SNIA COMPUTE + MEMORY + STORAGE SUMMIT

Architectures, Solutions, and Community
VIRTUAL EVENT, APRIL 11-12, 2023

2023 Cybersecurity & Privacy Landscape

Eric Hibbard, CISSP, FIP, CISA
Chair, INCITS/Cybersecurity & Privacy
eric.Hibbard@samsung.com

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!

Noteworthy Security Developments

- Nation state actors very active
- Access Brokers proliferate; target academic, technology, and industrials
- Adversaries move beyond malware; seeking access and persistence
- Technology giants targeted with data theft and extortion
- Social engineering used to overcome multi-factor authentication (MFA)
- Increased focus on cloud account discovery
- Increases in destructive actions such as account access removal, data destruction, resource deletion and service stoppage
- Hacktivism continues in support of numerous political ideals

Noteworthy Privacy Developments

- Increased regulatory activity
- Over 2/3 of the world’s population will have their personal data covered by modern privacy regulations
- Organizations required to implement a minimum level of security to prevent data loss, information leaks and other unauthorized data processing operations
- Restrictions on automated decisions on data changes that significantly affect an individual
- No data science without algorithmic accountability

SNIA COMPUTE + MEMORY + STORAGE SUMMIT

Architectures, Solutions, and Community
VIRTUAL EVENT, APRIL 11-12, 2023

Key Trends for 2023

Adversarial Expectations

- Ransomware will be back in new, more dangerous, blended forms.
- More attacks against non-traditional technology, from cars to toys to smart cities
- More critical infrastructure attacks that impact society
- Sophisticated firmware attacks will become more widespread
- More nation state cyber attacks against primary targets and allies
- Increased focus on 5G and APIs

Defensive Responses

- Adoption of zero trust
- Prosecution of Insiders
- Cyber insurance changes; harder to get and less coverage
- Enterprises veering away from point solutions and moving towards platforms to reduce complexity
- Use of public cloud computing and digital transformations grows
- Proliferation of cyber and privacy regulations; harmonization is elusive

SNIA COMPUTE + MEMORY + STORAGE SUMMIT

Architectures, Solutions, and Community
VIRTUAL EVENT, APRIL 11-12, 2023

Please take a moment to rate this session.

Your feedback is important to us.