Digital Edge

Architect, Implement, Maintain
CYBER SECURITY SYSTEMS

About DIGITAL EDGE

Established in 1996 as a Datacenter Management and Consulting Service, Digital Edge went through multiple client certifications including SSAE 16 SOC2, ISO, PCI, and HIPPA certifications. Our team provides a SOC team – Security Operation Center – for many organizations. We conducted hundreds of cyber security assessments and penetration tests. Digital Edge has participated in numerous Security Incident Investigations and a contributor to Verizon's Data Breach Investigations Report.

Today, based on the deep understanding of multiple cyber security frameworks, Digital Edge provides its clients with world class methodology and consulting services for implementing, certifying and supporting Information Security Management Systems.

Our mission is to provide clients with a structured understanding of security frameworks, required policies and procedures, as well as modern technology coupled with best practices to protect organizations against failures, breaches, and cyber attacks.

SERVICES

Penetration Testing

External Scan
Internal Scan
Social Media Reconnaissance
Automatic and Manual
Penetration Test
Ethical Hacking
Reporting

Security Assessment

Penetration Testing
Laws and Regulation Analysis
Compliance Deficiencies Analysis
Architecture Review
Risk Analysis and Reporting
Business Continuity Analysis
Policy Analysis
Reporting

Building, Certifying and Supporting Information Security System

Security Assessment
Framework Selection (ISO, SOC2, NIST, etc.)
Development of Policies and Procedures
Staff Training
Technology Review & Integration
Surveillance
Security Operations

Laws and Regulation Analysis
Gap Analysis
Risk Management
Controls Applicability and Artifacts
Security Information & Event Management
Audit, Certification
Security Incident Response

Digital Edge

OUR PERSPECTIVE

1. Security is not a technology – Security is a behavior.

2. Adapt a security framework.

3. Any modern framework will include all regulatory requirements and controls.

4. Adopt a certifiable framework.

5. Certification is proof the framework is implemented properly.

Digital Edge

PROS

1. It is widely adopted standard versus an opinion.

2. All frameworks overlap and are acknowledged by each other.

3. It is adaptive to your needs through statement of applicability.

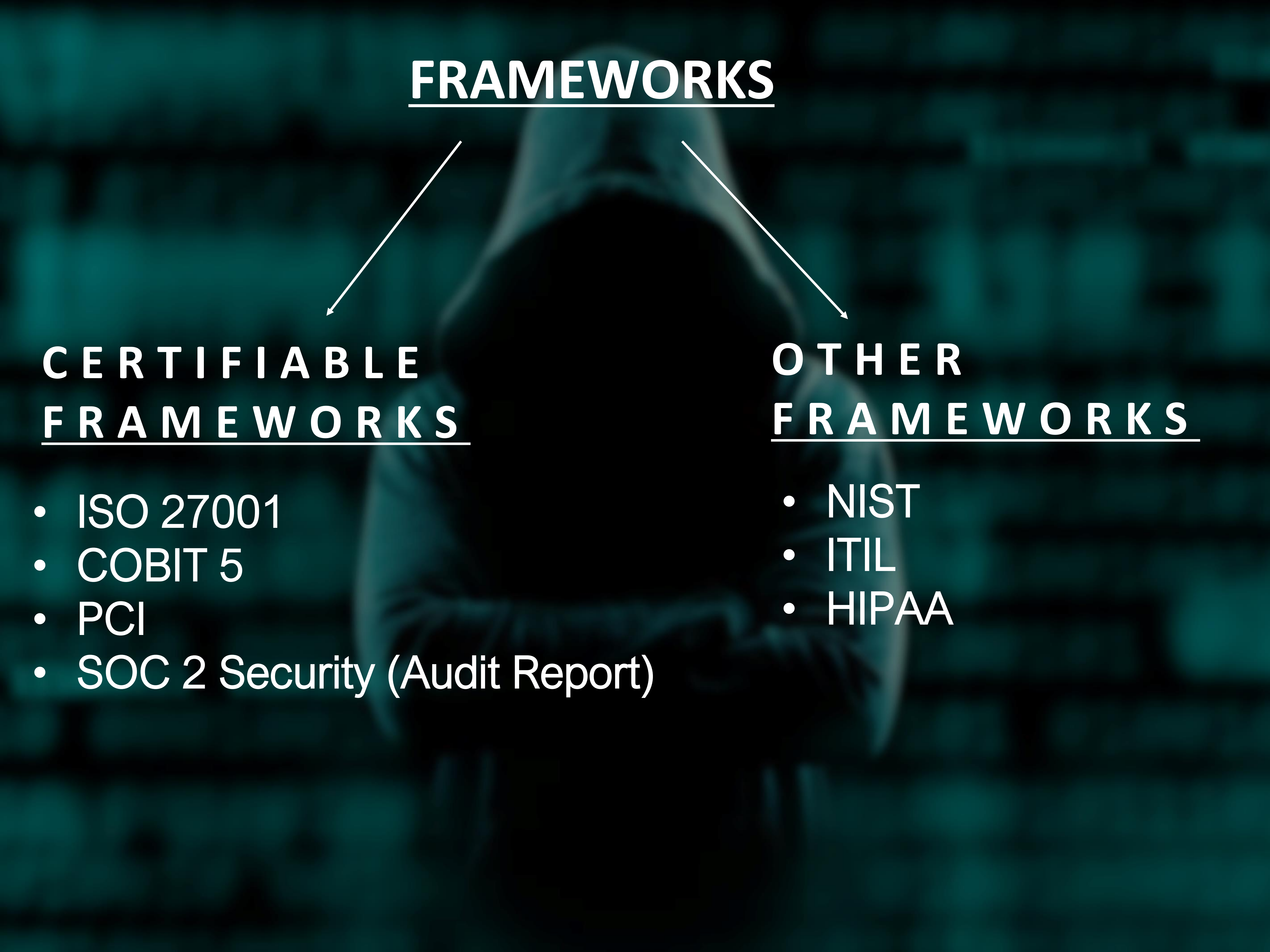
4. Control over IT Security technology, risks and spending.

5. It is a great business branding and marketing tool.

6. Potential lowered insurance costs can offset cost of adoption.

Digital Edge

FRAMEWORKS



CERTIFIABLE FRAMEWORKS

- ISO 27001
- COBIT 5
- PCI
- SOC 2 Security (Audit Report)

OTHER FRAMEWORKS

- NIST
- ITIL
- HIPAA

EXAMPLE - ISO FRAMEWORK

ISO 27001:

- 14 Information Security Domains (categories)
- 114 Security Controls
- Certifiable by a third party accredited body
- International

ISO 27001 14 Security Domains	
IS POLICIES	HUMAN RESOURCE SECURITY
ASSET MANAGEMENT	CRYPTOGRAPHY
ACCESS CONTROL	COMMUNICATIONS SECURITY
OPERATIONS SECURITY	SUPPLIER RELATIONSHIPS
SYSTEM DEVELOPMENT	IS ASPECTS OF BCM
IS INCIDENT MANAGEMENT COMPLIANCE	PHYSICAL & ENVIRONMENTAL SECURITY
ORGANIZATION OF INFORMATION SECURITY	SECURITY COMPLIANCE

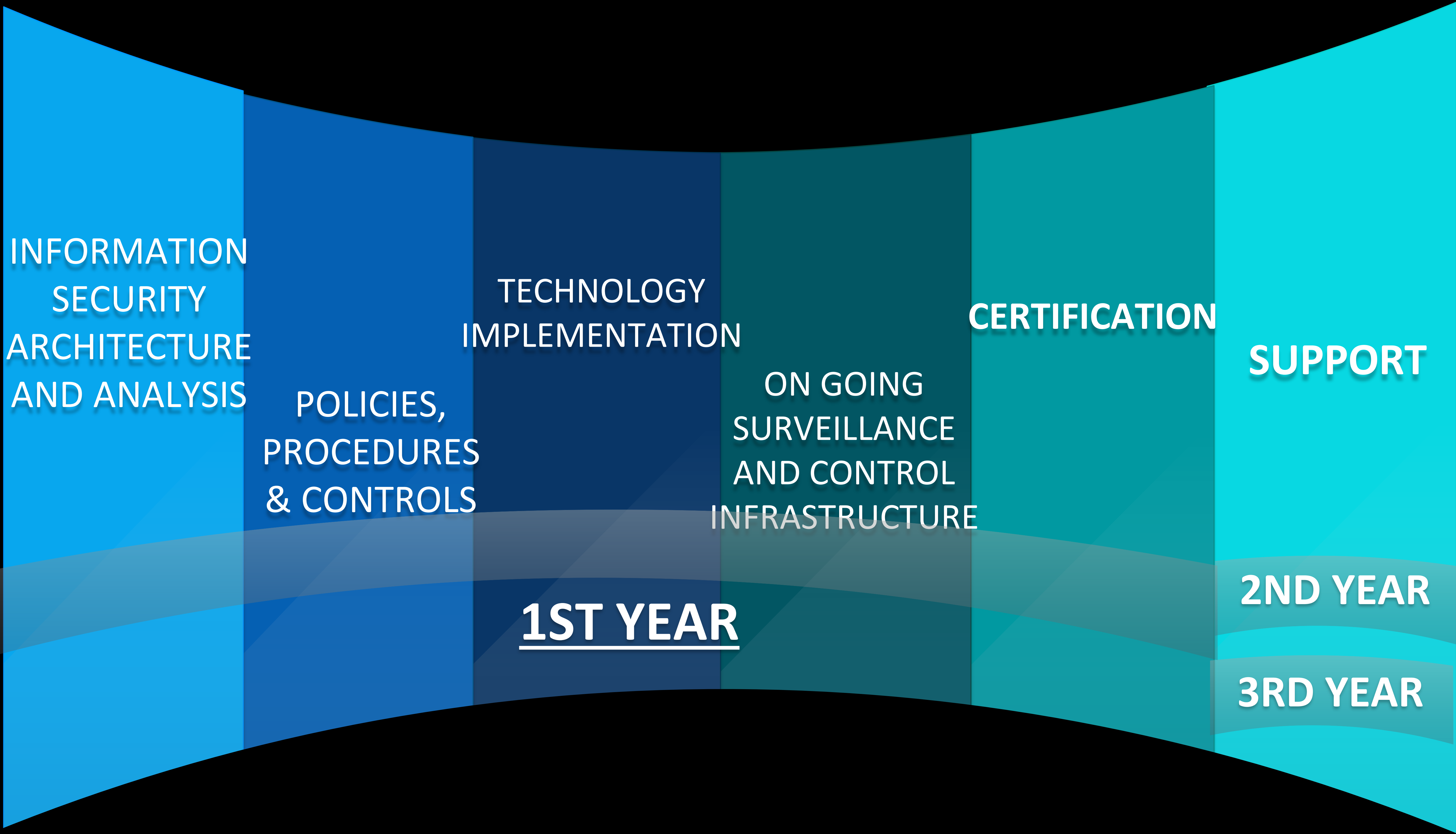
EXAMPLE - NIST FRAMEWORK

NIST Cybersecurity Framework Core

- 22 Information Security Domains (categories)
- 98 Security Controls
- Not Certifiable
- North America

NIST CSF 22 Security Domains	
BUSINESS ENVIRONMENT	ANOMALITIES AND EVENTS
GOVERNANCE	SECURITY CONTINUES MONITORING
ASSET MANAGEMENT	DETECTION PROCESS
RISK ASSESSMENT	RESPONSE PLANNING
RISK MANAGEMENT STRATEGY	COMMUNICATIONS
ACCESS CONTROL	ANALYSIS
AWARNESS AND TRAINING	MITIGATION
DATA SECURITY	IMPROVMENTS
INFORMATION PROTECTION	RECOVERY PLANNING
MAINTANANCE	RECOVERY IMPROVEMENTS
PROTECTIVE TECHNOLOGY	RECOVERY COMMUNICATION

FULL OFFER



INFORMATION SECURITY ARCHITECTURE AND ANALYSIS

POLICIES, PROCEDURES & CONTROLS

TECHNOLOGY IMPLEMENTATION

ON GOING SURVEILLANCE AND CONTROL INFRASTRUCTURE

CERTIFICATION

SUPPORT

1ST YEAR

2ND YEAR

3RD YEAR

STEP 1 - ASSESSMENT

SECURITY

EXTERNAL SCAN

INTERNAL SCAN

SOCIAL MEDIA RECONNAISSANCE

ETHICAL HACKING

CONTROL ANALYSIS

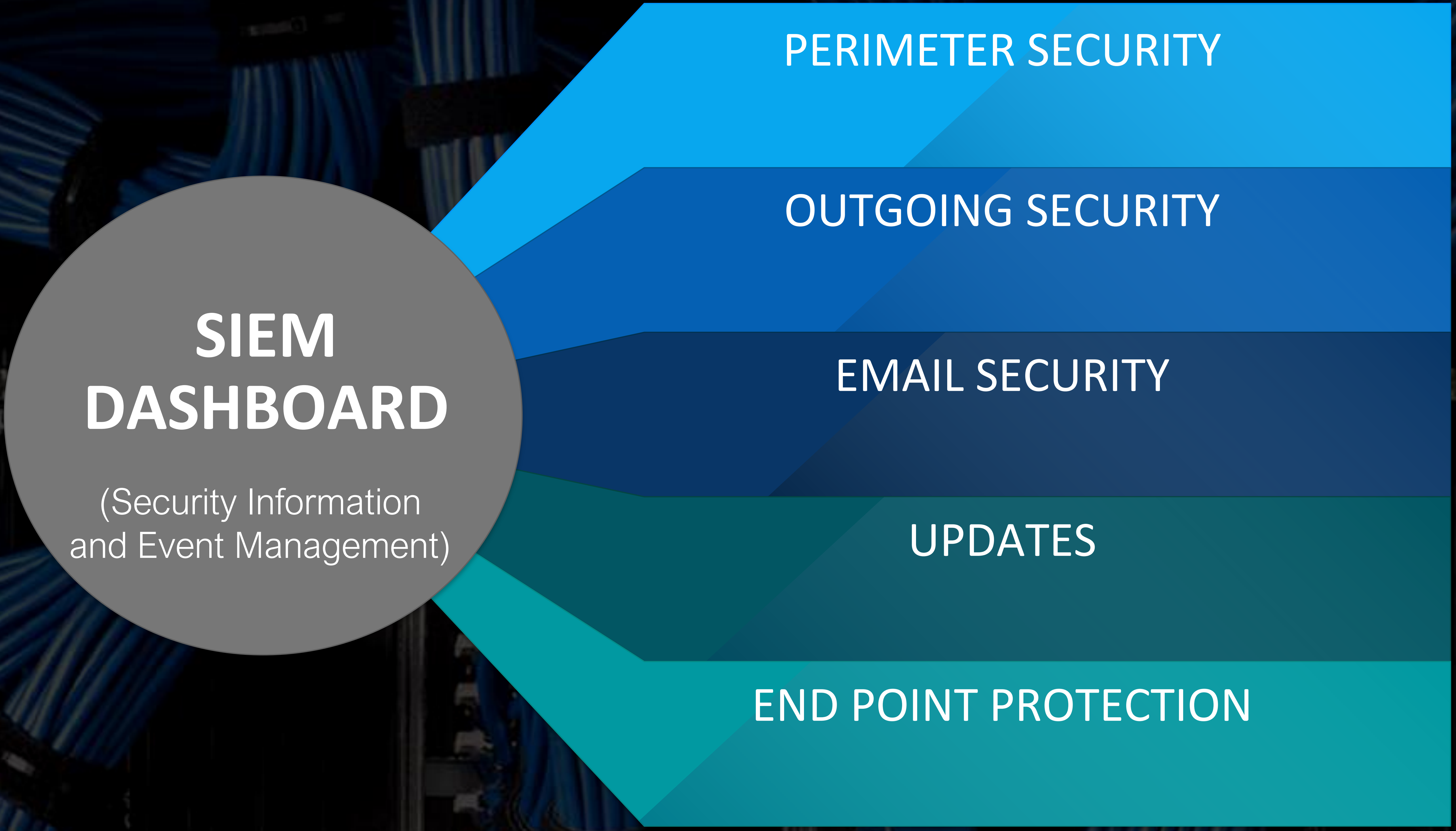
Digital Edge

STEP 2 - POLICIES, PROCEDURES AND CONTROLS

SSAE 16
CERTIFIED
TYPE II

ISO 27001

STEP 3 - TECHNOLOGY IMPLEMENTATION



SIEM DASHBOARD

(Security Information and Event Management)

PERIMETER SECURITY

OUTGOING SECURITY

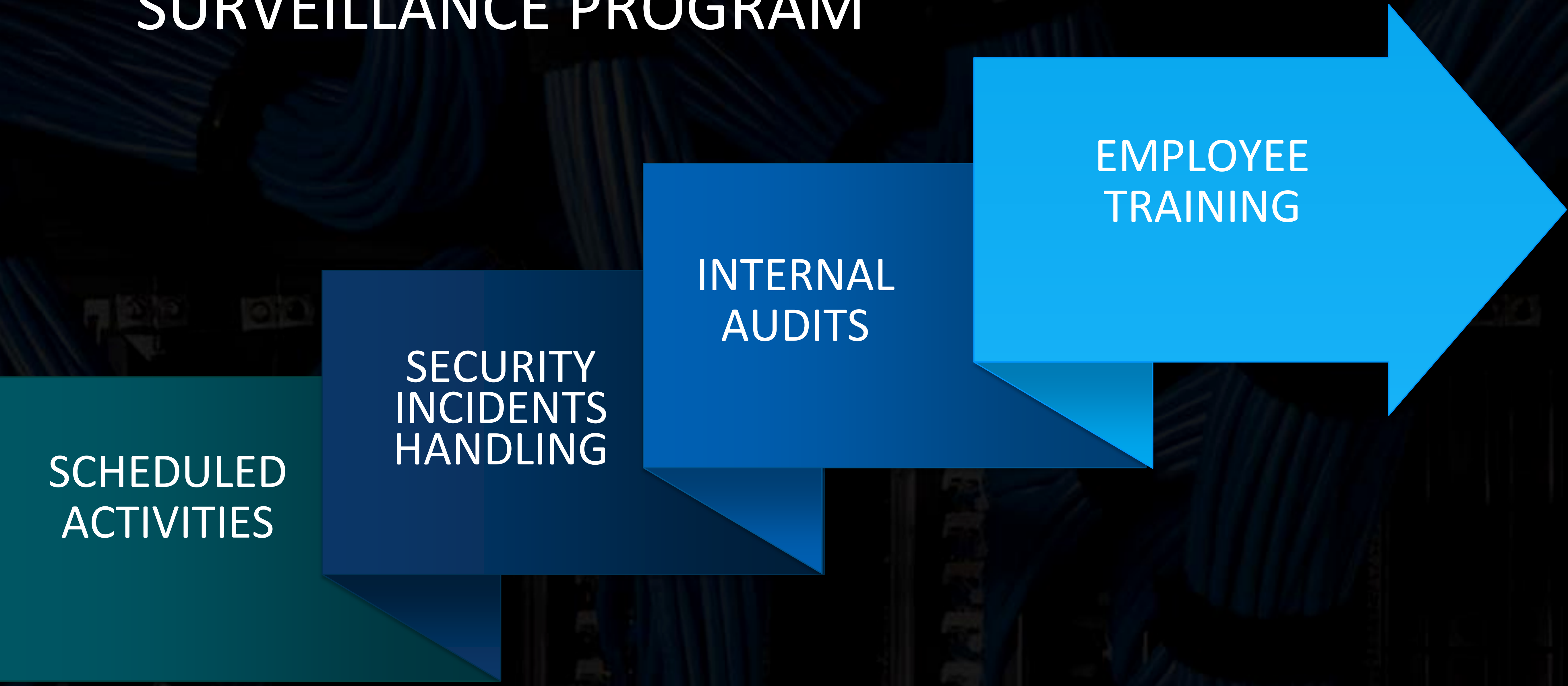
EMAIL SECURITY

UPDATES

END POINT PROTECTION

STEP 4 - SURVEILLANCE

SURVEILLANCE PROGRAM



SCHEDULED ACTIVITIES

SECURITY INCIDENTS HANDLING

INTERNAL AUDITS

EMPLOYEE TRAINING

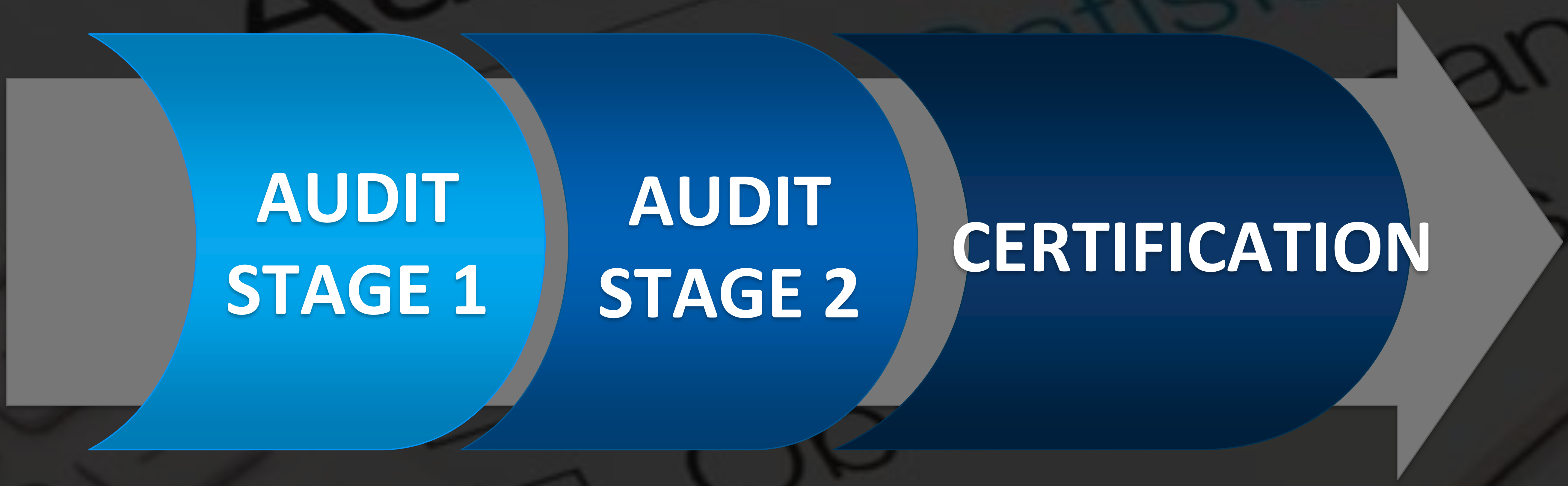
Digital Edge

STEP 4 - SURVEILLANCE

ACTIVITIES	FREQUENCY	RESPONSIBLE PARTY
ISO SURVEILLANCE	YEARLY	ISO ORGANIZATION
INTERNAL AUDIT	YEARLY	CYBERHOST + CLIENT
MANAGEMENT REVIEW	YEARLY	CYBERHOST + CXOS
SECURITY SCANS	3 MONTH	CYBERHOST
USER ACCESS AUDIT	3 MONTH	CYBERHOST
CONFIGURATION CHANGE REVIEW	3 MONTH	CYBERHOST
BUSINESS CONTINUITY TEST	3 MONTH	CYBERHOST
SECURITY AWARENESS TRAINING	YEARLY	CYBERHOST + CLIENT

Digital Edge

STEP 5 - CERTIFICATION



AUDIT STAGE 1

AUDIT STAGE 2

CERTIFICATION

Digital Edge

Digital Edge

For further questions and inquiries, please contact sales@digitaledge.net