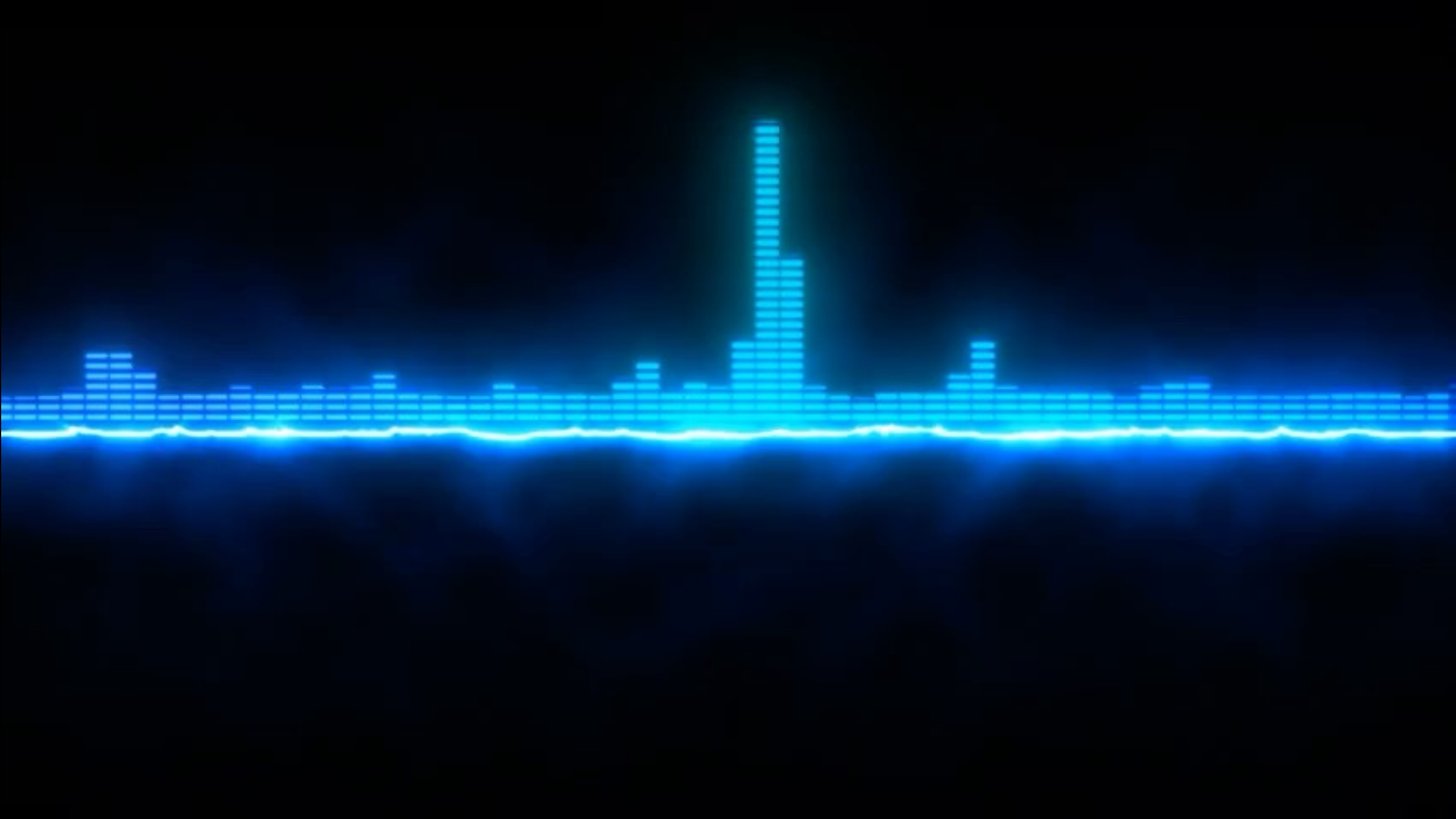
Jake Marcinko

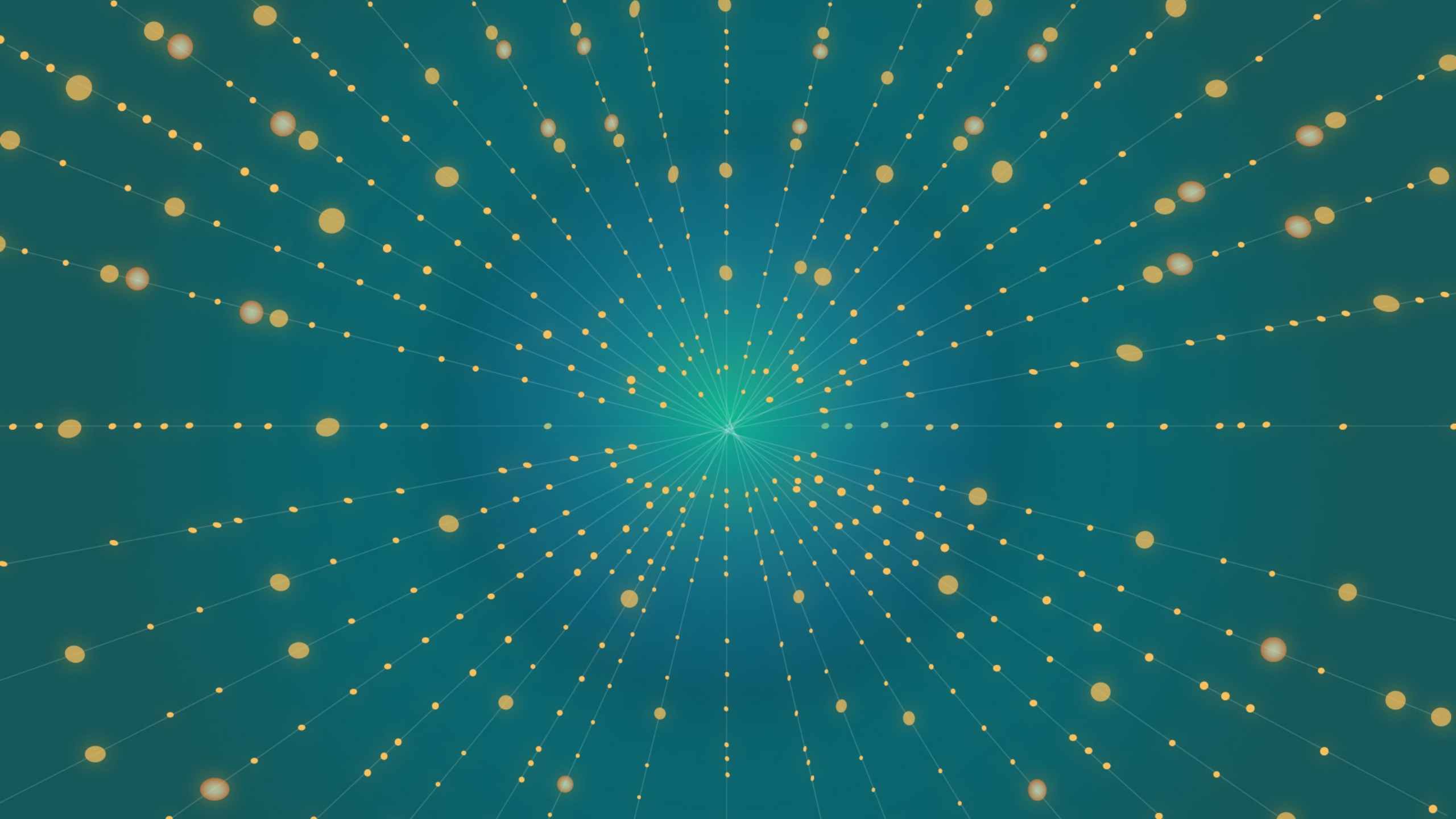
Senior Manager, Solution Standards
PCI Security Standards Council

PCI Security Standards Council®


DIGITAL REMOTE
02
POWER
VOLUME
CHANNEL
MTV


10



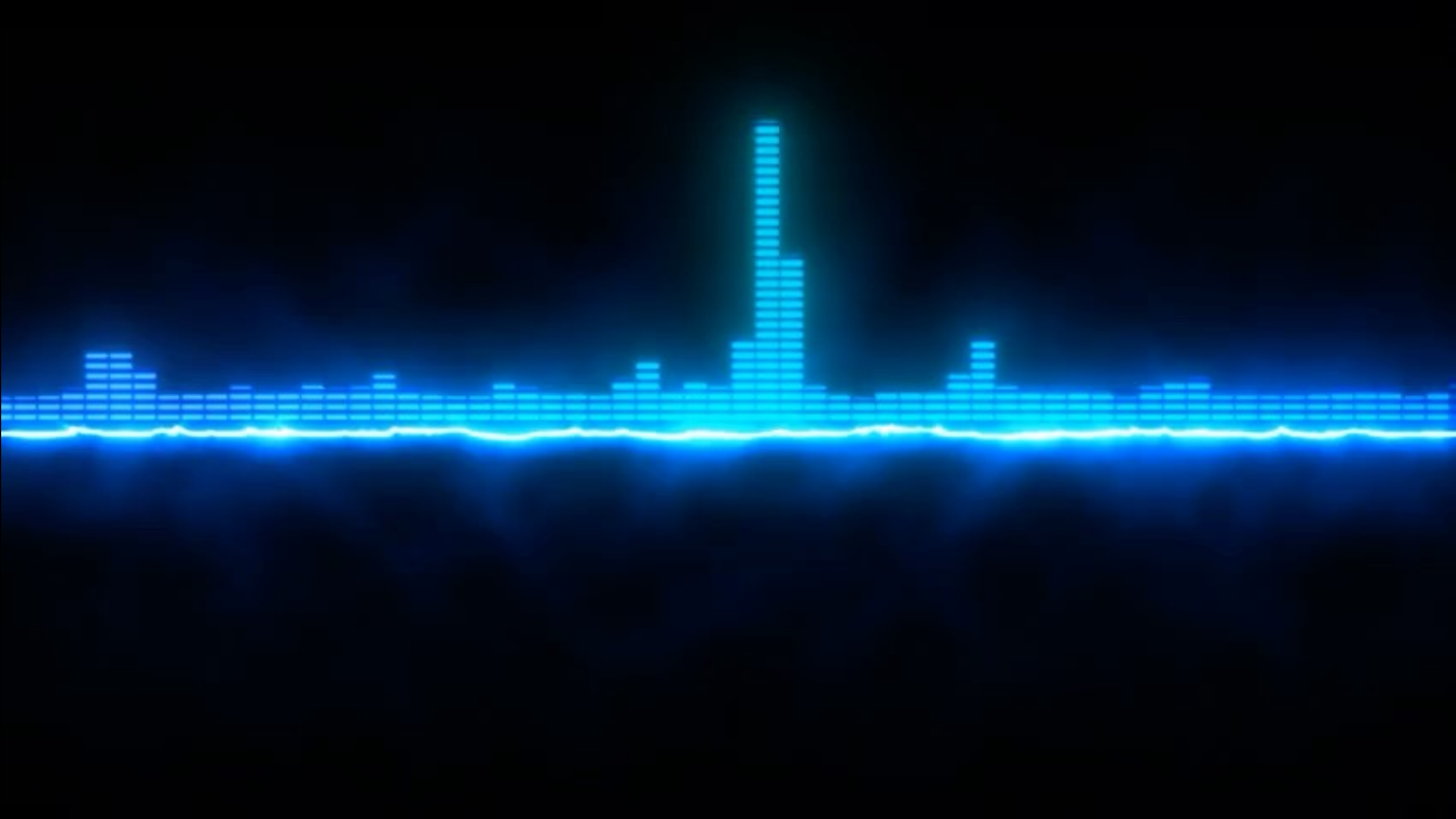


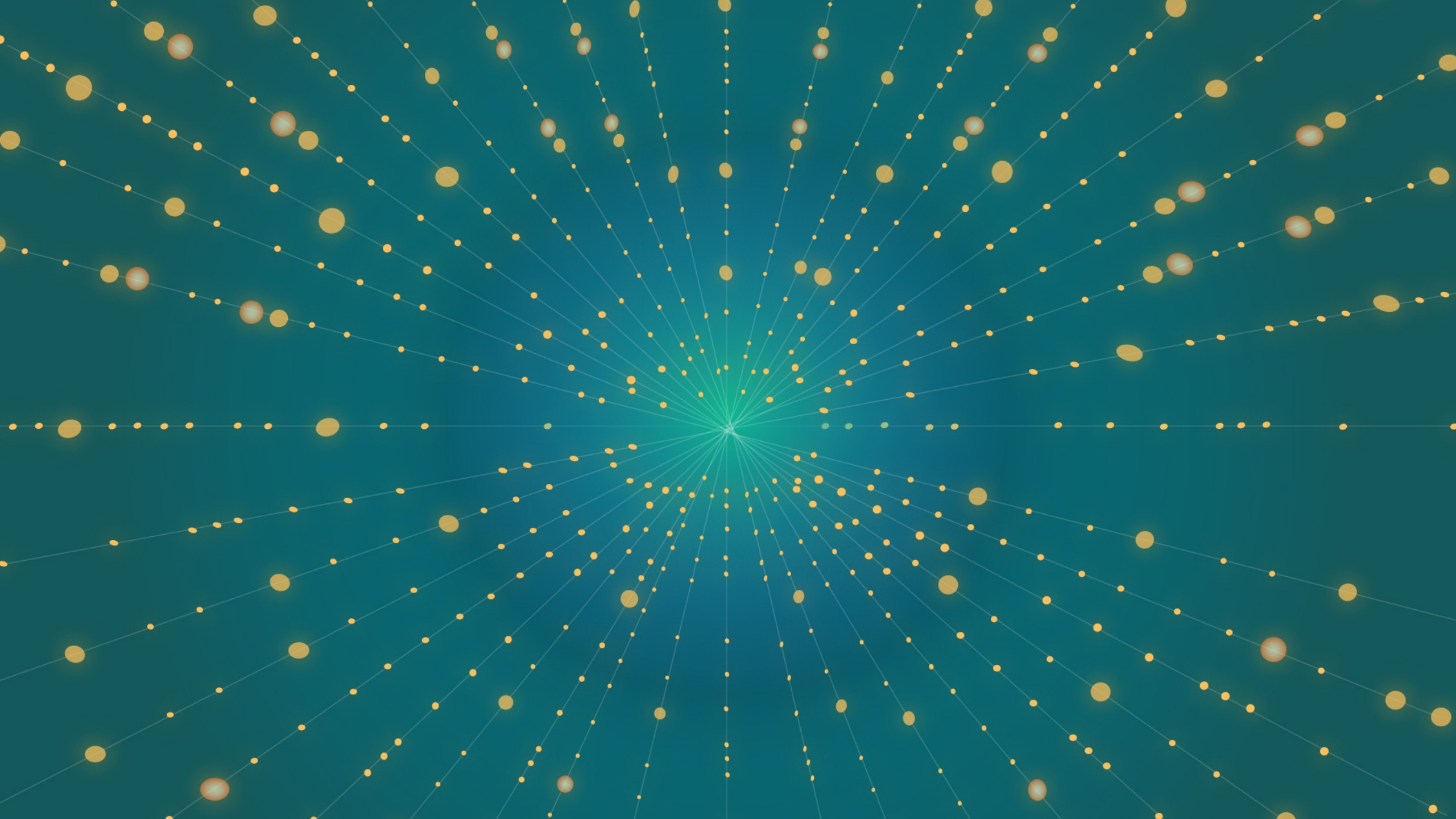
Software Security Principle #1

Software Security is a Function of Software Quality

- Success is dependent on customer satisfaction and trust.
- Quality is a major factor in building customer trust.
- Lower quality = less satisfaction = less trust = fewer customers.
- Once trust erodes, it is difficult to recover.

PCI Security Standards Council





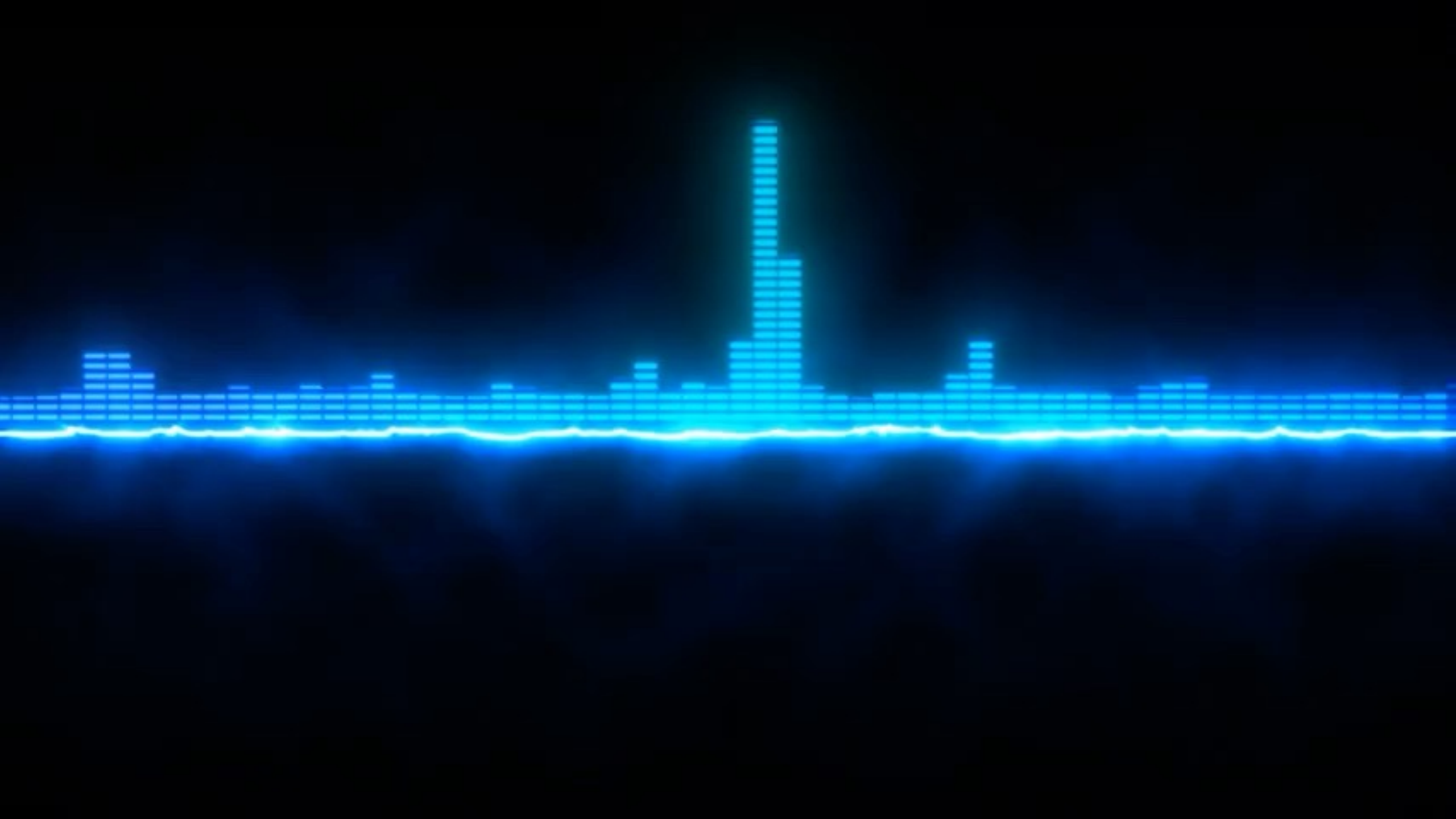

EDMUND FITZGERALD

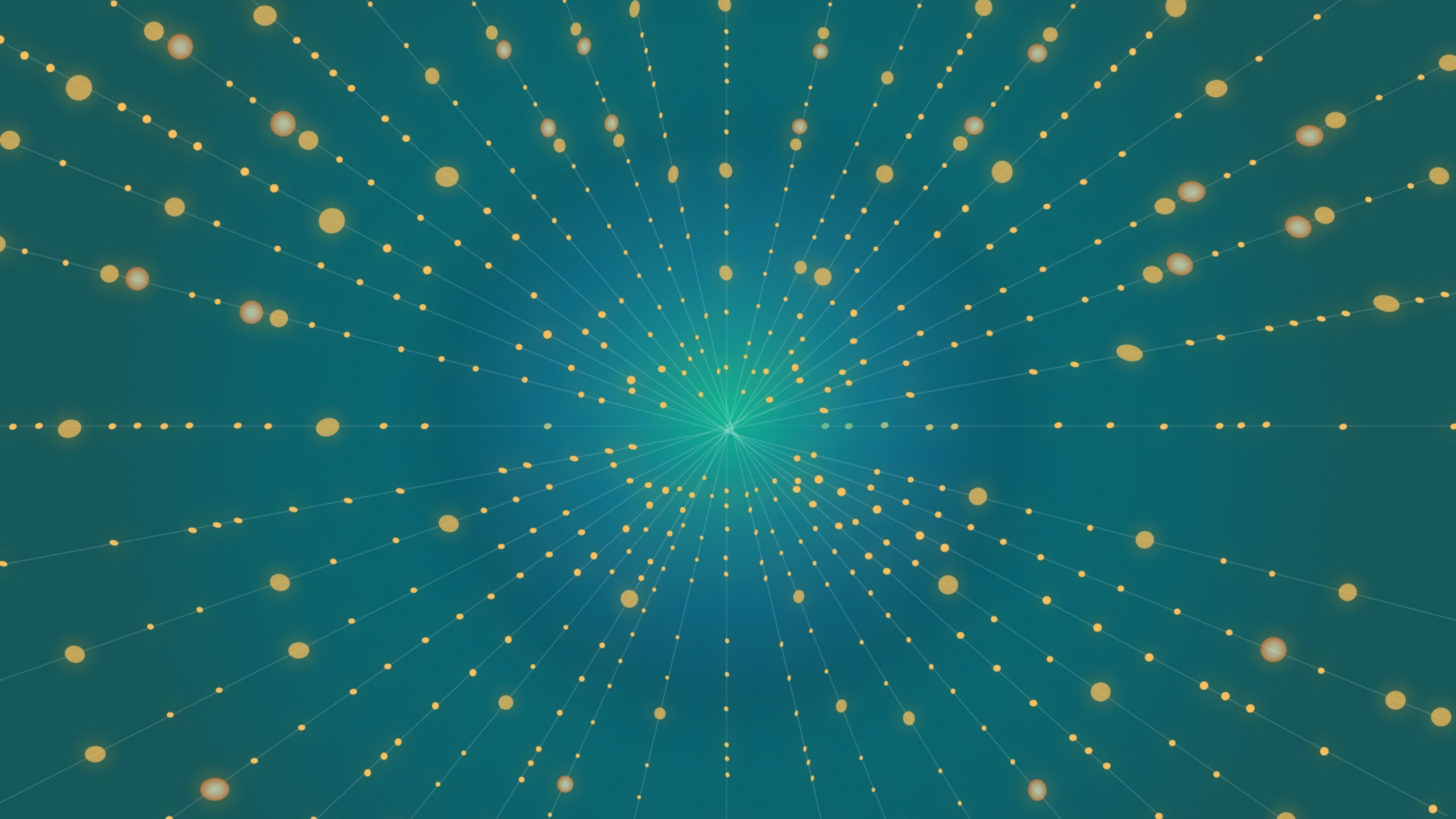
Software Security Principle #2

Minor Security Issues Can Have Major Repercussions

- The Internet is an extremely hostile environment.
- Software must be designed to withstand such conditions.
- Knowing one's weaknesses and how they may be exploited is key to one's survival.
- Insufficient testing and mitigation of threats and vulnerabilities can have catastrophic consequences.

PCI Security Standards Council





Software Security Principle #3

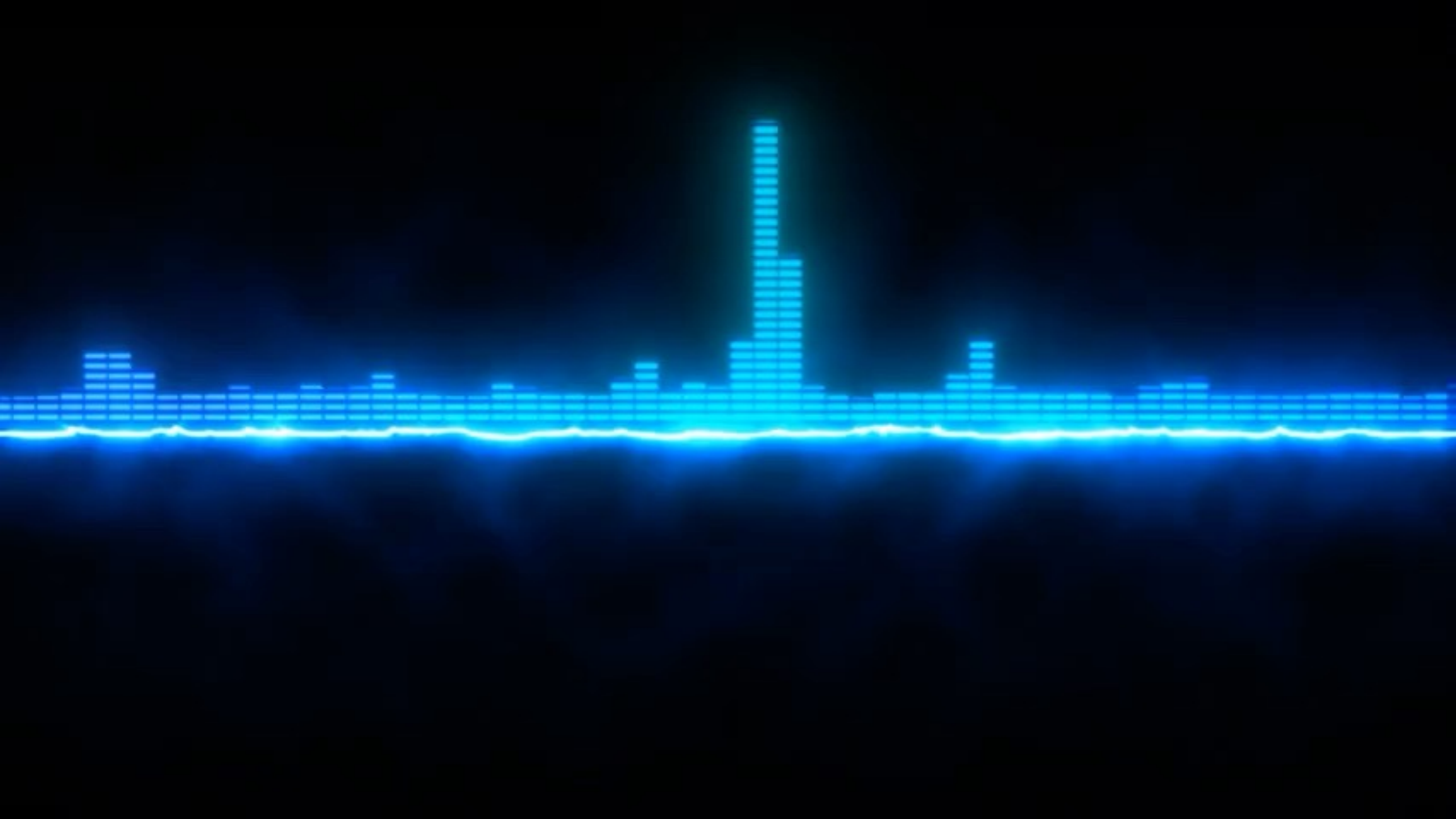
Software Security Requires Continuous Evolution

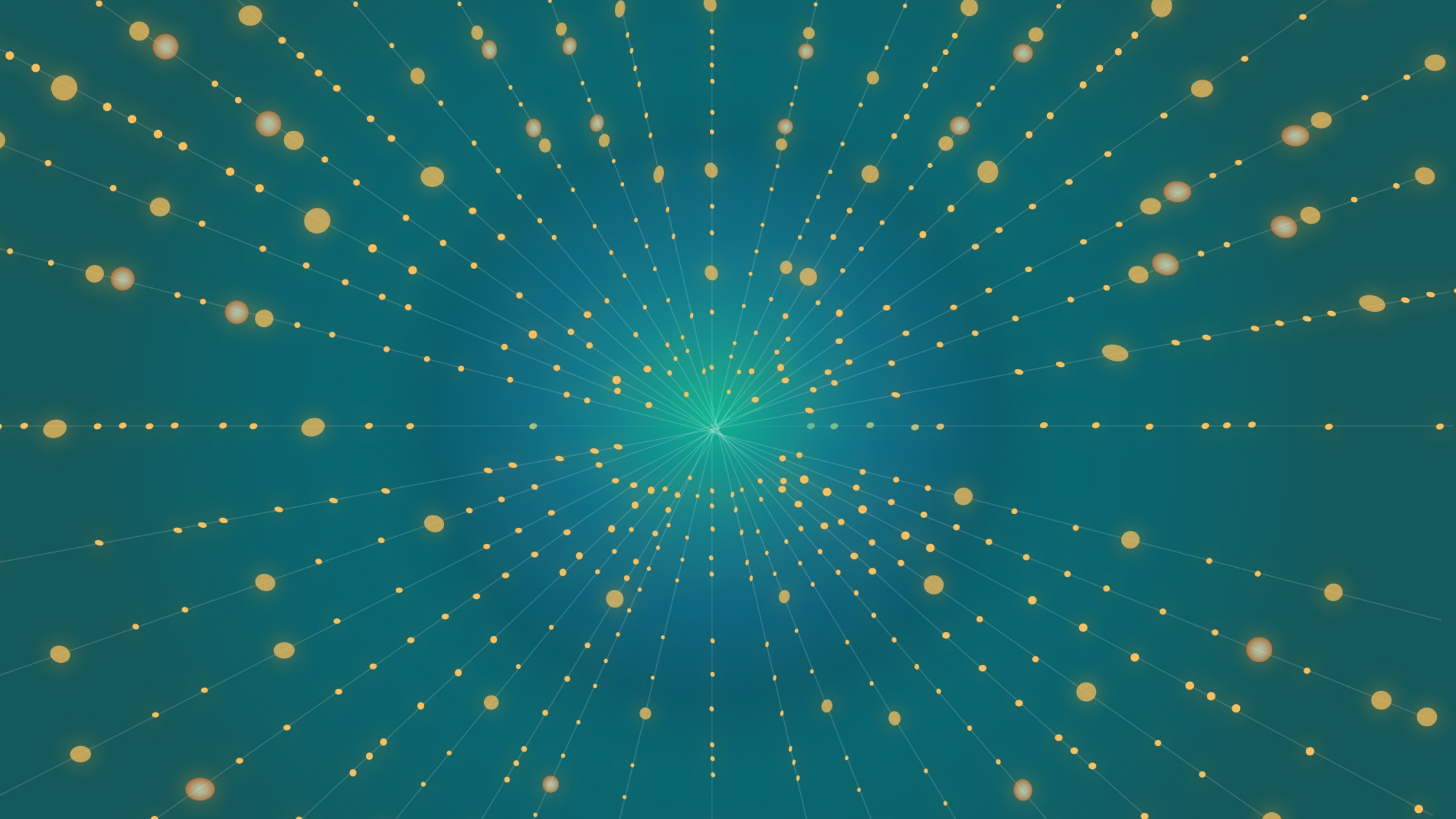
- Innovation often introduces new, unforeseen vulnerabilities.
- Threats aren’t static, so why are security practices often so?
- Maintaining software security requires continuous evolution in concert with product innovation.

PCI Security Standards Council

PCI Security Standards Council

Applying These Principles with the Web Software Module



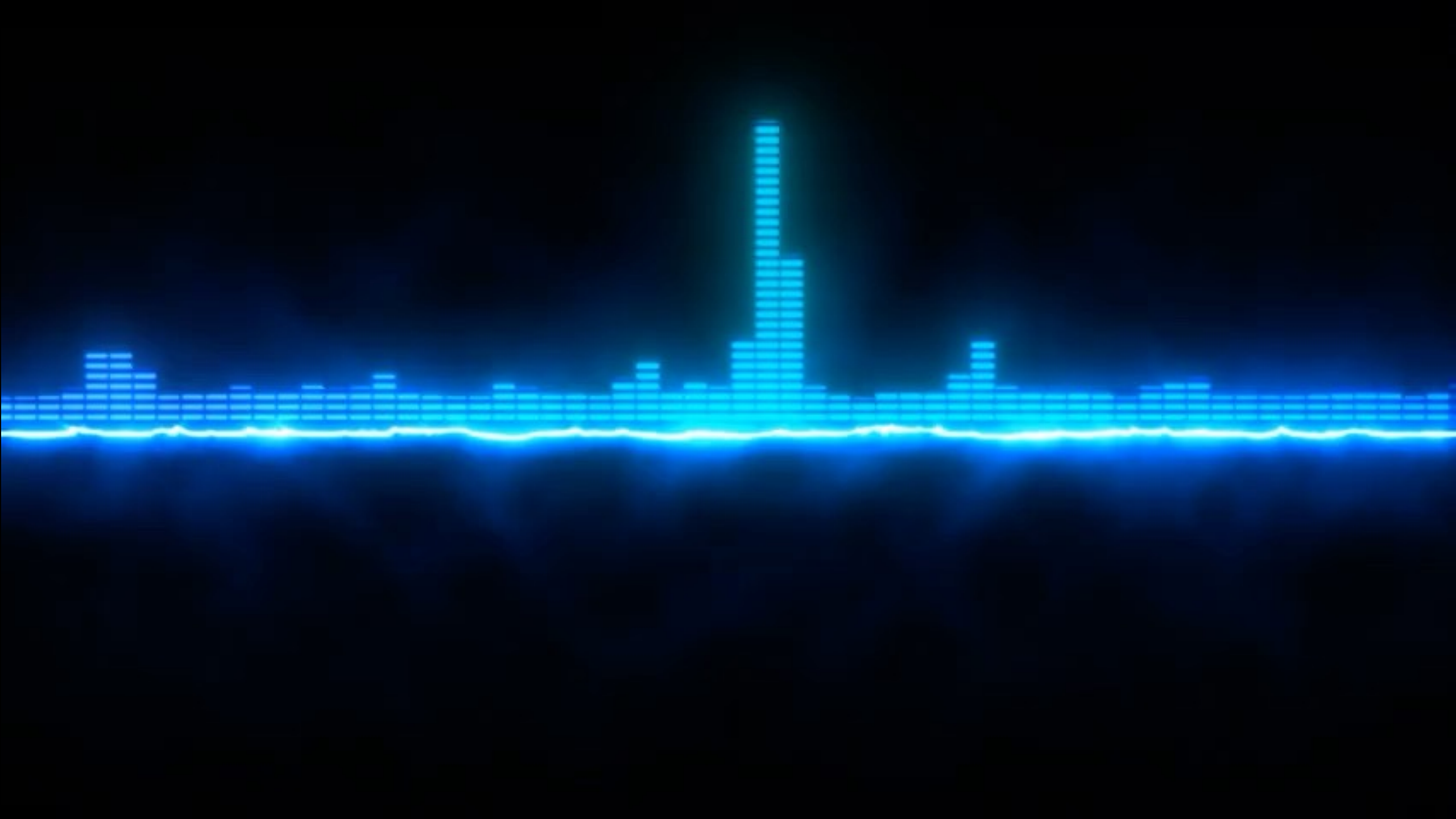


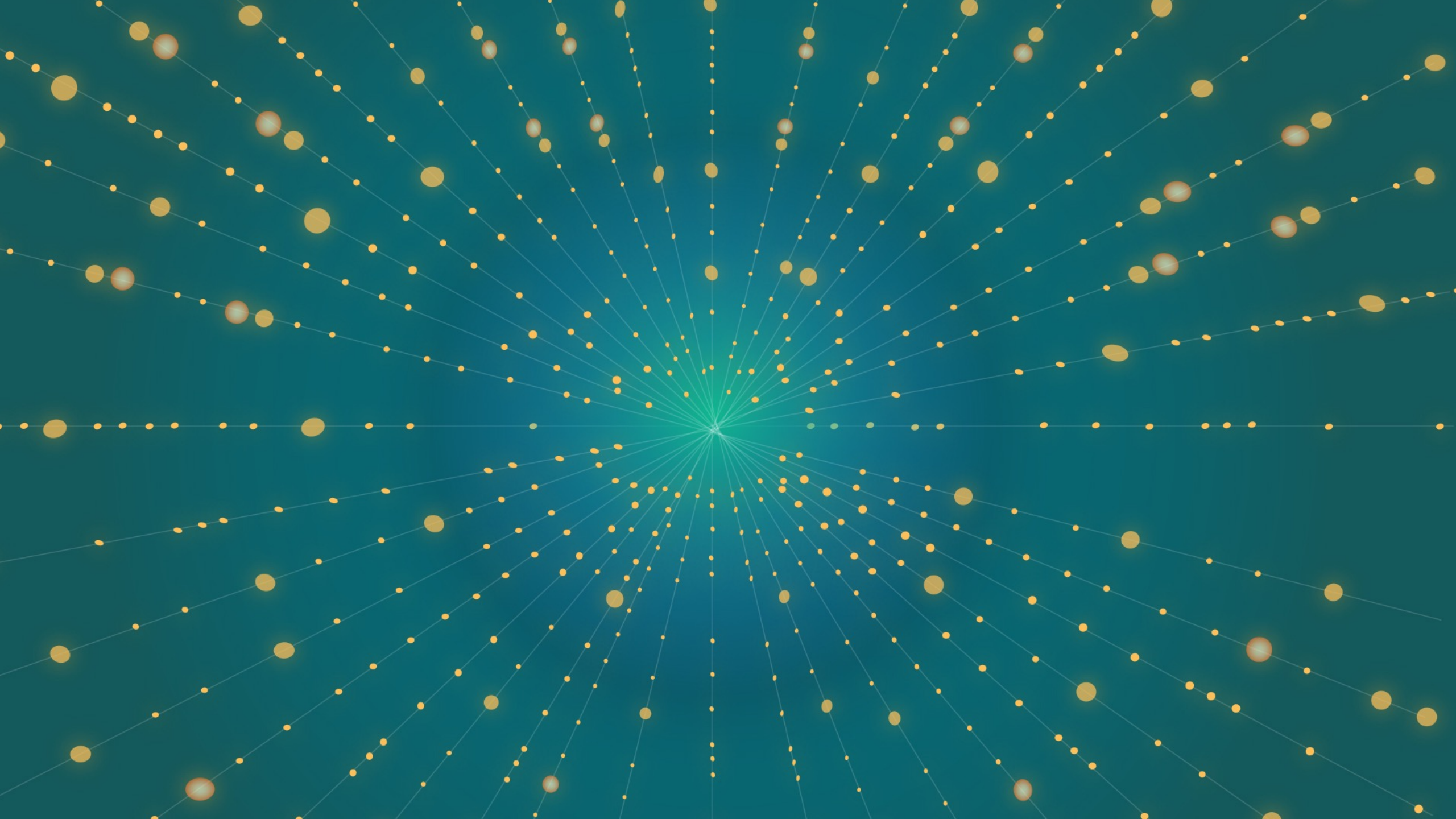
Applying These Principles

Objective C.1: Know Your Product Composition

- Cannot ensure software security & quality if you don’t know the composition of your own products.
- Vulnerabilities in third-party software components & services can lead to broader product vulnerabilities.
- Requires a detailed inventory of components, sub-components, and services (Software Bill of Materials or “SBOM”).

PCI Security Standards Council





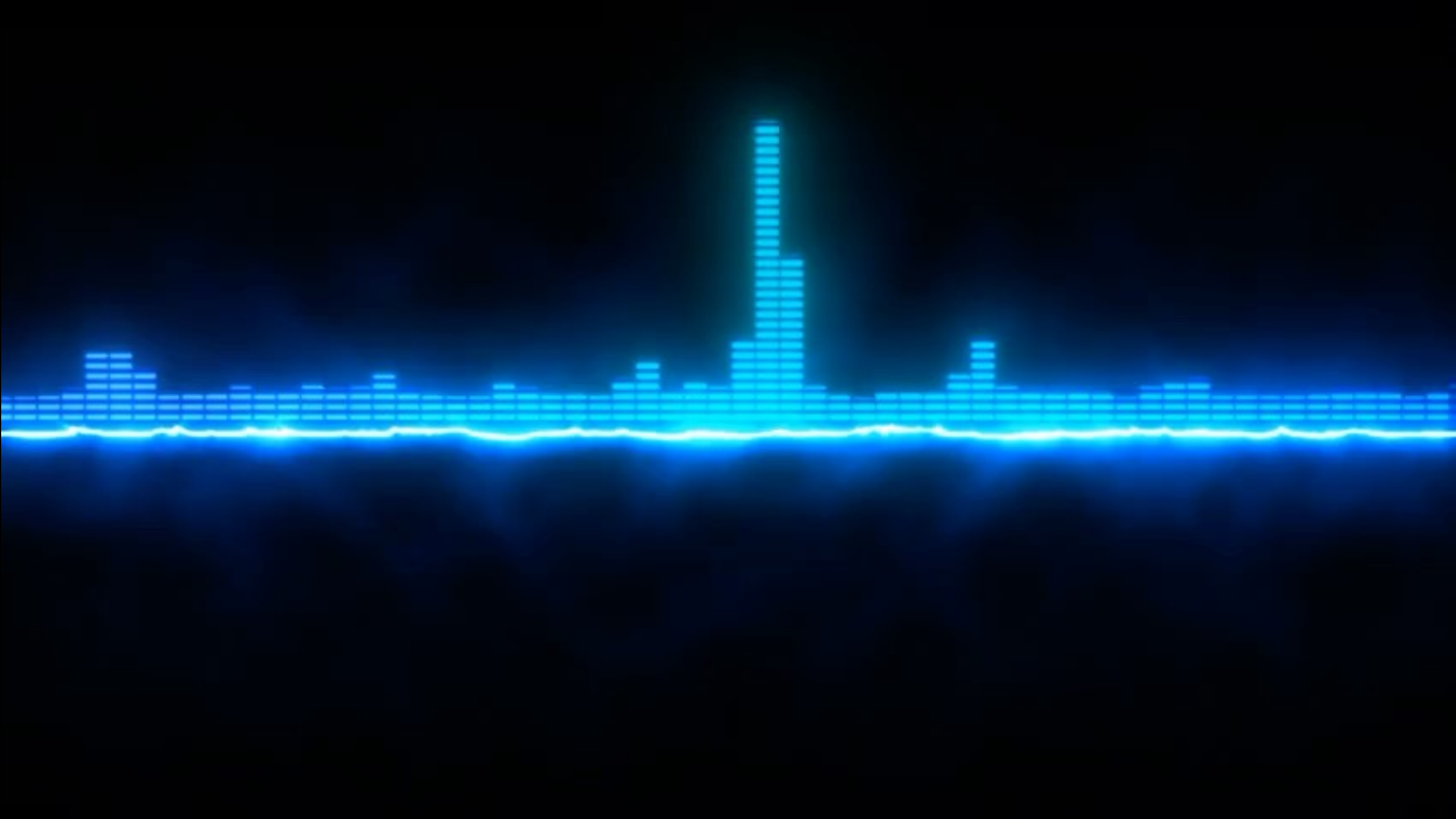

HIWATT
HIWATT
HIWATT
HIWATT
HIWATT
HIWATT

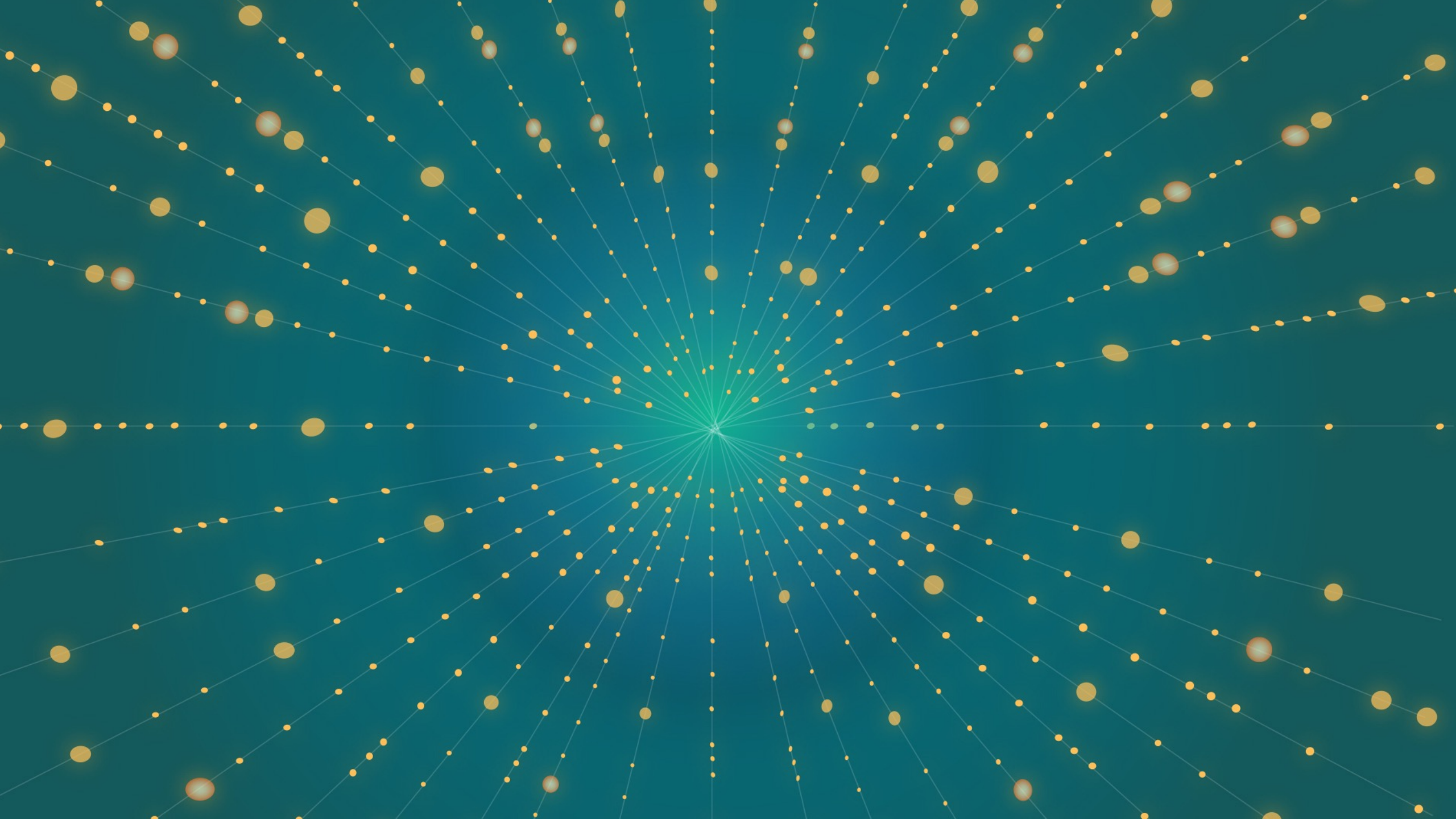
Applying These Principles

Objective C.2: Know Your Users

- Access control is fundamental to software security.
- Protecting the software and software assets requires robust authentication & access control capabilities.
- Failure to do so could enable unauthorized users to access sensitive functions and data or increase the software's attack surface.

PCI Security Standards Council

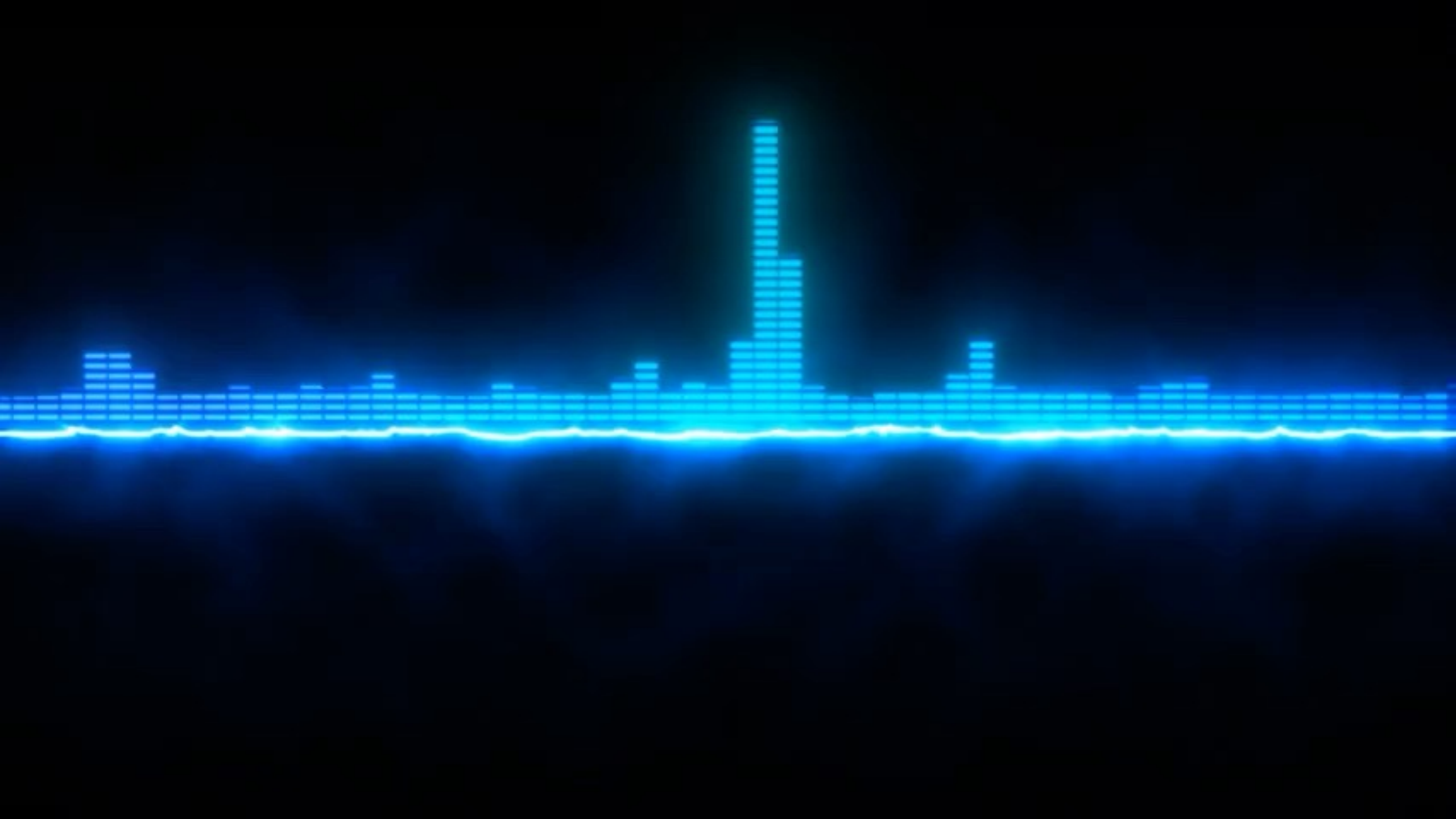


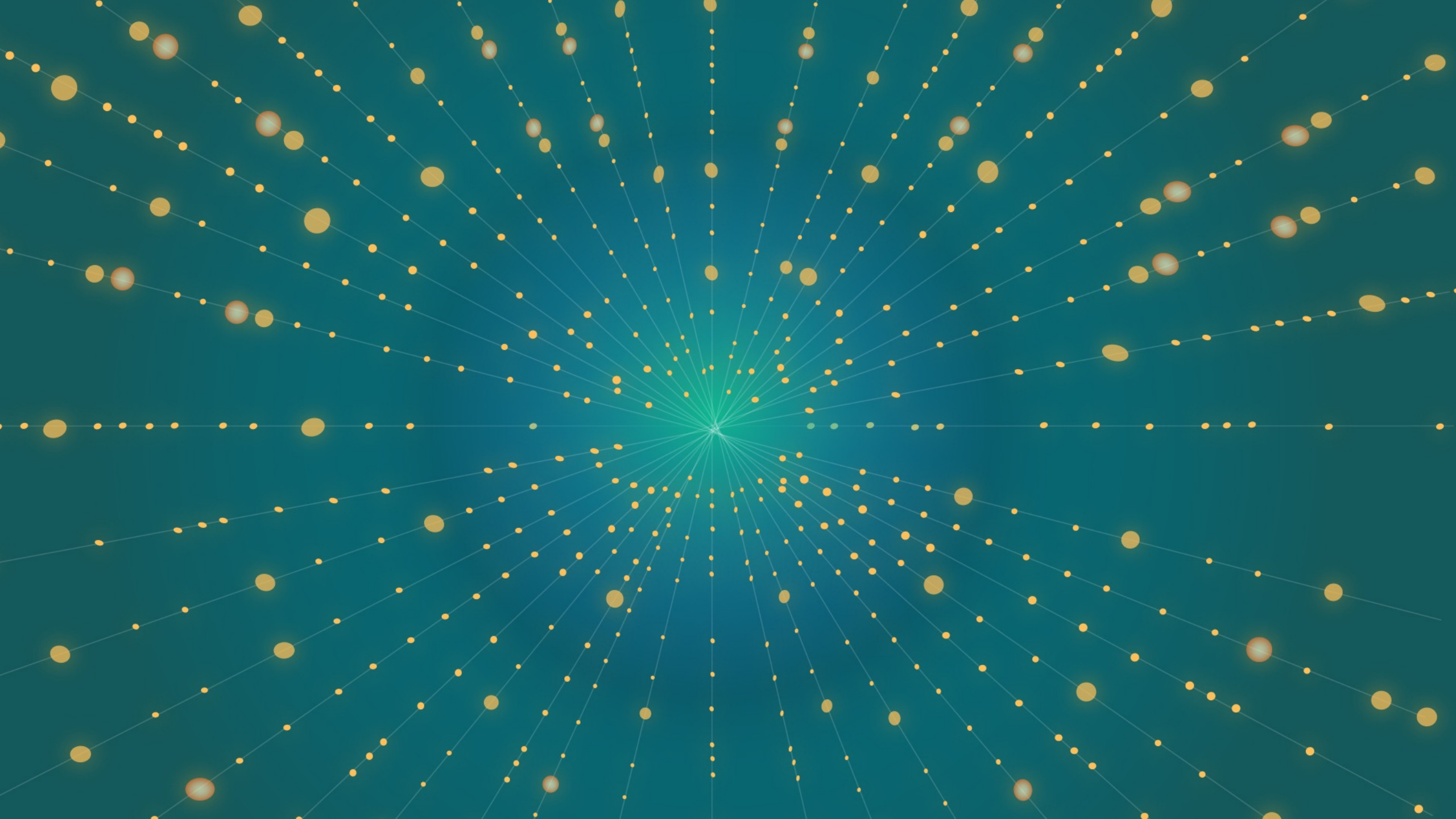


Applying These Principles

Objective C.3: Know Your Weaknesses and Address Them

- Identify and address vulnerabilities and design weaknesses.
- Do not repeat or reintroduce previously resolved vulnerabilities.
- Apply what you learn to other similar scenarios.
- Do not blindly trust user input. Verify input and output are valid and/or properly formatted.

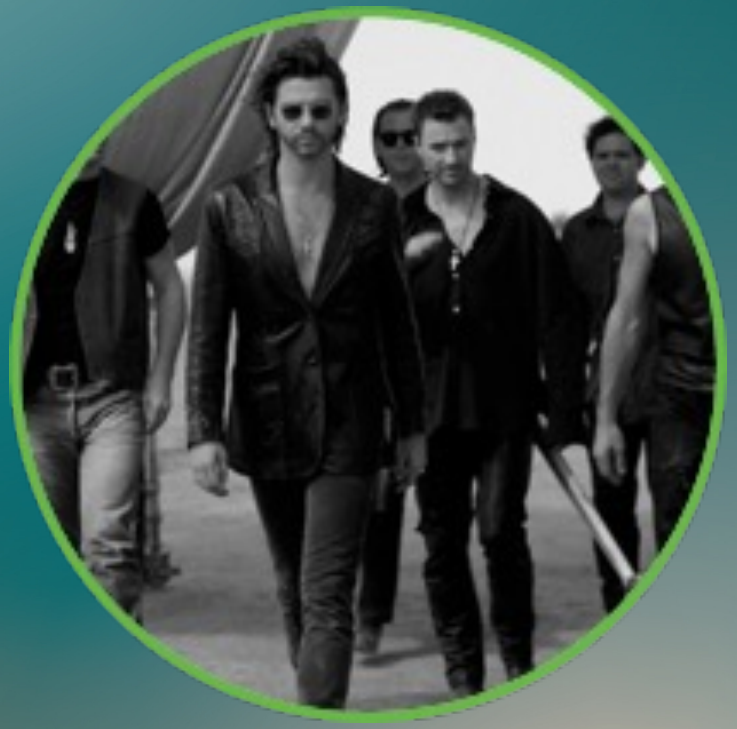





JPG
XVI

Applying These Principles

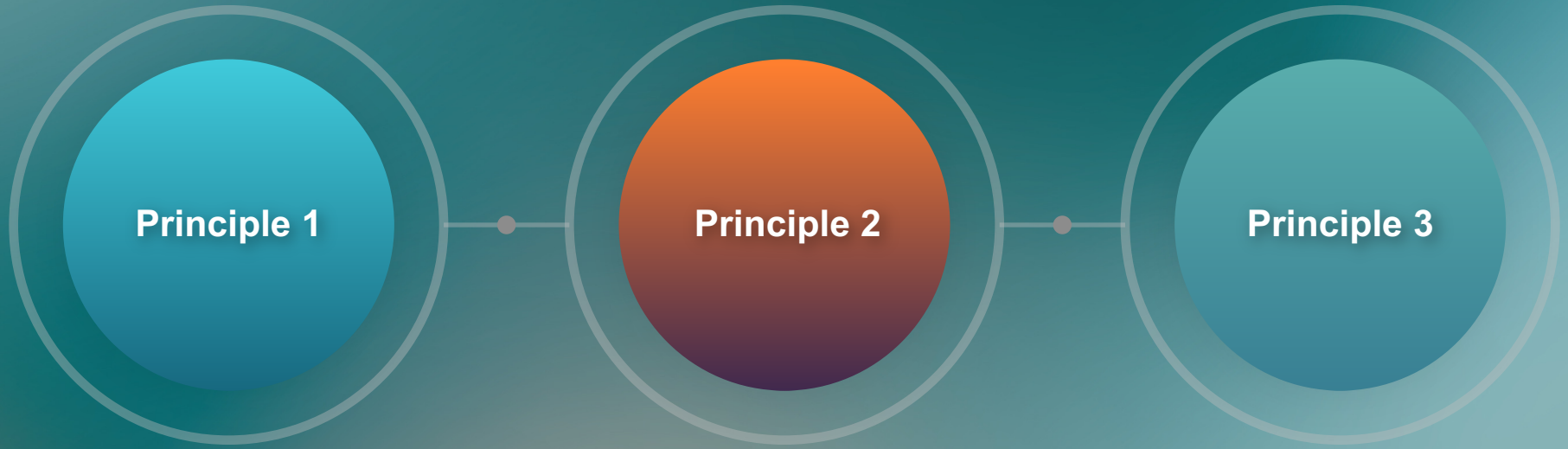
Objective C.4: Know Your Assets and Protect Them



- If you do not know your assets or their value, then you cannot adequately protect them.
- Someone wants what you have.
- Inadequately protected assets will almost certainly be compromised.

PCI Security Standards Council

Summary of Key Principles



Software Security is a Function of Software Quality.

Minor Security Issues Can Have Major Consequences.

Software Security Requires Continuous Evolution.

PCI Security Standards Council

Summary of Required Actions

C.1 Web Software Components and Services

Know your product composition.

C.3: Web Software Attack Mitigation

Know your weaknesses and address them

C.2: Web Software Access Controls

Know your users and ensure they are who they claim to be.

C.4: Web Software Communications

Know your assets and protect them.

PCI Security Standards Council

Thank You!

PCI Security Standards Council®

Europe Community Meeting 2023

PCI Security Standards Council