SANS

CYBERSECURITY LEADERSHIP

CISO Scorecard

Version 1.5

AND

Cloud Security Maturity Model

For Cyber Leaders of Today and Tomorrow

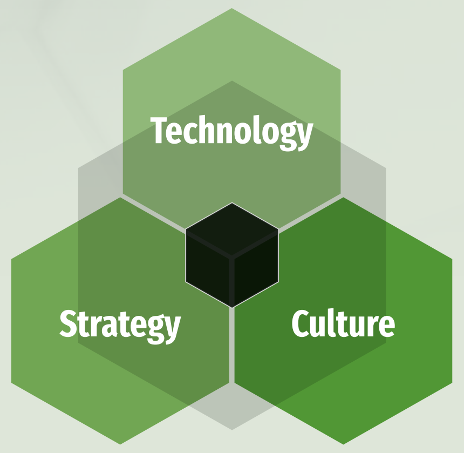
sans.org/cybersecurity-leadership

LDR_CISO-CSMM_v1.5_1-24

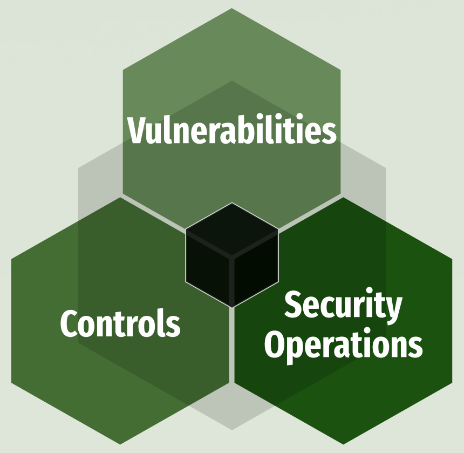
SANS

CYBERSECURITY LEADERSHIP CURRICULUM

FORMULA FOR
TRANSFORMATIONAL CYBERSECURITY LEADERS



FORMULA FOR
OPERATIONAL CYBERSECURITY EXECUTIVES



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

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

LDR 521 5 DAYS — **Security Culture for Leaders**
Build and measure a strong security culture.

LDR 516 5 DAYS — **Building and Leading Vulnerability Management Programs**
Stop treating symptoms. Cure the disease.

SEC 566 5 DAYS — **Implementing and Auditing CIS Controls** | GCCC
Prioritizing defenses to stop attacks with the appropriate cyber controls.

LDR 551 5 DAYS — **Building and Leading Security Operations Centers** | GSOM
Prevent – Detect – Respond | People – Process – Technology

Learn more at **sans.org/cybersecurity-leadership/triads**

sans.org/cybersecurity-leadership
@secleadership
SANS Security Leadership
sansurl.com/leadership-discord
sansurl.com/leadership-youtube

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

LDR 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

LDR 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

LDR 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

LDR 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

LDR 551 5 DAYS

SANS CLOUD SECURITY MATURITY MODEL

Data Protection

Data Encryption

Initial
- Enterprise encryption policy is aligned with necessary regulatory and compliance requirements
- The level of trust required has been determined with regards to key management (eg., compliance)
- Usage of the default CSP-managed key for encryption usage

Managed
- Encryption settings for each adopted service are configured
- Cloud to on-premise communication is routed over a secure and encrypted channel
- Key management service is used to manage keys
- Disaster recovery requirements for keys have been established

Defined
- Encryption-related configurations are implemented by IaC
- Key management service and customer-managed keys are leveraged for cloud-based encryption
- A workflow is established for key rotation
- Validated roles allowed to manage keys are based on least privilege principle

Quantatively Managed
- Where required by regulatory or industry requirements, HSM-based key management service is leveraged to safeguard keys
- Validated encryption requirements are implemented across in-transit and stored data across all cloud services

Optimizing
- Periodic validation is in place for all keys in the cloud environment are managed by a key management service
- Exercises on the recovery actions in a disaster affecting keys are performed

Data Classification and Protection

Initial
- Manual and limited automated inventory exists in locations where sensitive data is stored and SaaS services are used in alignment with policy

Managed
- Discovery technologies deployed to locate sensitive data
- Remediation is executed manually as needed
- Discovered sensitive data are manually validated and with protective configurations (encryption, deidentification) applied

Defined
- Coverage of scanned locations is expanded to the discovery of other SaaS services utilized (ie., CASB)

Quantatively Managed
- Digital-rights management is implemented, on top of automatic data protection by encryption and de-identification

Optimizing
- API integrations is used for scanning contents to find and respond to sensitive data patterns as well as threats like cloud malware

Data Backup and Resiliency

Initial
- Business continuity and disaster recovery requirements have been identified and documented

Managed
- Cloud environment is configured on a best-effort basis to match availability requirements
- Configuration guardrails for configurations are updated to include backup configurations
- Tags and resource IDs are used to automatically identify resources that store data for business-critical applications for backup considerations

Defined
- Infrastructure as code (IaC) and event-driven architecture are implemented as an essential part of backup strategy
- Data stored is evaluated to ensure compliance with availability requirements

Quantatively Managed
- Protect critical data using immutable backups (eg., AWS Backup Vault Lock)

Optimizing
- Data classification is leveraged to validate data retention and backup objectives are met

IAM

Segregation

Initial
- Mandated use of approved cloud environment/accounts
- Isolated functional area (eg., Dev, Test, Prod) used where possible and different projects for isolation to reduce blast radius

Managed
- Established enterprise resources permission segregation model in alignment with CSP's best practices
- Level of separation necessary separation has been determined (eg., multi-account, multi-subscription)
- The segregation model should have taken enterprise security variations into account (eg., department or subsidary differences)

Defined
- Updated the enterprise IaC templates with the segregation model

Quantatively Managed
- Segregation model aligned to multicloud environment
- Logical seperation maintained consistently across CSPs but the technical implementation can be different
- Leveraged automation to periodically identify the discrepency to the segregation model

Optimizing
- Configuration management solutions are being used to prevent segregation and misaligned resource/objects from being created

Identity Management

Initial
- Accounts are possibly created manually on an as-needed basis
- Adopted the use of MFA or passwordless authentication at minimum for all privileged users

Managed
- Consolidated enterprise identities into a single system allowing single sign-on, either federate on-premise system or cloud-based identity-management system
- Usage of the single-authentication system spans to all cloud-based data and control panes
- Usage of user templates for consistent provisioning and deprovisioning of accounts and implement account security policies

Defined
- Centralized access request, provision, and deprovisioning workflow is automated with proper approval and visibility built in
- Third-party and client-identity stategy have been established for access to the cloud environment and whether integration of identity directory is necessary

Quantatively Managed
- User-management practice aligned to multicloud environment
- Single directory system served across all leveraged cloud environments
- Customers' identities are consolidated on one directory and may be consolidated to the enterprise system with proper segregation
- Scope of MFA/passwordless usage expanded to more general users

Optimizing
- Usage of weak authentication eleminated in the environment

Access Management

Initial
- Roles established in the organization that have access requirements and mapped out access in relation to cloud environment
- Required access permission applied for each role type to the best extent
- Default permission configuration provided by the CSP leveraged
- Leadership and organizational buy-ins secured to transform the traditional rigor in network perimeter management to management of access controls

Managed
- Performed risk-reduction actions on priviledged identity
- Elimination of unecessary privileged access/accounts
- Dedicated administrative accounts that are not used for other purposes
- Role management is based on automated workflow and with proper approval and visibility built in
- Validated enterprise security teams have visibility to review and evaluate access permission for monitoring and incident response

Defined
- Just-in-time- or temporary-access management used for privileged access for as-needed privilege usage
- Adopted cloud services are individually reviewed and validated
- Permission is granted based on least-privilege principle—refining the perimission from the CSP's default role
- Expanded the dimensions of access control policies to incorporate telemetry data of endpoint, network, data, and application
- Enablement for zero-trust model

Quantatively Managed
- Administrative-account access is limited to certain isolated endpoint assets that are dedicated for such use
- Consistent approaches and workflow to multicloud environment

Optimizing
- Usage of attack simulations leveraged to identify the full extent of a breach situation and drive-access reduction

Security Governance

Cost Management

Initial
- Cost are attributed ad hoc to business process
- Best effort cost management on cloud resources

Managed
- Cost management principles generally agreed by all lines of business
- Clear financial alignment between resources and ownership using resource tagging to help with cost attribution

Defined
- Cost management policy established
- Cost planning effort in place
- Initial budget deviation reporting centralized

Quantatively Managed
- Education of cost management in place
- Subscription strategy alligned to utilization and purchasing model
- Reporting and alerting in place on deviation and underutilization for each line of business
- Remediation driven based on reporting

Optimizing
- Business goals alligned with planned budget
- Architecture patterns adjusted to align with subscription model
- Budget actively managed and forecasted to allign with business goals

Cloud Governance Committee

Initial
- An alliance of responsible executives is formed from multiple departments to delegate the cloud-related decisions
- Alliance meets on regular basis
- Identification of cross-functional stakeholders has started

Managed
- Stakeholders and sponsors from cross-functional areas have been identified
- Meetings are held on a regular basis with all stakeholders
- Charter of the committee is formulated

Defined
- Area of interest and focus for each team related to cloud governance is identified
- Sponsors have identified the delegate to support the continous operations
- Operating rthythm of the commitee is identified
- Key metrics to evaluate performance established

Quantatively Managed
- Decision authority, execution, and process to transition to enforcement of the committee has been formalized
- Continuous process in place to maintain a risk register and a pipeline of topics for committee to work on

Optimizing
- Continuous assessment of committee membership span in the organization
- Performance indicators are evaluated and feedback from leadership is accepted to adjust focus of committee

Security Policy

Initial
- Security policy in place to address security needs of the organization but may not directly address the cloud environment

Managed
- Key objectives of the controls for cloud have been defined and mapped to the detailed technical guardrails which implement the controls
- Communication plan drafted with emphasis on incremental nature of the cloud security policy
- Business appetite for risk identified for policy drafting

Defined
- Cloud security policy communicated to cloud-related personnel and third-party providers
- Recurring policy review process established
- Industry best practices aligned to the adopted policy
- Policy enforced via automated means through guardrails in the environment

Quantatively Managed
- Enforcement methods and processes refined based on feedback and metrics
- Established exception management process in place

Optimizing
- Continuous adjustment of policy in alignment to industry best practice changes, compliance, and also service adoption changes in cloud environment

Security Assurance

Posture Validation

Initial
- Relevant decision makers, risk owners, and executives accountable for business processess or objectives that are cloud dependent have been identified
- Baseline security posture report from the service providers has been reviewed

Managed
- Organizational use cases of the cloud have been analyzed and the current cloud security posture has been established
- The appropiate benchmark standards for measuring the organization's cloud security posture has been identified
- Top findings have been remediated based on the baseline security posture report from the service providers

Defined
- Controls are cross-mapped and benchmarked against different frameworks based on requirements
- Internal stakeholders for each area of posture issues are identified and a consensus reached to remediate issues in a given timeline

Quantatively Managed
- Automation is in place to measure CSP-related control for design and operational effectiveness and reported the results back to the key stakeholders
- Key metrics are published on the overall performance of the posture validation effort

Optimizing
- Tools such as GRC or CASB are adopted to streamline and automate the workstreams of day-to-day tasks

Regulatory Compliance

Initial
- Information gathered on the workload to be put in the cloud—type of data records involved, nature of the workload, and geographical locations of the cloud service are probably the most crucial information to collect
- The relevant regulatory has been identified and requirements with regards to using cloud-service providers for hosting workload
- Leverage CSP-provided regulatory compliance information for evaluation

Managed
- Based on the cloud services leveraged, assess the compliance of the cloud based workload end to end, including all involved service providers—taking into consideration the shared responsibility model

Defined
- Performed self assessment or audit with documentation on the compliance requirements for validation of compliance
- Recurring review of legal compliance requirements based on the cloud setup changes, possibly due to new service adoption or new workload architecture

Quantatively Managed
- Automation of the process for the compliance requirements that require recurring monitoring in the cloud environment is in place
- Reports generated are regularly reviewed to validate compliance

Optimizing
- Compliance-validation process has been largely rolled into the automated-assurance processes with compliance data recorded

Security Testing

Initial
- Vulnerability assessment is performed using traditional remote-scanning ability to detect known vulnerabilities
- Penetration testing exercises are performed with basic threat assumptions such as an external attacker attempting to breach the cloud environment
- Usage of CSP's security-validation services to generate report of commonly known misconfiguration and vulnerabilities

Managed
- Cloud-native or third-party assessment tools are leveraged to focus on the configuration validation area to detect misconfigurations
- Pentests are conducted on regular intervals
- Consolidated the vulnerability views across on-prem and cloud for holistic view

Defined
- Penetration testing is based on specific compromised scenarios that would reflect real-world attacks—the scenarios could come from threat intelligence or previous incidents in the industry or within the organization
- Findings from the testing process are remediated according to certain internal timelines and both validated for remediation and engineered to avoid future recurrence

Quantatively Managed
- Threat model of the cloud environment and common-access use cases are developed for penetration or purple team scenarios

Optimizing
- Regular attack simulations are conducted to gain better understanding of the blast radius and also validate the effectiveness in control technology and processes

Application and Workload Protection

Security Protection Services

Initial
- Cloud-native security components are leveraged by applications in an ad-hoc manner or follow an on-prem security standard

Managed
- Common cloud-based security protection services are leveraged on an ad-hoc basis to protect the cloud applications, such as cloud DNS, anti-DDoS protection services, content delivery network, API gateways and/or a cloud workload protection platform

Defined
- Enterprise standard for protection profile for each type of applications has been established. The standard contains the baseline configuration for the protection services for adoption

Quantatively Managed
- Enterprise protection profile extended to assist with the fine tuning of protecting profiles—allowing the application to further secure the environment beyond the basic protection
- Guidelines provided for a more complex rule-based system such as WAF

Optimizing
- The effectiveness of the protective set of services and related configuration via threat modeling and red team exercises are validated and fine tuned

Cloud Workload Assessment

Initial
- Pentest or other end-of-development-cycle testing are performed with most critical workloads
- Other forms of testing may be performed on an ad-hoc basis

Managed
- SAST and/or DAST are leveraged during development lifecycle
- Red team exercises are performed on applications

Defined
- Testing performed across the various development steps of the CI/CD pipeline including check-ins, build, release, and deployment phases

Quantatively Managed
- The testing pipeline applies to all applications and related resources running in the cloud environment
- Threat modeling is performed for applications on a best-effort basis and the results are leveraged to fine tune the red team exercises

Optimizing
- Threat modeling for all cloud-based applications is performed—the scope includes application logic as well as the environmental aspects

Cloud Application Practices

Initial
- DevSecOps practices and cloud-development resources/services are used in an ad-hoc manner for managing cloud-based applications
- Development team is involved in the cloud security committee and major change management

Managed
- Department or application projects leverage cloud-native services to manage application secrets, source code and build processes—enterprise preference towards PaaS-based security services
- CI/CD pipeline is secured according to best practices and adopted enterprise-wide
- Updated enterprise-coding standard to reflect in the cloud-native environment

Defined
- Application design and architecutre patterns are established for cloud-native solutions—patterns are aligned with the enterprise's cloud architecture with respect to availability, scalability, and security
- Security functions are embedded within development teams
- Enterprise-established standard pipelines for application replatforming towards cloud-native solutions

Quantatively Managed
- Approved design and architecture patterns are distributed as code for adoption by teams enterprise-wide
- Development teams are confident in automated development and deployment capability, and are able to adopt a high rate of regular changes to support software lifecycles

Optimizing
- Development teams, supported by cloud-native tooling and collaboration, are able to continuously improve applications not only at coding of modules level but able to adopt new cloud capabilities and new architecture within a very short period of time and in quick succession

Detection and Response

Security Intelligence

Initial
- Subscription to intelligence feed is available to organization—can be industry aligned

Managed
- Cloud environment setup is analyzed and generates original detection logic for the cloud environment that is in use
- Industry intelligence feed is refined to attain better detection

Defined
- Recurring generation of new detection logic through the learnings from incidents or threat hunting activities in the environment
- Pivot the detection logic from known bad IP and binary running in the environment to behavior and activities that are suspicious

Quantatively Managed
- Threat modeling and purple team exercises are performed to determine the abuse cases for monitoring
- Continued evaluation of additional threat feeds to be integrated
- Threat intel analysis outputs are integrated with detection and monitoring tools

Optimizing
- Metrics have been integrated into the security intelligence evaluation process

Analysis and Monitoring

Initial
- Cloud-native platform monitoring capability is turned on
- CSP out-of-the-box monitoring capabilities are used

Managed
- Cloud platform logs are collected for analysis
- Integration with self-generated intelligence
- Prioritization of event and log types that have a higher security value for monitoring are in place

Defined
- Events are mostly normalized across different sources to allow effective analysis across resources in the environment
- Cloud platform logs and enterprise platform logs have been consolidated into SIEM
- Network flow/traffic-based logs are collected and analyzed to provide added context

Quantatively Managed
- Alerts are maintained at expected false-positive ratio through detection-logic optimization to avoid alert fatigue

Optimizing
- Logs of multicloud platforms are either consolidated into a single technology or first analyzed in cloud-native environment then the relevant alerts and logs are consolidated together for analysis

Response

Initial
- A start has been made documenting playbooks for common tasks for response
- Cloud-native platform security monitoring technology is utilized for responding to critical detection

Managed
- Containment and eradication workflow in cloud environment is established
- Playbooks have been defined to support these operations

Defined
- Tabletop walkthrough/exercise is used to help refine the incident response playbooks
- The most frequently used playbooks are automated
- The focus is on automating passive response tasks to gain confidence

Quantatively Managed
- Purple team exercises are conducted to validate detection and response capabilities

Optimizing
- Most playbooks are automated
- A recurring process is in place to review playbooks' effectiveness and efficiency
- Metrics KPI are used to refine the playbooks and processes

Log Management

Initial
- Logs may be sent to on-prem log collection for analysis
- Log storage plans have been defined, with considerations for storage costs, ingestion, and transfer

Managed
- Logging standards have been established for cloud-native components and configuration is integrated into automatic resource provisioning
- Cloud platform and core set of high-security value resource logs have been consolidated in cloud

Defined
- Collection and retention of logs have been evaluated and optimized striking a balance between security and efficiency/cost
- Logs are parsed and metric reports are generated
- Logging levels are clearly defined
- Additional logs from the environment are being collected centrally

Quantatively Managed
- Enterprise logs have been consolidated
- Event logging requirements and config are aligned enterprise-wide
- Log sources are monitored for errors and remediation process is in place

Optimizing
- Multicloud log consolidation and configuration normalization is in place

Infrastructure Architecture and Protection

Config Management

Initial
- CSP best security practices are being followed where possible

Managed
- Defined enterprise guardrails in place for adopted cloud services
- Ad-hoc validation of config against guardrail templates

Defined
- Automated config guardrail validation in place to validate resources conformance to configuration standard
- Alerts and notification generated on non-compliance configuration

Quantatively Managed
- Periodic review of config based on lessons learned from incidents
- Automated config validation to prevent bad configuration from being provisioned and remediation of some key violations

Optimizing
- Automated config validation remediates all non-compliance configuration

Image Management

Initial
- Usage of images manually built or from public marketplace repository

Managed
- Enterprise standard has been developed for images taking into consideration of security requirements
- Virtual machine and container images are restricted to approved ones

Defined
- Golden images are centrally managed
- VM and container builds are performed through automated code based on building process with security patches, configuration, and tooling bundled in

Quantatively Managed
- Automated process extended to manage full lifecycle of image including evergreen-running images, across all computing environments (multicloud and on-prem)

Optimizing
- Image management practices extended to multicloud environments

Cloud Secure Architecture

Initial
- Landing Zone's best practices are adopted where possible

Managed
- Benchmarked against the Well-Architected Framework/Architecture Framework
- Roadmap created to adopt the necessary steps

Defined
- Path towards immutable architecture and ZeroTrust architecture has been defined
- Target patterns and roadmap for implementation
- Incorporate defensive architecture decisions based on threat intelligence that have been laid out

Quantatively Managed
- Most components of the Well-Architected Framework/Architecture Framework have been adopted for automation of enforcement and provisioning
- Learnings from security monitoring/response in architecture advancements have been adopted

Optimizing
- Periodic refinement of target with regards to alignment with updates of the Well-Architected Framework/Architecture Framework and patterns updated in alignment with organizational demands

Resource Management

Initial
- Defined tagging scheme and inventory system in place taking cost management in consideration
- Resources maybe managed over ad-hoc and manual methods

Managed
- Automated resource management (using code) to ensure resources are consistently created and managed
- Enforcement of enterprise tagging scheme

Defined
- Mostly automated resource provisioning and management
- Automated mechanism in place to apply the guardrail
- CSP/third-party asset inventory system used to map out assets in cloud

Quantatively Managed
- Resource visibility and management are consolidated in multicloud environment preferably using the same tool across all cloud service providers

Optimizing
- Continous allignment of security guardrail with resource management automation tool

Network Control

Initial
- Geolocation and network segmentation requirements have been determined—possible usage of traditional enterprise network security appliances for initial ease of management

Managed
- Option for reliable and high-performing connectivity with on-prem network has been determined
- IP schemas for VNet and VPC determined
- Defined usage of cloud network components, such as VNet/VPC, Internet gateways, subnets, VPC/Private Endpoints and other ACLs, for the protection of posture

Defined
- IP address management strategy has been determined to avoid resource dangling
- Prioritized usage of native defense components over third-party appliance
- Centralized management of network firewall rules

Quantatively Managed
- SASE is leveraged to enforce trusted access to the cloud environment
- Management of Egress traffic from all cloud resources on top of inbound controls

Optimizing
- Automated usage of catalog multicloud and SaaS services to enforce secure connectivitity for the resource access

Workforce Readiness

Skill Readiness

Initial
- Training effort is focused on "pioneer" group of core users and members who are working directly on and responsible for setting up the cloud environment

Managed
- Job functions have been mapped to skill requirements to align with training
- Developed security-specific training and certification paths for main groups of enterprise users
- Key roles consisting of developers, infrastructure, engineering, security, management, and operational teams

Defined
- On-the-job training has been established, hands-on and/or job-shadow training in addition to classroom and certification programs

Quantatively Managed
- Cloud security training made available to general IT team members to expand talent pool
- Validation conducted with teams via survey on the relevance of training and job functions
- Training scope refined to align with job requirements

Optimizing
- Gamified the certification and training effort to attract a higher level of interest

Organizational Alignment

Initial
- Cloud transformation supported by each member of the team on an as-needed basis
- As security-related requirements come up, the best suited departments, teams, or individuals address the needs. Some departments may be more aligned to cloud-related work than others

Managed
- Mapped and documented the required security functions to support the cloud environment
- The requirements are mapped to teams or departments to support in RACI (responsible, accountable, consulted, and informed) charts
- Initially focused on the engineering aspect of cloud security, this establishes the accountability and collaboration across the organization

Defined
- Reviewed organization reporting structure and/or virtual team setup to align with the cloud support functions
- The organization's alignment to support the DevSecOps movement has been determined
- Established the RACI for the cloud operations as it relates to security

Quantatively Managed
- Established the effectiveness of each aligned functional area by reviewing funding, resources, and operational metrics. This is an enabler to adjust supporting model for cloud

Optimizing
- Business, audit, and external review factors are taken into adjusting the organization's alignment from RACI, resources, and strategic angles

SANS training:

LDR520: Cloud Security for Leaders

sans.org/ldr520