STORAGE DEVELOPER CONFERENCE

SDC 23

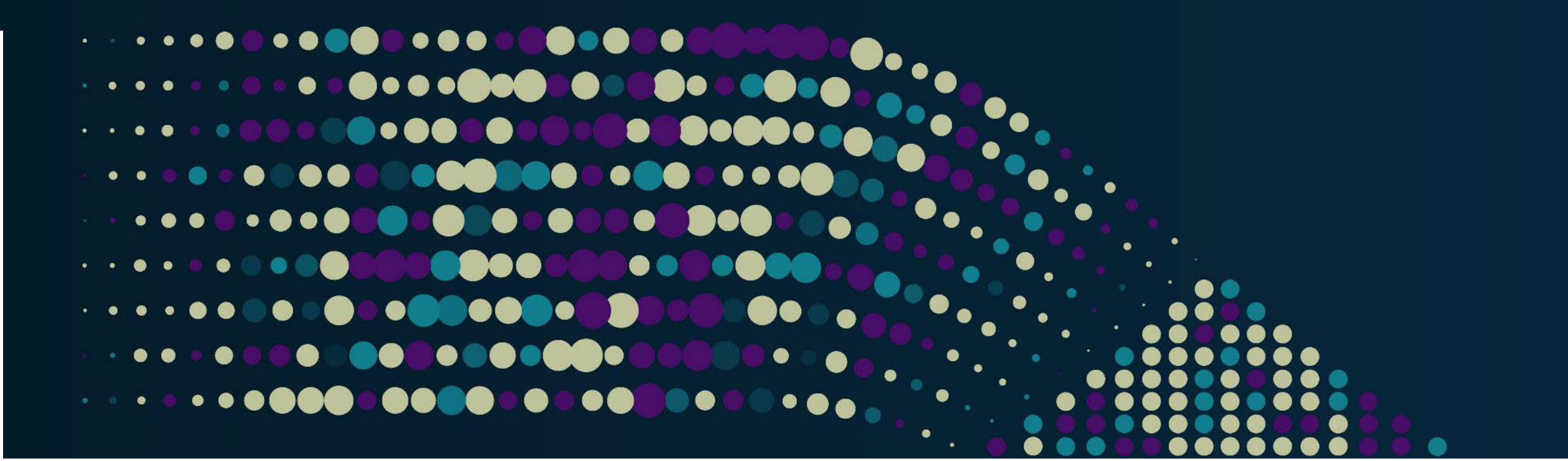
*BY Developers FOR Developers*

# Storage Security Update for Developers

Presented by

Eric Hibbard, CISSP, FIP, CISA

Samsung Semiconductor, Inc.



# The Back Story

Section Subtitle

# Current Threat Landscape

- Social Engineering
- Advanced Persistent Threat (APT)
- Ransomware/Malware
- Unpatched/Updated Systems
- Security Misconfiguration
- Denial of Service
- Sensitive Data Exposure
- Injection Flaws
- Cryptojacking
- Cyber Physical Attacks
- Broken Authentication
- Broken Access Control
- Third Party (Supplier)
- Insider Theft
- Mobile Malware
- Physical Loss of Devices
- Cross-site Scripting (XSS)
- Man-in-the-Middle Attacks
- IoT Weaponization

## Common Threat Actors

- Cyber Terrorists
- Government-sponsored/State-sponsored Actors
- Organized Crime/Cybercriminals
- Hacktivists
- Insiders
- Script Kiddies
- Internal User Errors

## Common Motivations

- Political, Economic, Technical, and Military Agendas
- Profit/Financial Gain
- Notoriety
- Revenge
- Multiple/Overlapping

***Security is a People Problem!***

SDC 23

# Profile of 2023 Breaches

- **Number of data breaches in August 2023:** 73 (publicly disclosed)
- **Breached records in August 2023:** 79,729,271

- **Number of data breaches in 2023:** 767
- **Number of breached records in 2023:** 692,097,913
- **Biggest data breach of 2023 so far:**
  - Twitter (220 million breached records)
- **Most breached sectors:**
  - Healthcare (229), education (126), public (106)

**Source: IT Governance Ltd**

# Recent Notable Breaches/Attacks

- MOVEit: June 2023 – 200 organizations; up to 1.75 million individuals
- T-Mobile: May 2023 (and January 2023) – over 37 million customers
  - 100 million customers in 2021 breach; settled a class action lawsuit to the tune of $350 million in 2022
- Yum Brands: January 2023 – ransomware attack
  - Unknown amount of PII also stolen
- ChatGPT: March 2023 – 1.2% of the ChatGPT Plus subscribers
- Activision: February 2023 – internal data related to games and employees
- MailChimp: January 2023 – employee info and credentials
- Norton Life Lock: January 2023 – 6000 accounts breached
- LastPass: August 2022 – source code and technical information stolen
  - Password management provider servicing 30 million people; customer data safe

# Legal/Regulatory Landscape

- Cybersecurity (many)
  - US SEC Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure
  - US National Cybersecurity Strategy
  - EU NIS2 (Network and Information Security) Directive
  - EU Cyber Resilience Act (CRA)
- Privacy (many)
  - EU General Data Protection Regulation (GDPR)
  - China Personal Information Protection Law (PIPL)
  - Multiple US state (e.g., CA CCPA/CCRA)
- Cybersecurity/privacy litigation on the rise

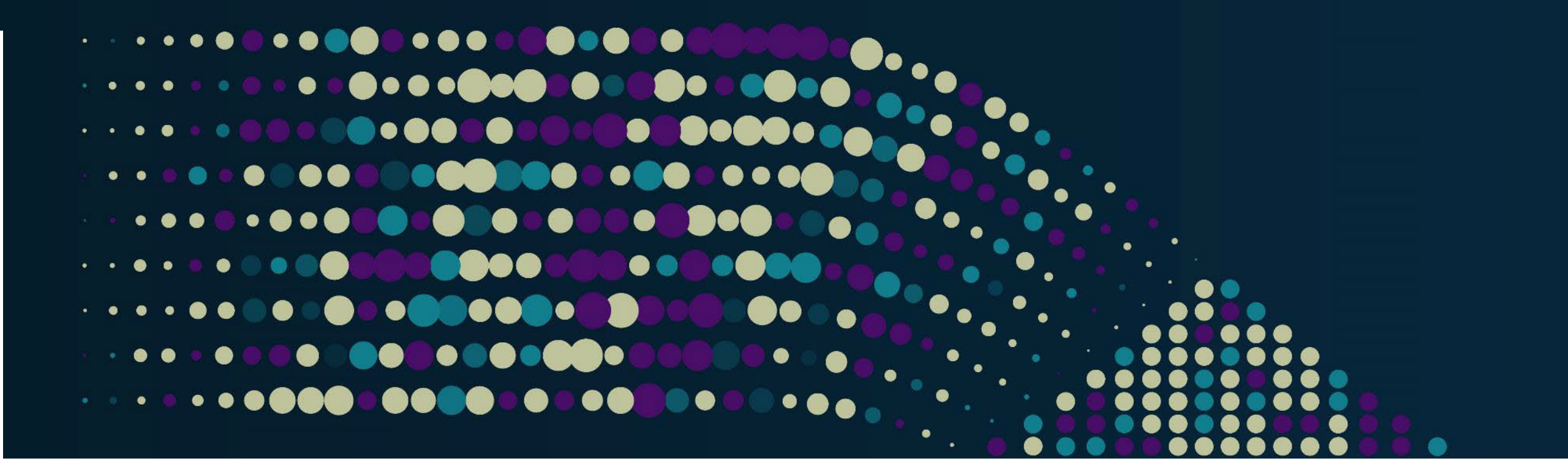
 

# Key Security Frameworks

- NIST Cybersecurity Framework 2.0 (under development)
- ISO/IEC 27000-series Security Standards (transitioning)
- Payment Card Industry Data Security Standard (PCI DSS) 4.0 (transitioning)
- Cybersecurity Maturity Model Certification (CMMC)

- Significance:  Security professional adjusting to changes (distracted)



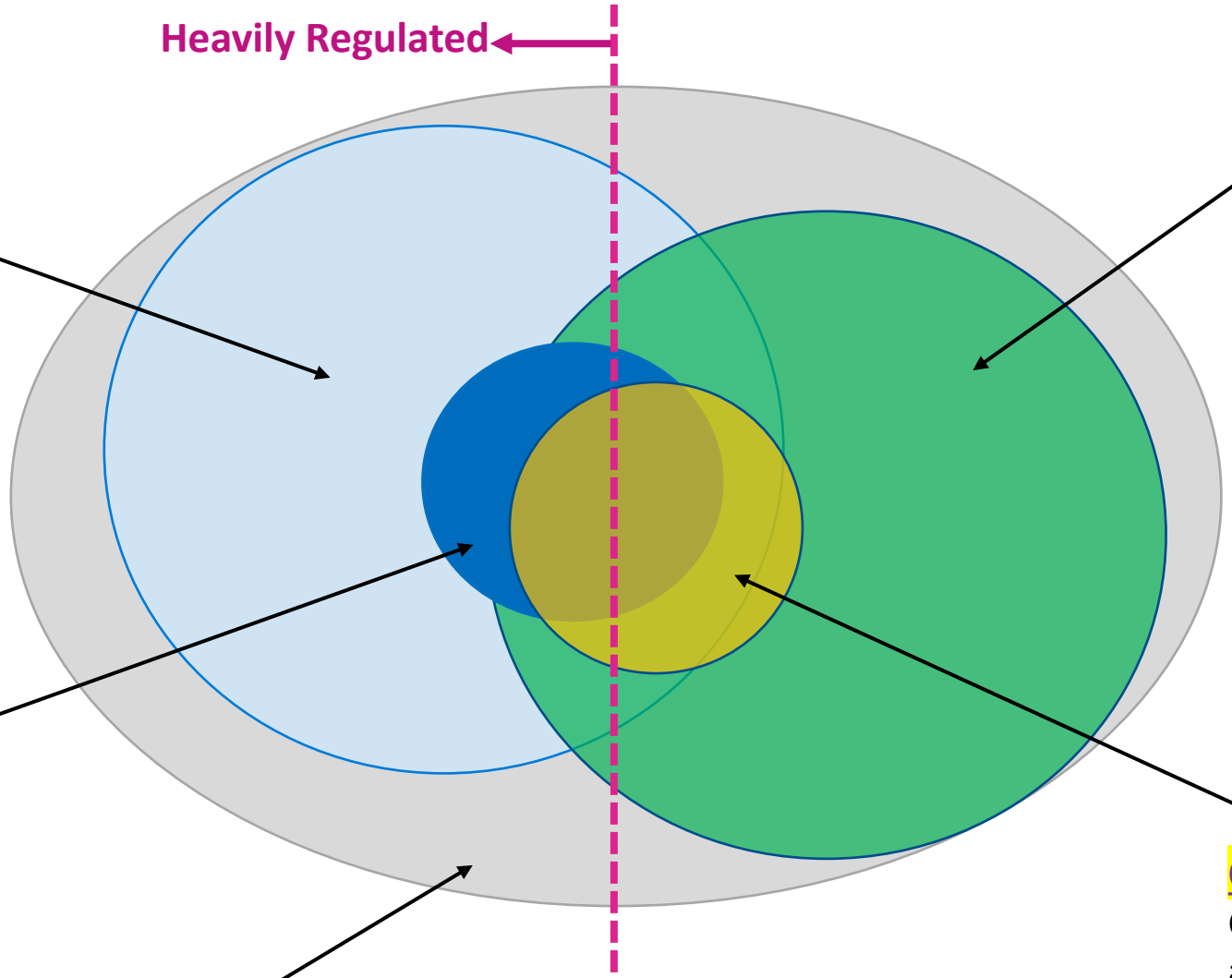
# For Developers

Section Subtitle

**Privacy**: Collection Limitations, Data Quality, Purpose Specification, Use Limitation, Security Safeguards, Openness, Individual Participation, Accountability

Heavily Regulated



**Information Security**: Ensures Confidentiality, Integrity, and Availability (CIA) of information

**Personal Data Protection**: Safeguards applying under various laws and regulations to personal data (PII, PHI, etc.) about individuals that organizations collect, store, use and disclose

**Ethics**: Moral principles that govern a person's behavior or the conducting of an activity

**Cybersecurity**: Ensures Confidentiality, Integrity, and Availability of data; Identify, Protect, Detect, Respond, Recover

# Why Should Developers Care?

- Secure by design and secure by default are expected
- Vulnerability prevention and management are expected elements of the product development process
- Practicing poor cyber hygiene can have legal implications
- Source code and design specifications stolen on regular basis
- Ransomware attacks are delaying or wiping out projects
  - Paying a ransom does not guarantee a recovery
- Attackers are attempting to inject malicious code into code base
  - Open source and vendor proprietary

# Certification May Become Mandatory

- With the primary exception of encryption of sensitive US/CA Government data, certifications are currently optional for vendors
- Several governments and regions (EU) are considering mandatory security certifications as a condition of sales/use in their jurisdictions
- States are requiring “reasonable” security and considering ways to validate product security

# Product Development with an Eye to Certification

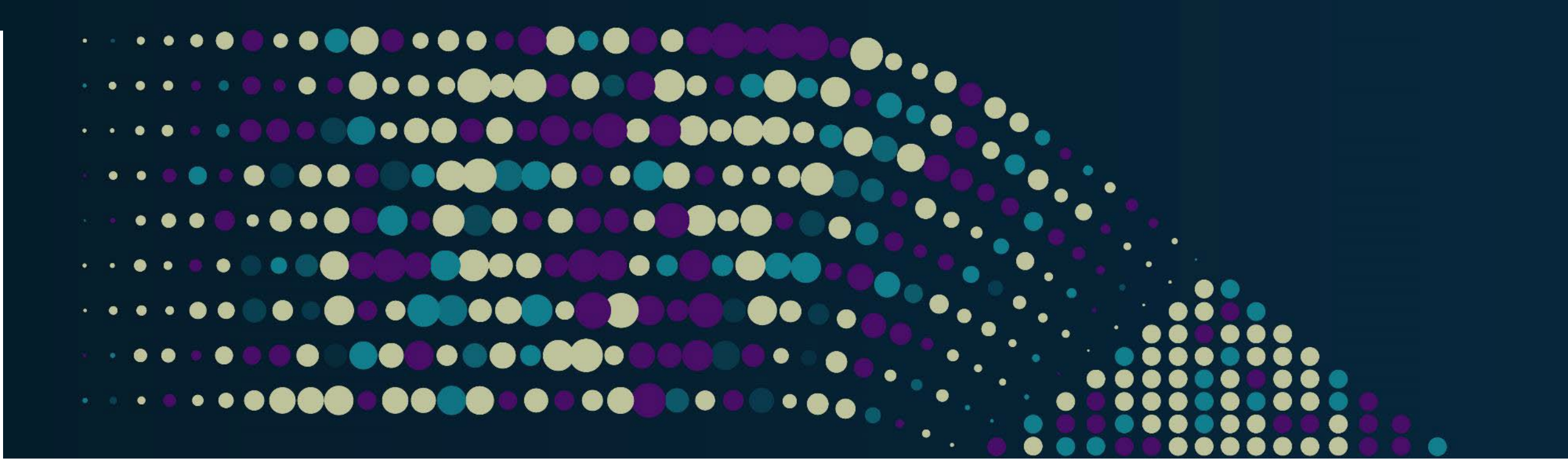
- System security engineering practices can be important
- Past vulnerability reports can be considered by the lab
- Documentation is important; CC and FIPS 140 are paper tigers
- Stated assumptions (e.g., the network is not a threat) have to pass the security giggle test
- Testing is critical to the third-party evaluation, so understand the testability of the security claims

# Additional Considerations

- Vulnerability management and disclosure programs
- Trustworthy supplier
- Secure software development lifecycle
- Incident response
- Cyber recovery solutions – counter ransomware
- Cyber insurance



# Gazing into the Crystal Ball

Section Subtitle

# Important Trends

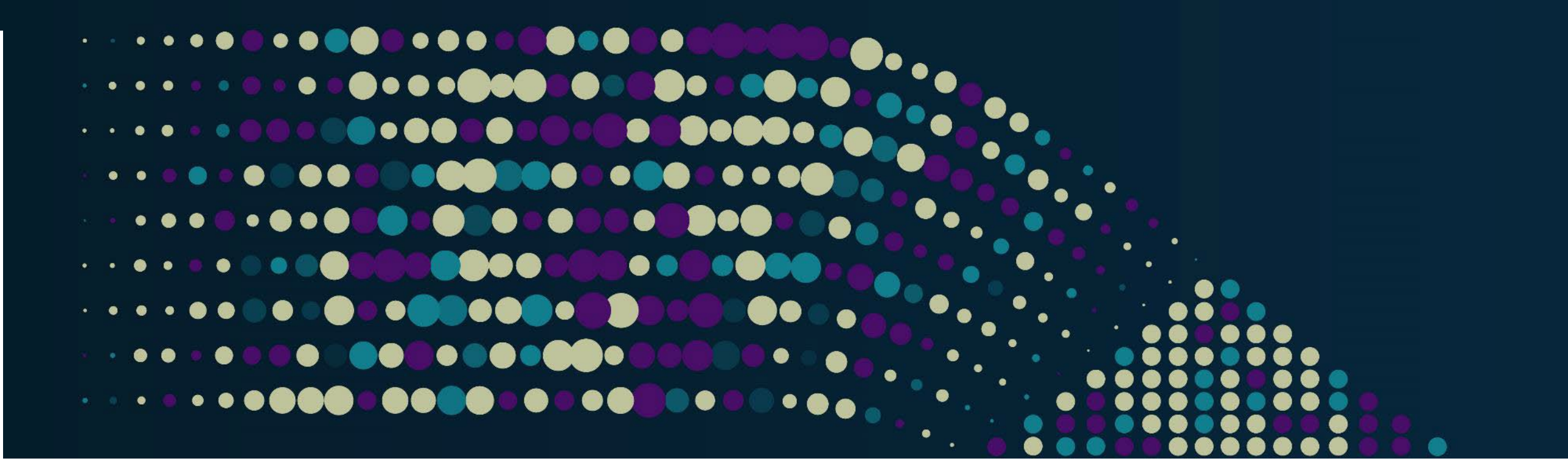
- “Reasonable” security has a risk-based aspect
- Supply chain security (approved vendors)
- Circular economy (reuse) – Data/Storage sanitization a prerequisite
- Product security certifications (FIPS 140, Common Criteria, etc.)
- Zero Trust Architectures (primarily US Government)
- Cloud/Edge computing
- Post Quantum Cryptography (PQC)

# Storage Security Event Horizon

- Secure eradication of data on storage devices and media
  - IEEE 2883-2022 provides specific requirements and guidance
  - Additional sanitization standards on verification and virtual storage
- Storage security added to security audit criteria
  - ISO/IEC 27040 (2nd Ed) storage security requirements/guidance (Dec 2023)
- Key Per IO for NVMe storage



# Summary

Section Subtitle

# Conclusions

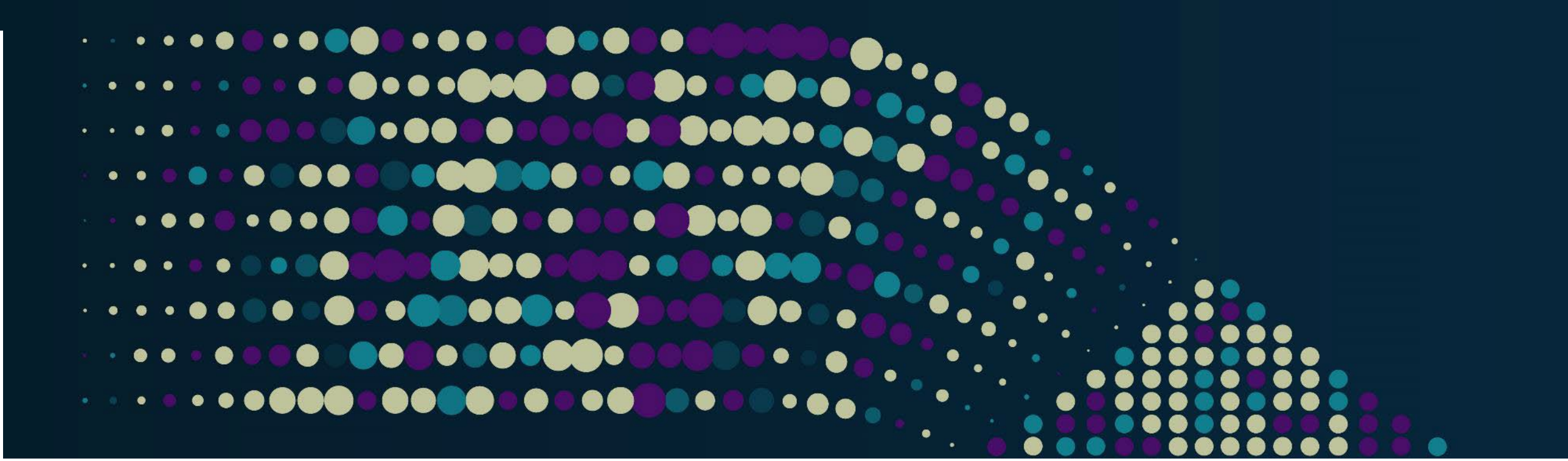
- Many of the security standards that are relevant to storage are new or recently updated; typically have requirements
- Exploiting some of the new storage security capabilities and practices can require significant changes
- The *trust, but verify* security mantra is practiced by many organization; vendors must earn and maintain this trust to be a supplier
- Prepare for the inevitable attacks

# Additional Resources

- SNIA Storage Security Resources
  - https://www.snia.org/security
- NIST Cybersecurity
  - https://www.nist.gov/cybersecurity
- ISO/IEC Information security, cybersecurity, privacy protections
  - https://www.iso.org/committee/45306.html
- Payment Card Security Standards Council
  - https://www.pcisecuritystandards.org/
- Center for Internet Security (CIS)
  - https://www.cisecurity.org/cis-benchmarks/



# Please take a moment to rate this session.

Your feedback is important to us.