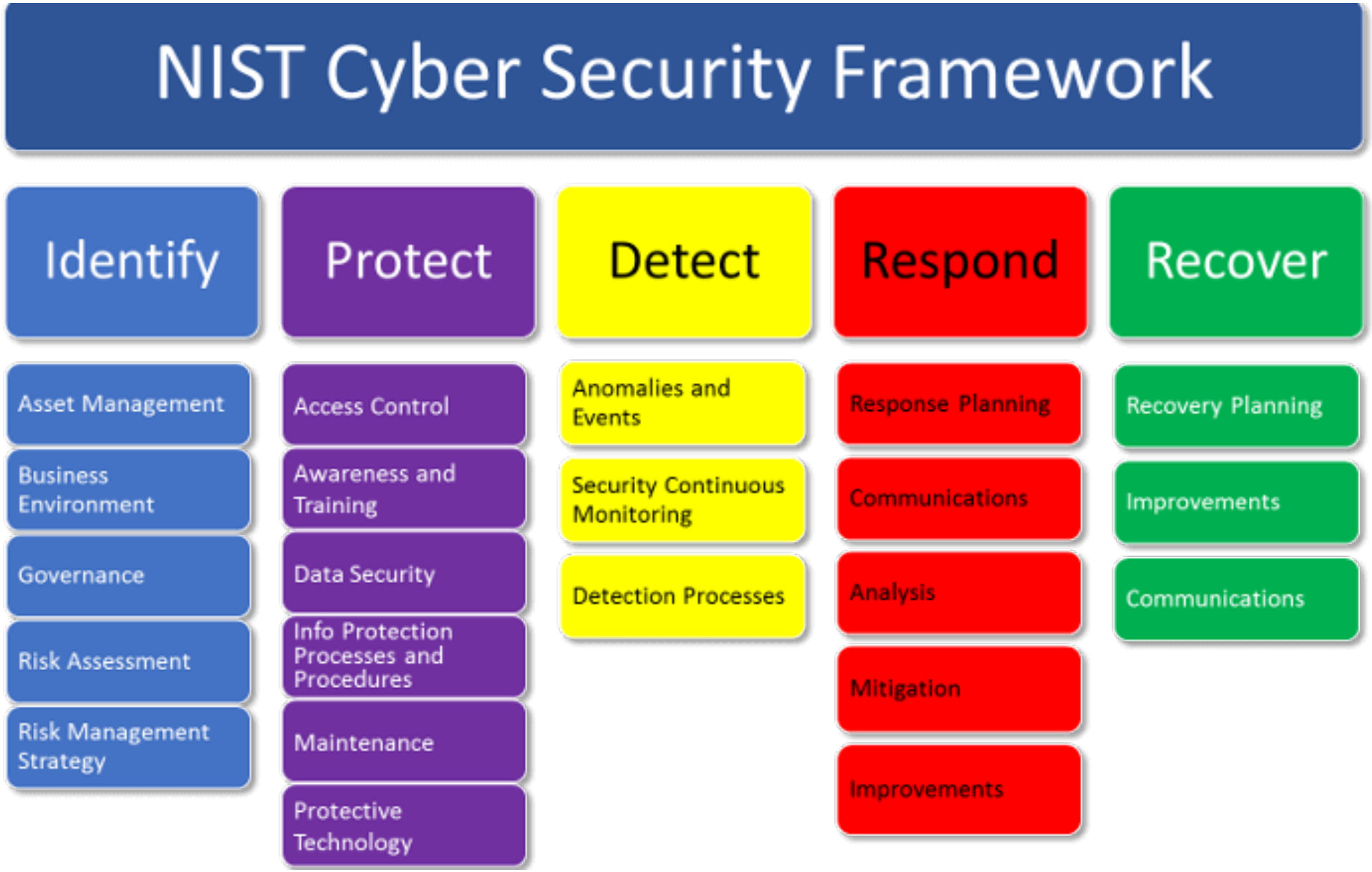
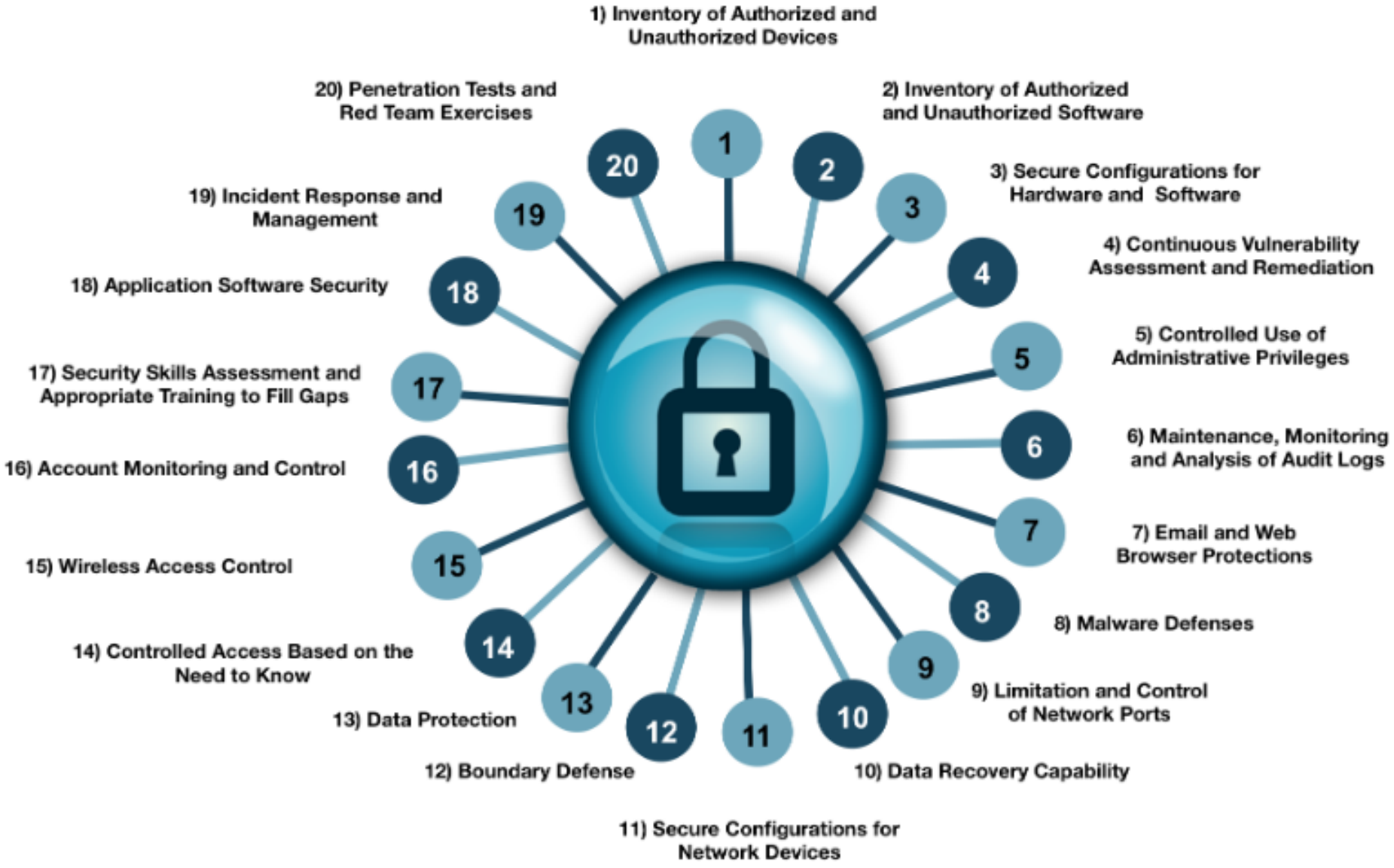
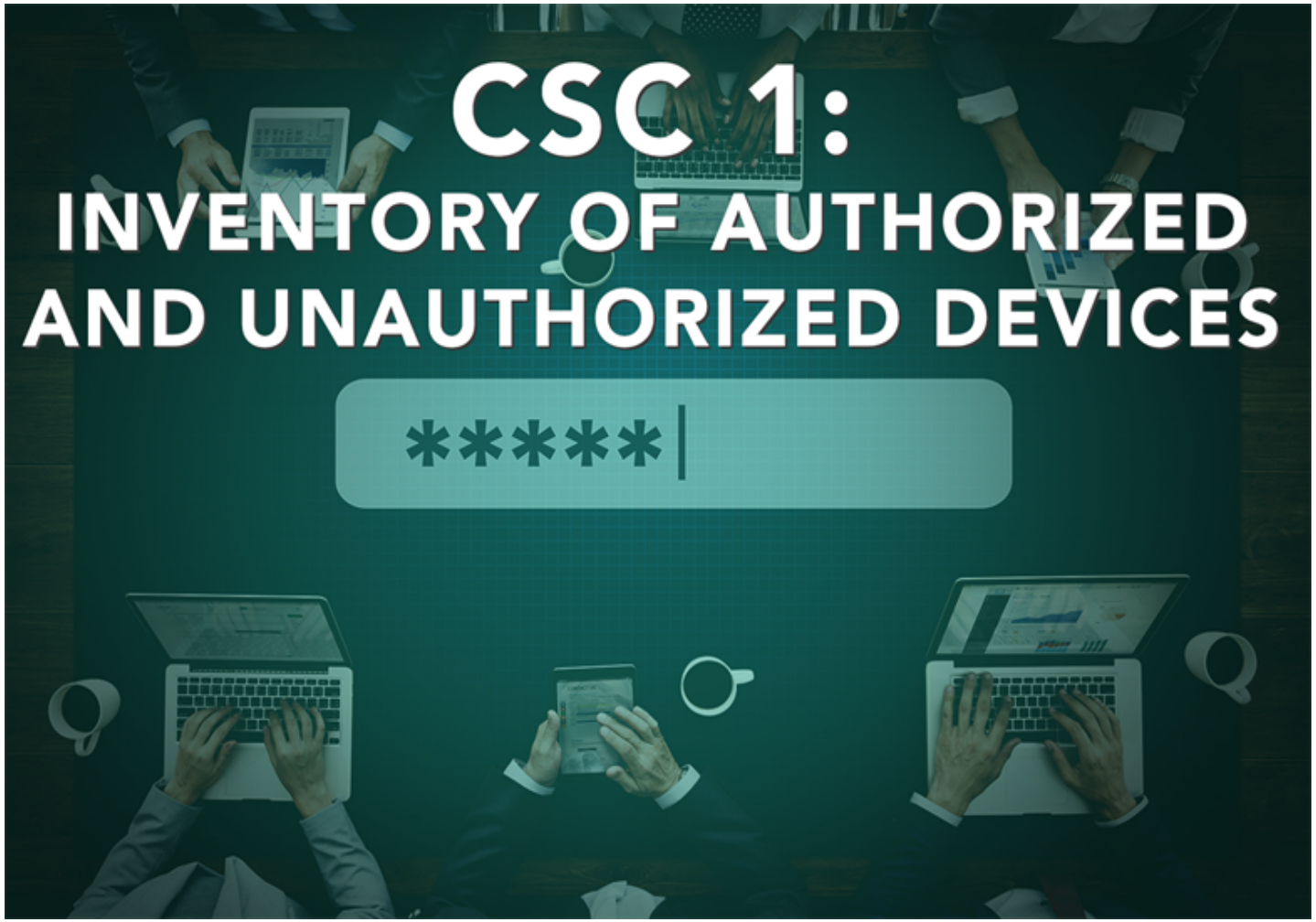
20 CRITICAL SECURITY COMPONENTS

NIST CSF

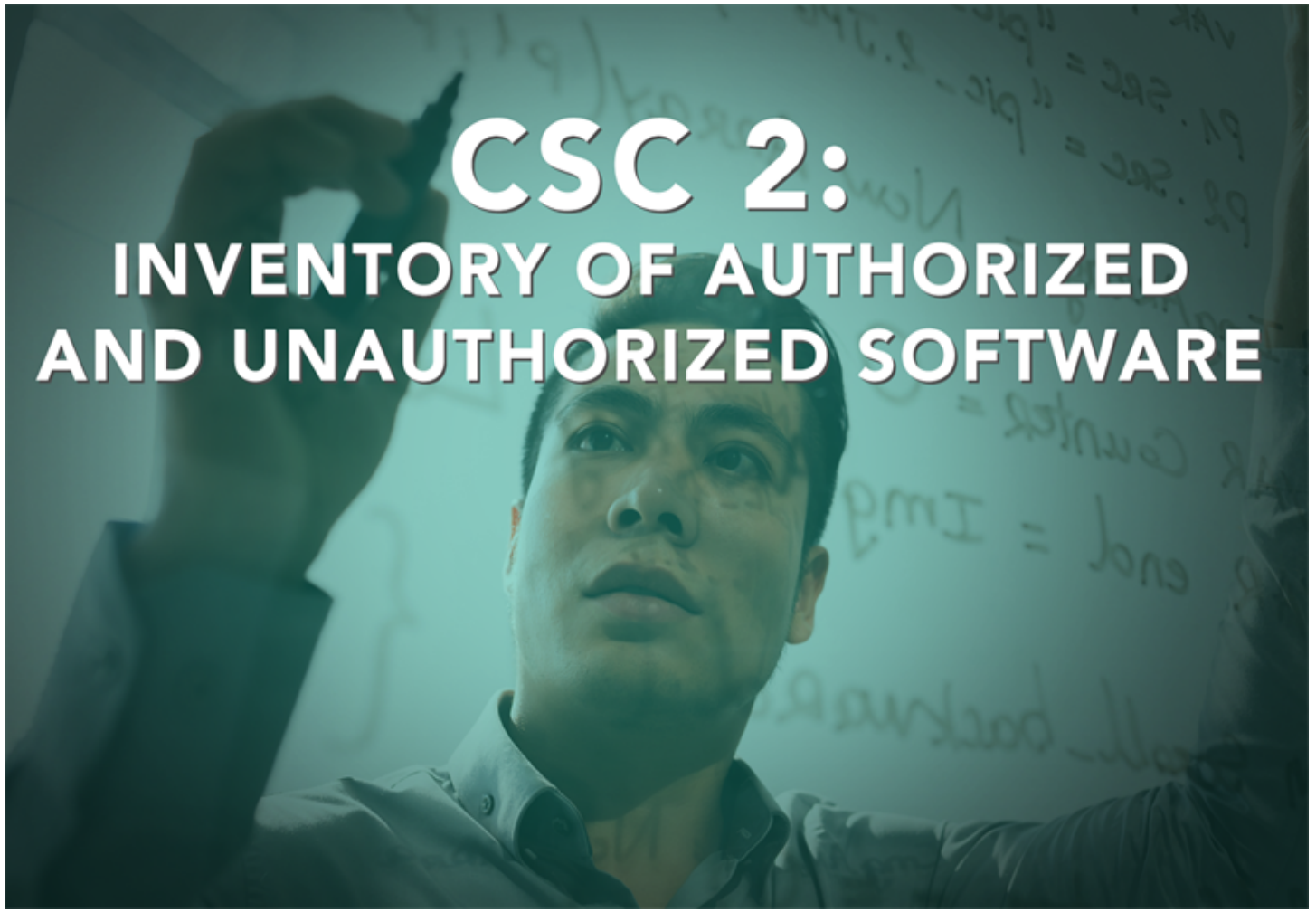

NIST Cyber Security Framework
Identify
Asset Management
Business Environment
Governance
Risk Assessment
Risk Management Strategy
Protect
Access Control
Awareness and Training
Data Security
Info Protection Processes and Procedures
Maintenance
Protective Technology
Detect
Anomalies and Events
Security Continuous Monitoring
Detection Processes
Respond
Response Planning
Communications
Analysis
Mitigation
Improvements
Recover
Recovery Planning
Improvements
Communications


1) Inventory of Authorized and Unauthorized Devices
2) Inventory of Authorized and Unauthorized Software
3) Secure Configurations for Hardware and Software
4) Continuous Vulnerability Assessment and Remediation
5) Controlled Use of Administrative Privileges
6) Maintenance, Monitoring and Analysis of Audit Logs
7) Email and Web Browser Protections
8) Malware Defenses
9) Limitation and Control of Network Ports
10) Data Recovery Capability
11) Secure Configurations for Network Devices
12) Boundary Defense
13) Data Protection
14) Controlled Access Based on the Need to Know
15) Wireless Access Control
16) Account Monitoring and Control
17) Security Skills Assessment and Appropriate Training to Fill Gaps
18) Application Software Security
19) Incident Response and Management
20) Penetration Tests and Red Team Exercises

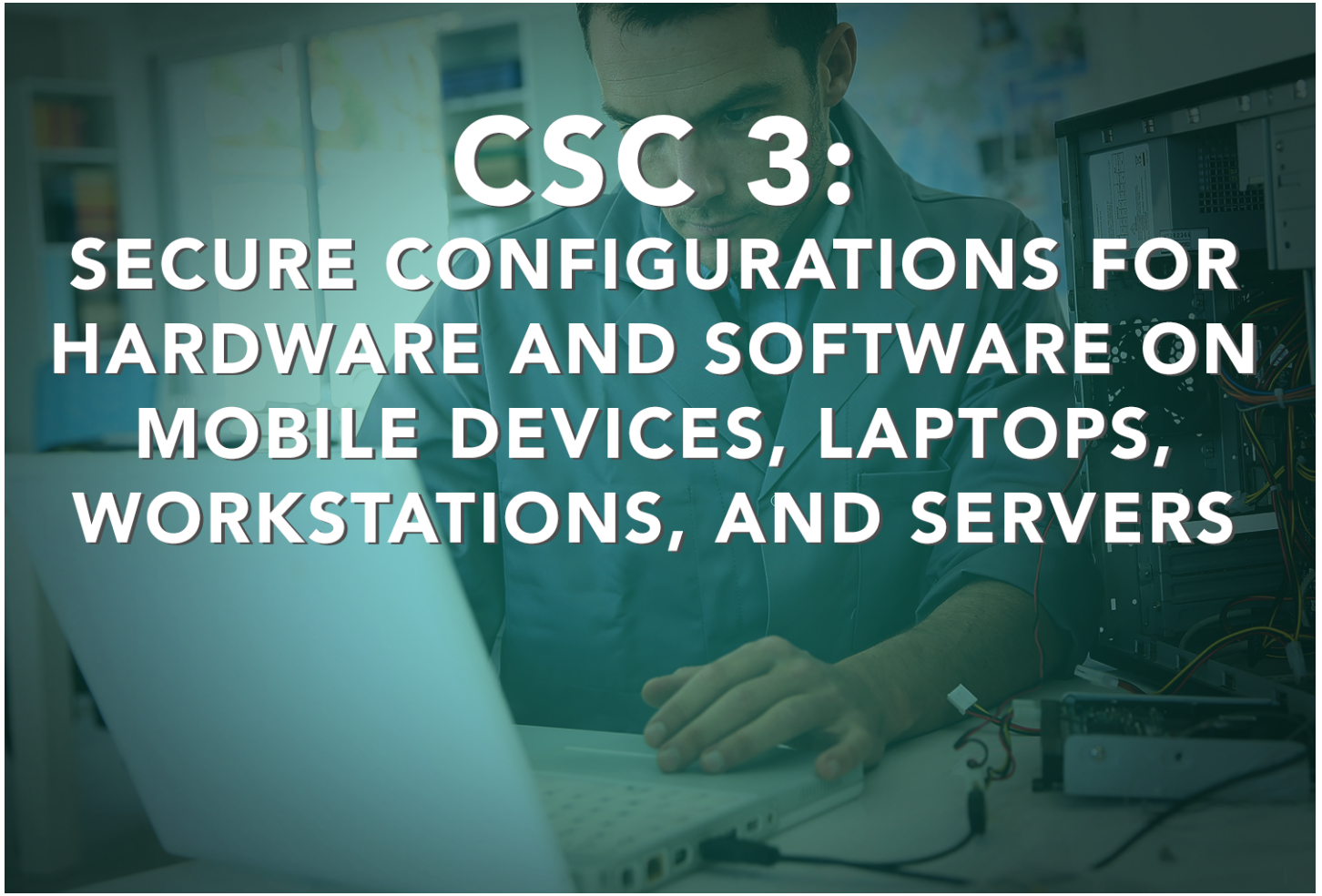
- Critical Control 1: Inventory of Authorized and Unauthorized Devices



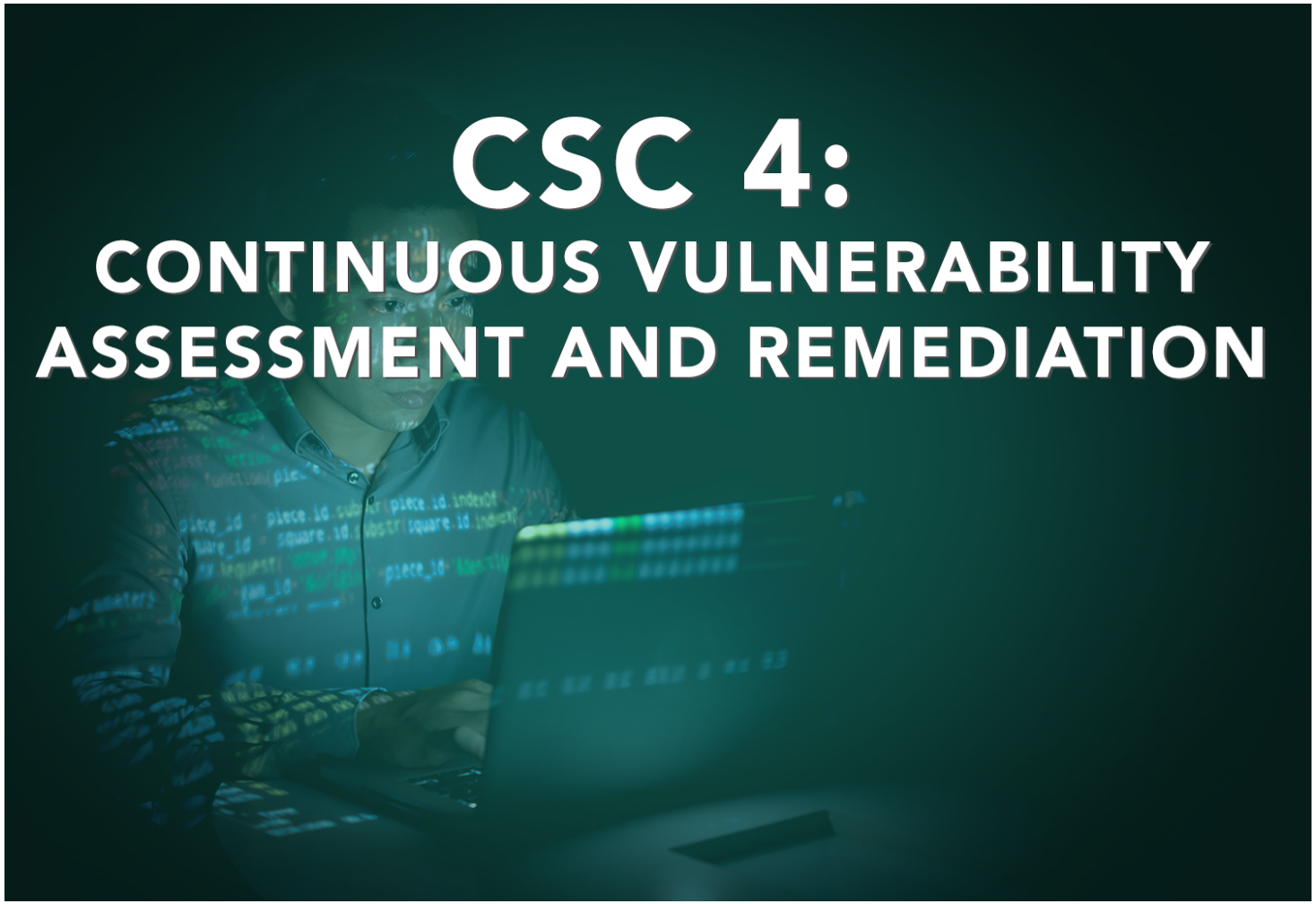
- Critical Control 2: Inventory of Authorized and Unauthorized Software



- Critical Control 3: Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers

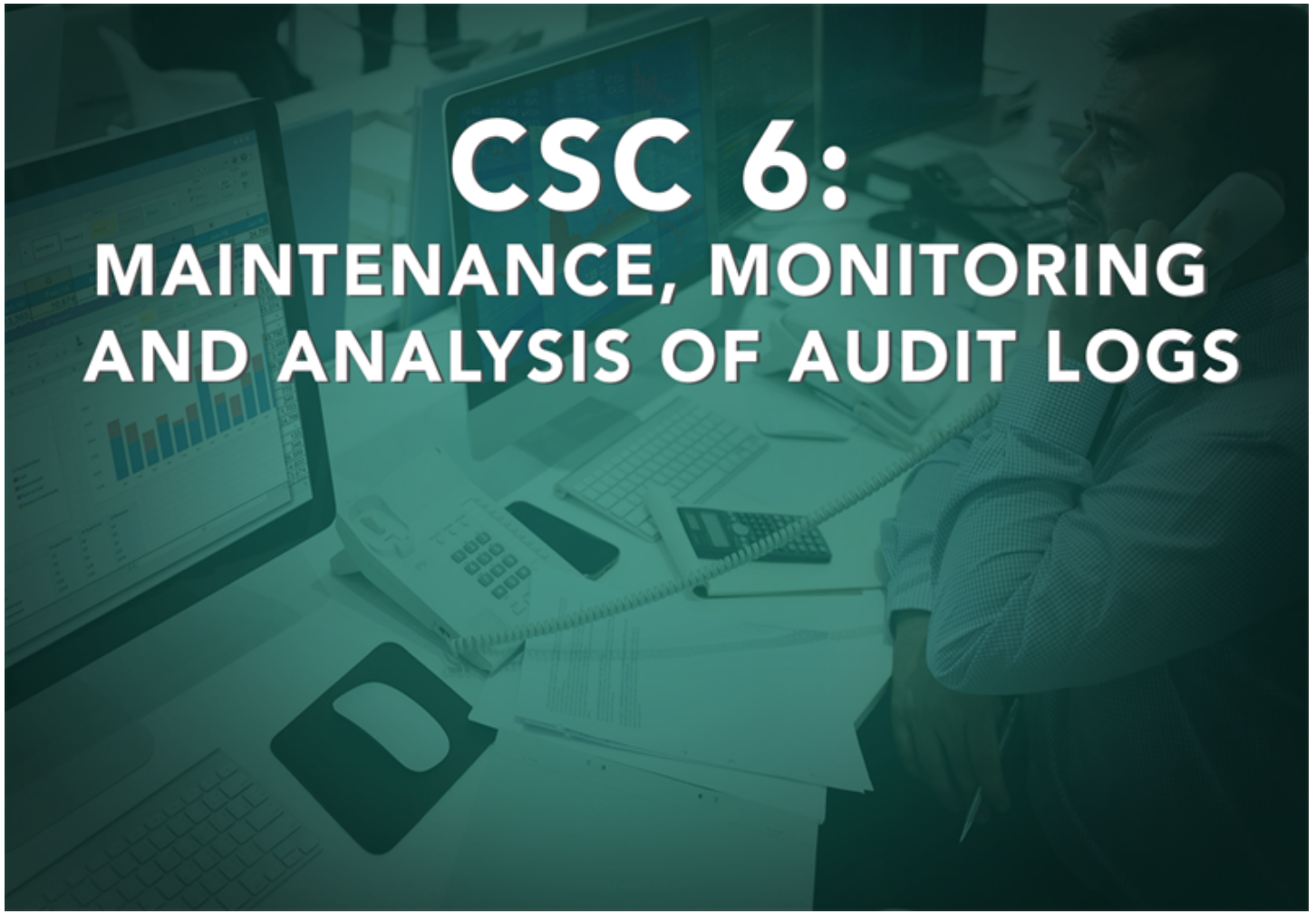


- Critical Control 4: Continuous Vulnerability Assessment and Remediation



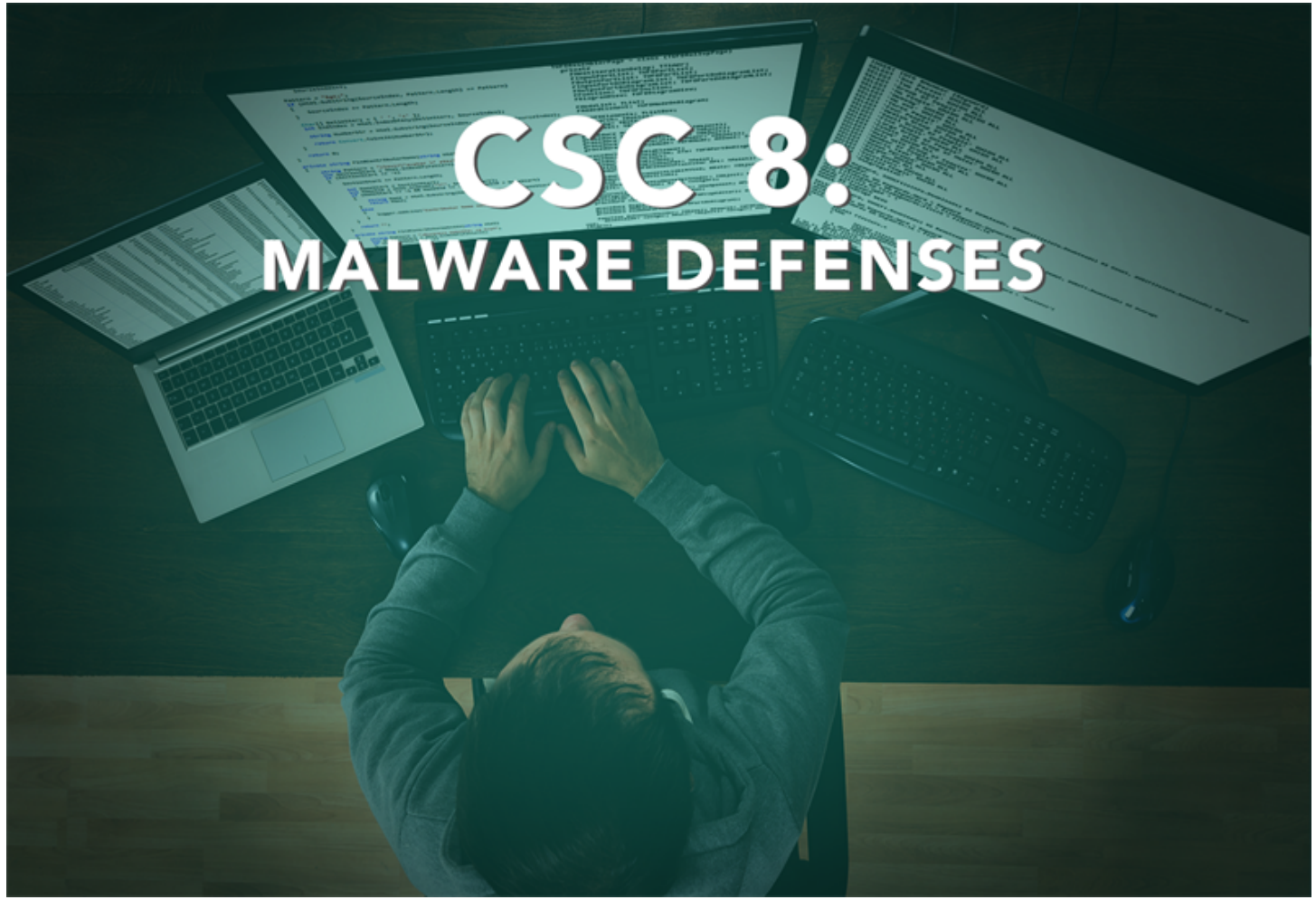
- Critical Control 5: Controlled Use of Administrative Privileges

- Critical Control 6: Maintenance, Monitoring, and Analysis of Audit Logs



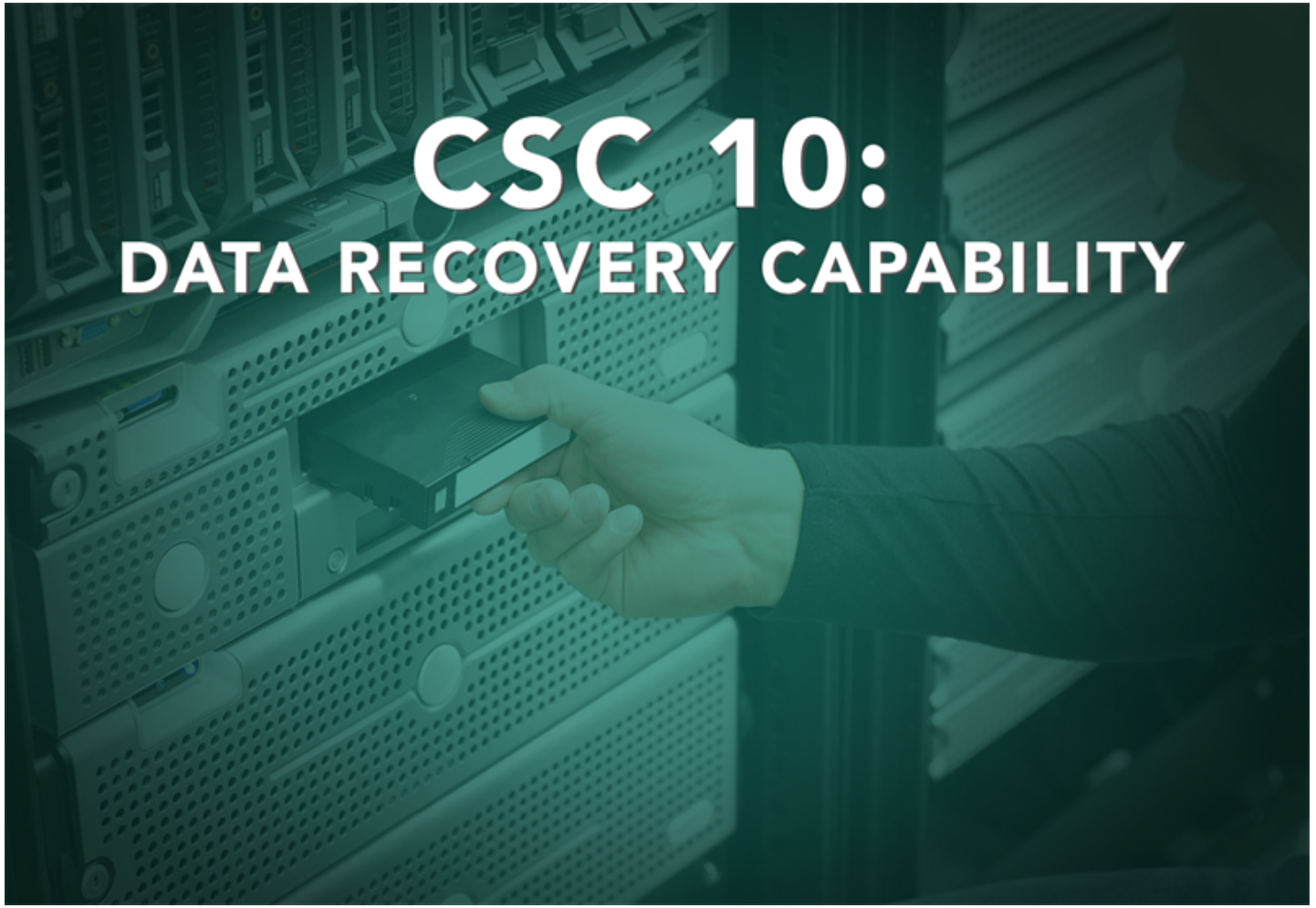
- Critical Control 7: Email and Web Browser Protections

- Critical Control 8: Malware Defenses

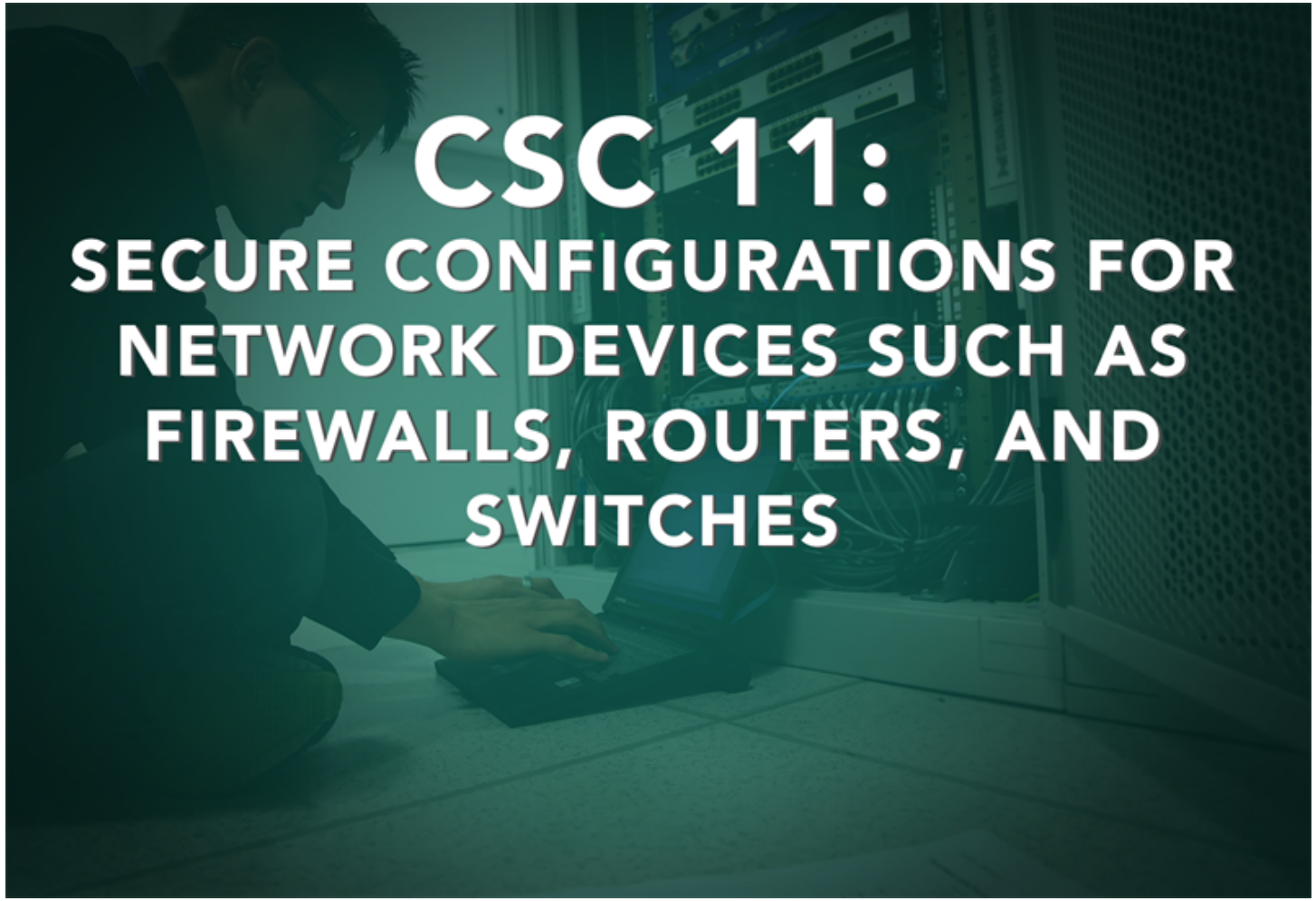


- Critical Control 9: Limitation and Control of Network Ports, Protocols, and Services

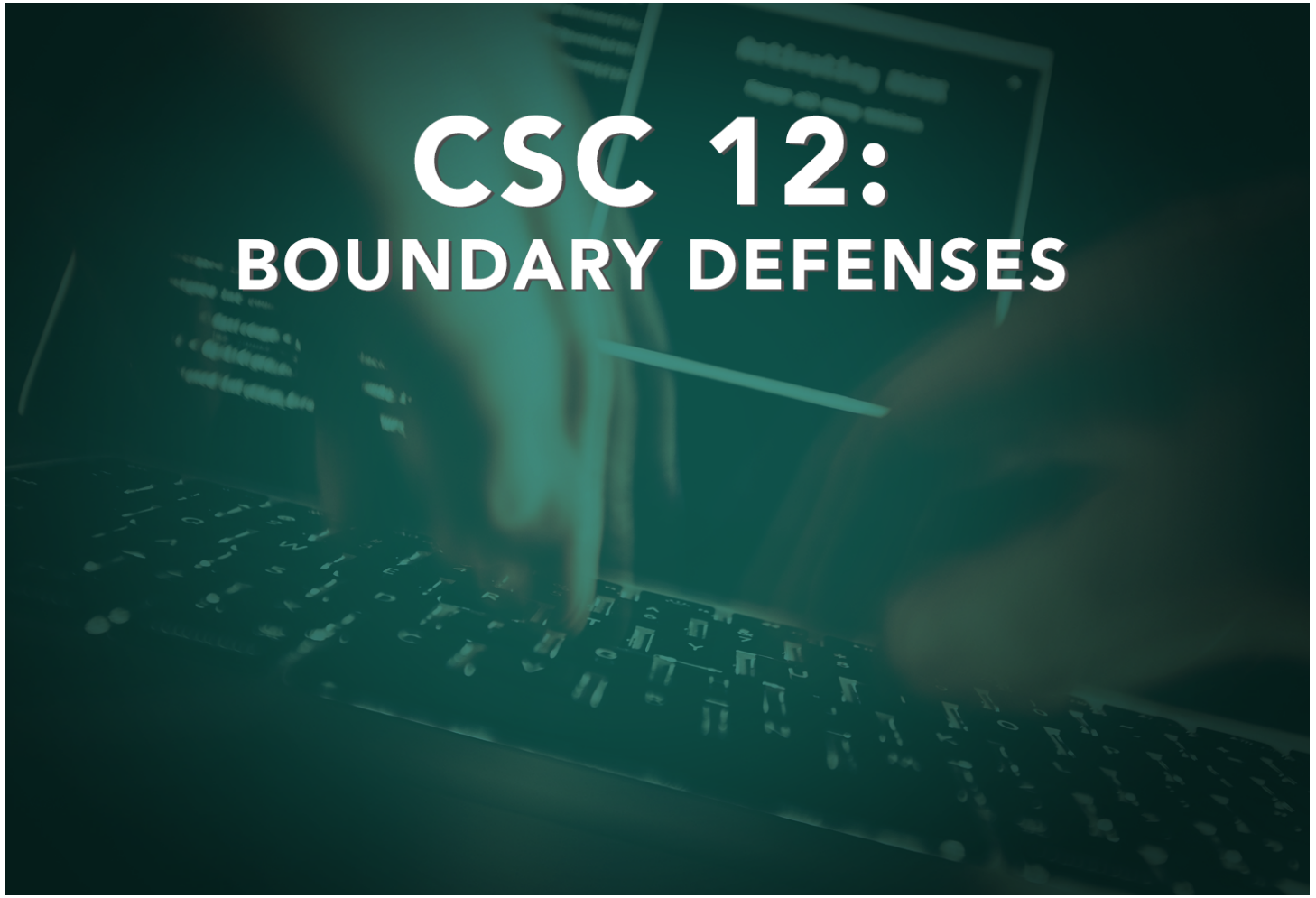
- Critical Control 10: Data Recovery Capability



- Critical Control 11: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches

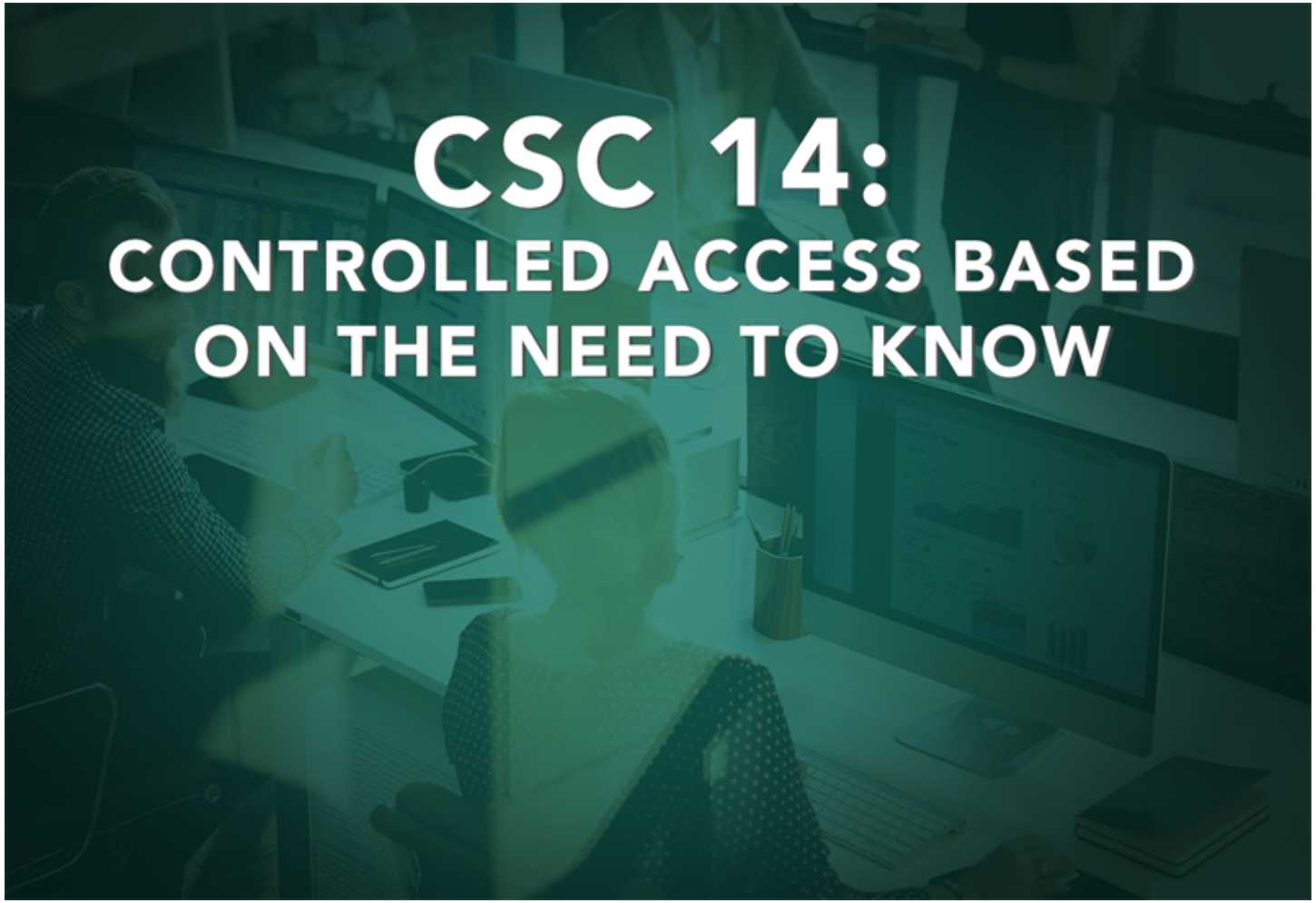


- Critical Control 12: Boundary Defense



- Critical Control 13: Data Protection

- Critical Control 14: Controlled Access Based On Need to Know



- Critical Control 15: Wireless Device Control

- Critical Control 16: Account Monitoring and Control

- Critical Control 17: Security Skills Assessment and Appropriate Training to Fill Gaps

- Critical Control 18: Application Software Security

- Critical Control 19: Incident Response and Management

- Critical Control 20: Penetration Tests and Red Team Exercises