SANS

CYBERSECURITY LEADERSHIP

CISO Scorecard

Version 1.1

AND

Cloud Security Maturity Model

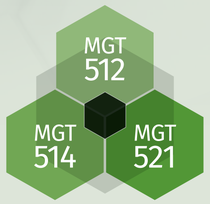
Coming Soon!

For Cyber Leaders of Today and Tomorrow

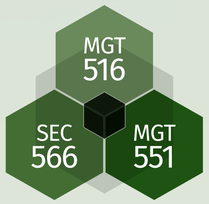
sans.org/cybersecurity-leadership

SANS CYBERSECURITY LEADERSHIP CURRICULUM

FORMULA FOR
TRANSFORMATIONAL CYBERSECURITY LEADERS



FORMULA FOR
OPERATIONAL CYBERSECURITY EXECUTIVES



MGT 512 5 DAYS — **Security Leadership Essentials for Managers** | GSLC
Leading security initiatives to manage information risk

MGT 516 5 DAYS — **Managing Security Vulnerabilities: Enterprise and Cloud**
Building and leading a vulnerability management program

MGT 514 5 DAYS — **Security Strategic Planning, Policy, and Leadership** | GSTRT
Aligning security initiatives with strategy

SEC 566 5 DAYS — **Implementing and Auditing CIS Critical Controls** | GCCC
Building and auditing Critical Security Controls

MGT 521 5 DAYS — **Leading Cybersecurity Change: Building a Security-Based Culture**
Leading & aligning security initiatives with culture

MGT 551 5 DAYS — **Building and Leading Security Operations Centers**
Building and leading Security Operations Centers

sans.org/cybersecurity-leadership

@secleadership

SANS Security Leadership

MGTPS_CISO-SC_v1.1_0921

CISO SCORECARD

SECURITY LEADERSHIP

DO YOU KNOW HOW TO:

TECHNOLOGY

Manage information risk by implementing security capabilities
- Security Program Structure
- Control Frameworks (NIST 800-53, CIS Controls, CMMC)
- Program Frameworks (NIST CSF, ISO 27001)
- Risk Frameworks (NIST 800-39, 800-37, 800-30)
- Threat Frameworks (Kill Chain, MITRE ATT&CK)

Lead modern security initiatives and technologies
- Security Architecture
- Zero Trust Model
- Cloud Security Maturity Model
- Vulnerability Management Maturity Model
- Security Awareness Maturity Model
- Negotiation Strategies

Structure your security program and team
- Roles and Responsibilities
- Guiding Principles
- How to Prioritize Work
- Security Reporting Relationships
- Three Lines of Defense Model
- RACI Matrix

Build business enabling security capabilities
- Product Security
- Cloud Security
- DevSecOps
- Mobile Security
- Emerging Technologies
- Security Due Diligence

MGT 512 5 DAYS

STRATEGY

Develop a security strategic plan and roadmap
- Security Roadmap
- PEST Analysis
- SWOT Analysis
- Gap Analysis
- Maturity Models

Get buy-in from all levels of the organization
- Mission and Vision Statements
- Stakeholder Management
- Power/Interest Grid

Craft effective presentations for senior leadership
- WIIFM approach
- Elevator pitch
- Maturity Models
- KPIs and metrics

Create security policy and procedure
- Policy Pyramid
- Policy voicing
- SMART approach

Align with business objectives
- Security Business Case
- Multi-Year Budget
- SNAP approach for marketing

Respond to legal and regulatory risks
- Conduct critical legal analysis
- Contract drafting styles
- Case studies on policy, privacy, digital evidence, contracts, regulatory investigations, and liability

MGT 514 5 DAYS

CULTURE

Create a sustainable cybersecurity culture
- The Culture Factor
- Values Statement

Drive long-term organizational change
- ADKAR Model
- Kotter's 8 Steps
- Satir Model

Improve effectiveness and impact of security initiatives
- Curse of Knowledge
- ADDIE Model
- Kirkpatrick Evaluation Model
- System 1 vs. System 2
- Choice Overload

Lead, motivate, and inspire teams to execute the plan and improve security
- Circle of Trust
- FILE Feedback Model
- ABCs of Delegation
- Conflict Resolution
- AIDA Model
- Ambassador Programs
- Incentive Framework

Build a mature security awareness program
- Security Awareness Maturity Model
- Maturity Model Indicators Matrix
- BJ Fogg Behavior Model

MGT 521 5 DAYS

SECURITY MANAGEMENT

DO YOU KNOW HOW TO:

VULNERABILITY MANAGEMENT

Build a vulnerability management program
- Asset Management
- Vulnerability Management Governance Model
- Vulnerability scanning architecture and design

Analyze and prioritize vulnerabilities
- CVSS severity scores and ratings
- Leverage asset context
- Root cause analysis
- STIX, TAXII, STAXX

Report and communicate vulnerability data
- Metrics Hierarchy
- Define reporting frequency

Treat and remediate vulnerabilities to manage risk
- PIACT Process
- Automated patch management
- Hardening and configuration guidance and templates

Build relationships and processes to make vulnerability management fun
- Relationship Map
- Define incentives, set goals, hold challenges, reward effort

MGT 516 5 DAYS

SECURITY CONTROLS

Implement and automate critical security controls
- Minimum Controls Baselines and Sensors
- PowerShell commands and scripting
- Windows Management Instrumentation (WMI)
- iPost reporting and data feeds
- Security Content Automation Protocol (SCAP)

Measure effectiveness of security controls
- Measures and metrics for the CIS Controls
- CIS-CAT to audit configurations
- Root cause analysis
- Vulnerability scanning
- Red Team exercises & penetration testing

Manage projects, programs, and initiatives to successful completion
- Project Management Hierarchy
- Project Management Information System (PMIS)
- Project Priority Triangle
- Work Breakdown Structure
- Deming's Plan-Do-Check-Act (PDCA) Cycle
- RACI Matrix
- Thomas-Kilmann Conflict Model
- Risk Breakdown Structure (RBS)
- Decision Tree Analysis

Build dashboards for security and compliance
- Using spreadsheets as data sources and as visualization tools
- Configuring Graphite and loading data
- Adding Grafana data sources and building dashboard
- Building tactical reports directly from acquired data using pivot tables and graphs

Plan and execute effective audits
- Scoping to cover highest risk areas
- Effective audit reports
- Approved baseline configurations
- Scripting audit tasks

SEC 566 5 DAYS

SECURITY OPERATIONS

Build a Security Operations Center (SOC)
- SOC Functional Model
- Collect, Detect, Triage, Investigate, Respond

Lead incident response planning and execution
- RE&CT Framework
- Hardening, Telemetry, Process, and Practice
- Plan activities

Develop analysis techniques, playbooks, and detection use cases
- MITRE ATT&CK for use cases
- Sigma and YARA for detections
- Jupyter for data analysis and threat hunting

Create metrics and strategies for SOC improvement
- Metrics vs. KPIs. vs. OKRs

Implement training and retention strategies to prevent burnout
- SOC Human Capital Model

MGT 551 5 DAYS