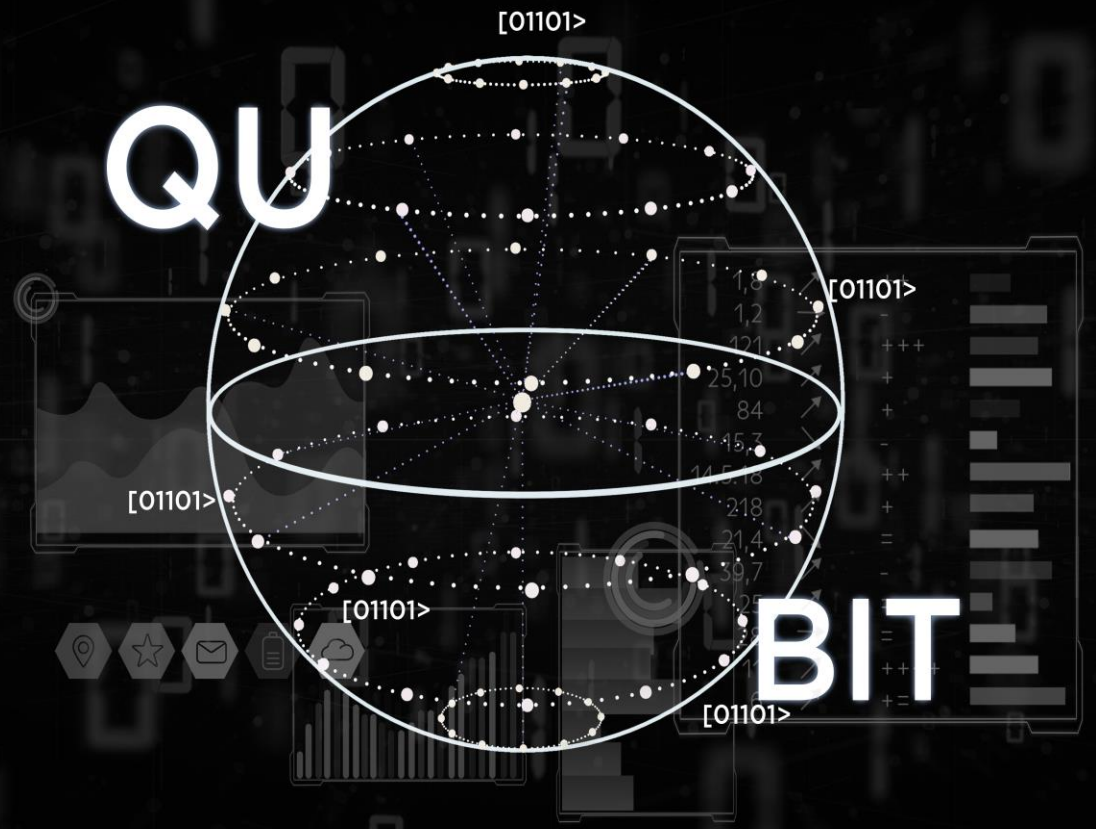
Quantum Computing

Quantum computing harnesses the phenomena of quantum mechanics to deliver a huge leap forward in computation to solve certain problems.

IBM are designing and building quantum computers to solve complex problems that today's most powerful supercomputers cannot solve, and never will.

Can perform certain mathematical computations exponentially faster than today’s computers – making current encryption standards obsolete

With quantum computers, hackers will be able to forge transactions and change legal history by manipulating data that they gained access to using forged digital signatures



Traditionally, a bit is either a 0 or a 1

There are two possible values

A Qubit can be all possible values, at the same time

For a bit wise value, it can be both a 0 AND a 1

Two Qubits can be 00, 01, 10, and 11- all at the same time

The current IBM 127 Qubit system, can have 2^{127} possible bit combinations – all at the same time!

Quantum applications span three general areas

Simulating Quantum Systems

Quantum chemistry
Material science
High energy physics

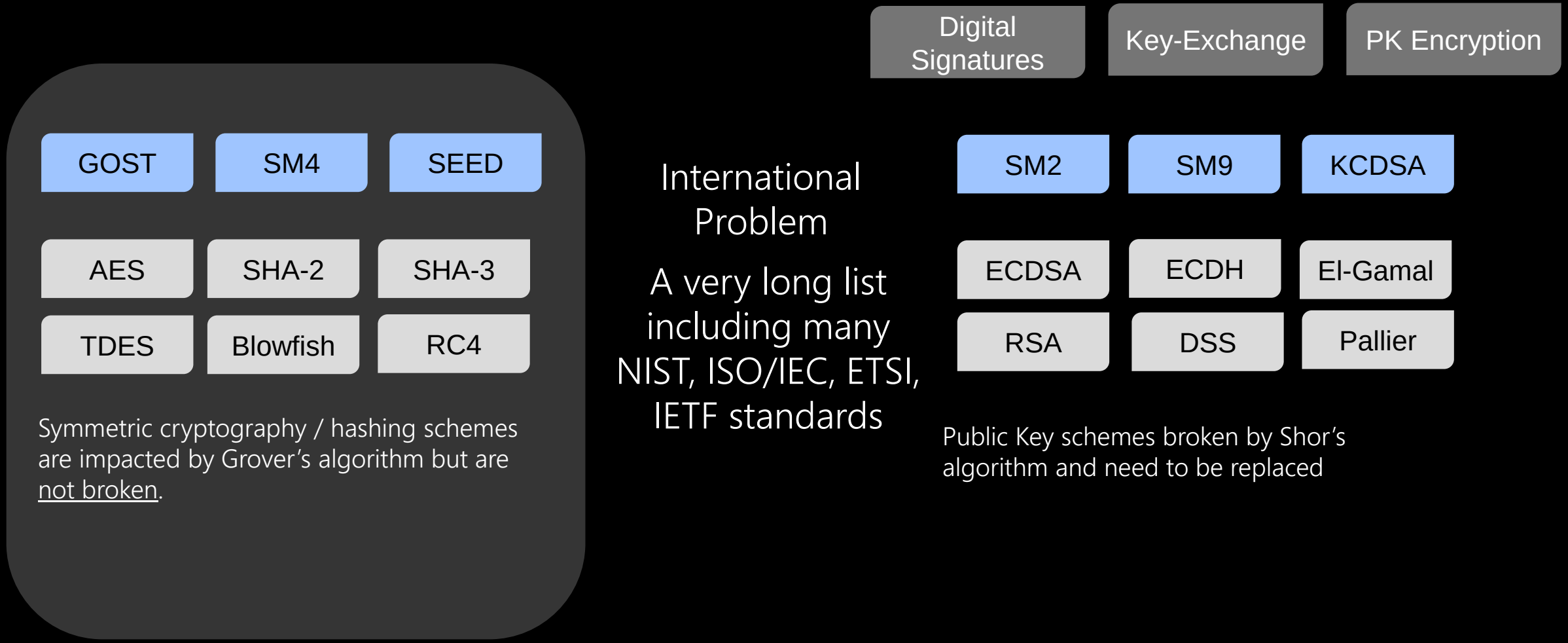
Artificial Intelligence

Better model training
Pattern recognition
Fraud detection

Optimization / Monte Carlo

Portfolio optimization
Risk analysis
Loans & credit scoring
Monte Carlo-like applications

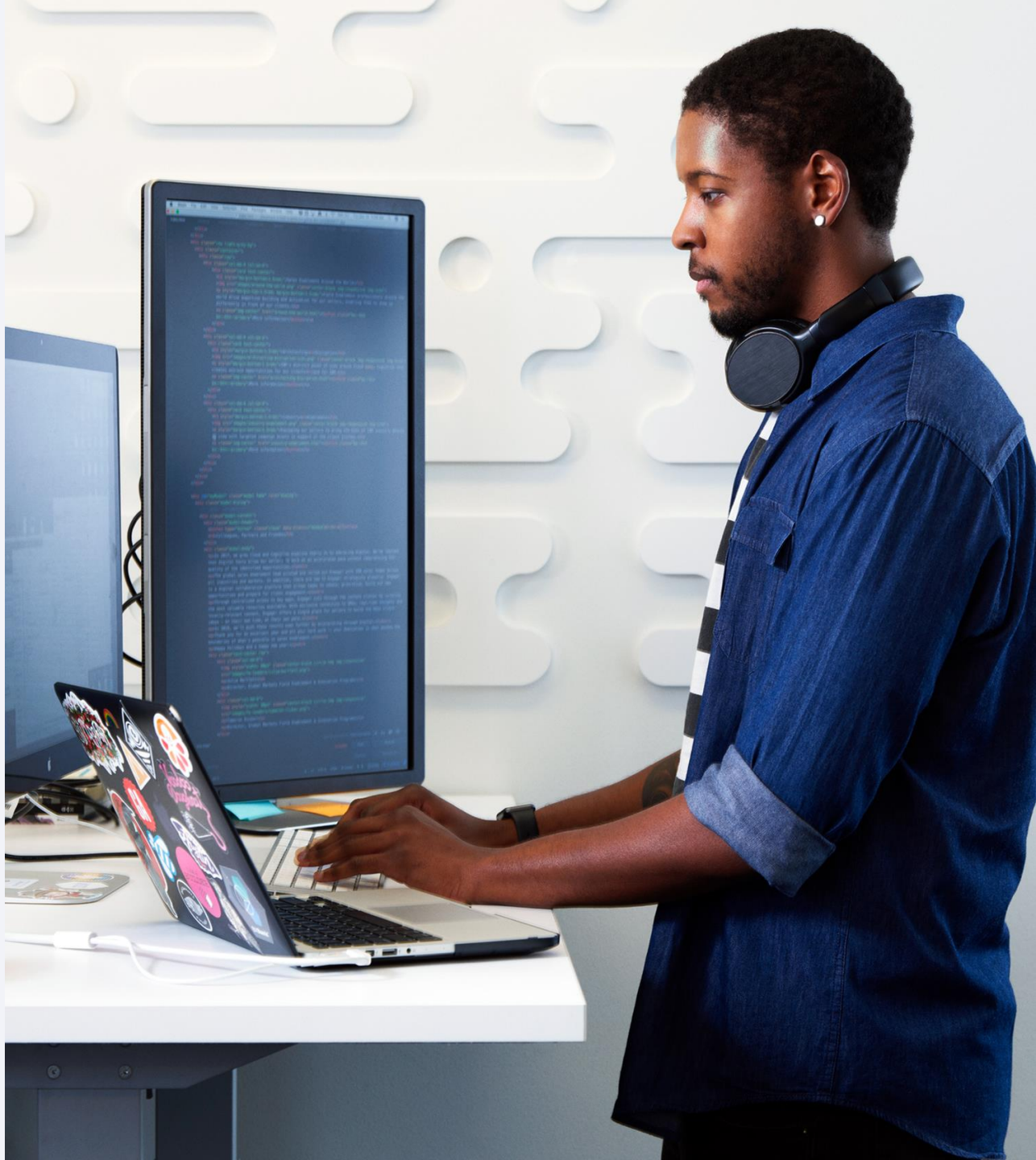
What cryptographic schemes are impacted?



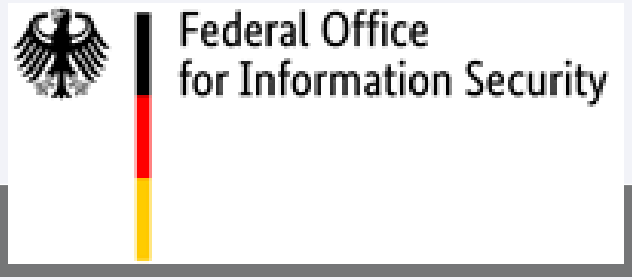
We need quantum-safe cryptography …

Quantum-safe cryptography refers to efforts to identify algorithms that are resistant to attacks by both classical and quantum computers, to keep information assets secure even after a large-scale quantum computer has been built.

Source: https://www.etsi.org/technologies/quantum-safe-cryptography



Start now!



- Critical to begin planning for the replacement of hardware, software, and services that use public-key algorithms now
- Be ready to adopt and implement the new algorithms at the end of the standardization process
- 5 to 15 or more years following, standardization to replace most of the vulnerable public-key systems currently in use

- The protection of long-lasting secrets makes it urgent that actions be taken now or as soon as possible
- BSI is not waiting for NIST to come out with a standard to issue technical guidance
- In high security applications, hybrid schemes (use classical algorithms + quantum-safe algorithm) are required by BSI

https://www.nccoe.nist.gov/projects/building-blocks/post-quantum-cryptography

Quantum is here –Get Started

Classical Cryptographic Algorithms are widely used to protect data and communications in computer systems and networks.

An adversary with access to a sufficiently strong quantum computer can break the classical algorithms we have used for many years.

Most vulnerable are Asymmetric Algorithms and Protocols.

Risks include theft of digital assets, forged documents, transactions, signatures, code and the like. Secure communications are also in jeopardy.

Researchers and standards bodies are moving to address the threats.

IBM is playing a prominent role.

They are identifying new quantum-safe algorithms that can be used to protect classical and quantum computer workloads and data from the attacks that can be launched from quantum computers.

Organizations are providing migration guidance.

Dilithium, an algorithm for quantum safe digital signatures, is our first step to address these threats and is available in Hyper Protect Crypto Services today

Next Steps

Get ready for future battles with AI

- Learn how IBM Security Solutions are leveraging AI
- https://www.ibm.com/ai-cybersecurity
- Introducing the IBM Framework for Securing Generative AI:
- https://www.ibm.com/blog/announcement/ibm-framework-for-securing-generative-ai/
- The value of AI in Cybersecurity:
- https://www.ibm.com/blog/announcement/ibm-framework-for-securing-generative-ai/
- The Power of AI in Security:
- https://www.ibm.com/thought-leadership/institute-business-value/en-us/report/ai-security-automation

Get ready for the quantum future

- Find out how you can become quantum-ready—and how this bleeding-edge technology can help you and your business thrive the moment quantum computers come of age.
- Because that moment is closer than you think.
- For more information and for a vast collection of IBM Quantum materials, see the following links:
- https://www.ibm.com/quantum
- https://qiskit.org
- https://www.ibm.com/thought-leadership/institute-business-value/

Thank you

Follow us on:

ibm.com/security

securityintelligence.com

ibm.com/security/community

xforce.ibmcloud.com

@ibmsecurity

youtube.com/ibmsecurity