SANS

CYBERSECURITY LEADERSHIP

CISO Scorecard

Version 1.2

AND

Cloud Security Maturity Model

For Cyber Leaders of Today and Tomorrow

sans.org/cybersecurity-leadership

LDR_CISO-CSMM_v1.2_0922

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 Security Frameworks and 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*

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

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

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

SANS CLOUD SECURITY MATURITY MODEL

Infrastructure Architecture and Protection

Config Management

Initial
- Follow the CSP's best security practices where possible

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

Defined
- Automated config guardrail validation in place and validating resources are adhering to configuration standard. Alerts and notification are generated on non-compliance

Quantatively Managed
- Periodic review of config guardrails
- Automated config validation automatically prevent bad configuration from being provisioned and automatically remediate some key violations

Optimizing
- Automated config validation automatically remediates all non-compliance configuration

Image Management

Initial
- May use manually built images or images from marketplace public repo

Managed
- Develop an enterprise standard for images in terms of security requirements. Restrict virtual machine and container images to approved ones

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

Quantatively Managed
- Automated process extend to manage full lifecycle of image including evergreening running images, across all computing environment (multi-cloud and on-prem)

Optimizing
- Image management practices extend to multicloud environments

Cloud Architecture

Initial
- Adopt applicable Landing Zone's best practices where possible

Managed
- Reviewed and adopted most of Land Zone's best practices. Benchmark against the Well Architected Framework/ Architecture Framework, set a roadmap to the necessary adoption steps.

Defined
- Defined path towards immutable architecture and ZeroTrust architecture. Laying out target patterns and road map for implementation

Quantatively Managed
- Mostly adopted Well Architected Framework/ Architecture Framework and have most of the components automated in code for enforcement and provisioning

Optimizing
- Periodic refinement of target state with regards to alignment with Well Architected Framework/ Architecture framework due to both updates to the framework and needs/improvement of the organization

Resource Management

Initial
- Define tagging scheme and inventory system with cost mangement in consideration
- Resources maybe managed over ad-hoc and manual methods

Managed
- Automate the resource management (using code), ensure resources are consistently created and managed. Enforcing the enterprise tagging scheme

Defined
- Resource provisioning and management are mostly done over automation. Automation mechanism applies the guardrail.
- Use CSP/third party asset inventory system to map out assets in cloud.

Quantatively Managed
- Consolidate resource visibility and management in multicloud environment, preferable using the same tool across all CSPs

Optimizing
- Continuously align the secruity guardrail with the resource management automation tool

Network Control

Initial
- Determine the geolocation and network segmentation requirements. May involve the use of traditional enterprise network security appliance for initial ease of management

Managed
- Define cloud network components protection posture including PaaS offerings. Involving the use of VNet/VPC, Internet gateways, subnets, VPC/Private Endpoints and other ACL's.
- Determine the best option to create a reliable and high performing connectivity with on-prem network

Defined
- Determine IP address management strategy especially to avoid resource dangling.
- Prioritize the use of native defense components over 3rd party appliance eg. security groups over firewall appliance.

Quantatively Managed
- Leverage SASE to enforce trusted access to the cloud environment.
- Manage egress traffic from all cloud resources on top of inbound controls.

Optimizing
- Catalog multi-cloud and SaaS services, use automation to enforce secure connectivitity for the resource access.

Security Governance

Cost Management

Initial
- Adhoc cost attribution to business process. Manual cost management with resources

Managed
- Cost management orinciples generally agreed by all lines of business.

Defined
- Cost management policy established. Cost planning effort in place. Initial budget deviation reporting. Clear financial alignment between resources and ownership.

Quantatively Managed
- Education of cost management in place. Align subscription strategy to utilization and purchasing model. Report deviation and underutilization to each line of business. Drive remediation based on reporting

Optimizing
- Align business goals with planned budget. Adjust architecture patterns to align with subscription model. Active addressing of plan vs. actual spending.

Cloud Governance Committee

Initial
- Formed an alliance of responsible executives from multiple departments to delegate the cloud related decisions. This alliance would meet on regular basis. Begin to identify the cross functional stakeholders

Managed
- Stakeholders, especially sponsors from cross functional areas (eg., legal, lines of business, IT, security) are identified and meeting on regular basis
- Charter of the committee formulated

Defined
- The area of focus by each team related to cloud governance is identified. Sponsors identified the delegation model. Operational rthythm is identified. Key metrics to evaluate performance established

Quantatively Managed
- Formalize the decisions of the committee and the execution and enforcement transition. Continuous process to maintain a risk register and also a pipeline of topics for committee to work on.

Optimizing
- Continuously assessment of committee membership span in the organization. Evaluate performance indicators and accept feedback from leadership of the organization to adjust focus of committee

Policy

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

Managed
- Define the key objectives of the controls and the relationship to the detailed technical guardrails which implement the controls. Communication plan drafted with emphasis on incremental nature of cloud security policy. Business aptite for risk identified for policy drafting. Compliance requirements identified

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

Quantatively Managed
- Enforcement methods and processes refined based on feedback and metrics.
- Establish exception management process.

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

Strategy/Plan

Initial
- Roadmap establishment with clear understanding of business objectives and shared responsibilities model

Managed
- Consolidation of various factors (business objectives, IT pirorities, budget, time constraint) in the organization to make initial choices in roadmap. Determine the right level of security friction
- Incorporate the automation and devsecops aspects into security roadmap

Defined
- Strategy/Roadmap communication and buy-ins

Data Protection

Data Encryption

Initial
- Enterprise encryption policy is aligned with necessary regulatory requirements.

Managed
- Encryption settings for each adopted service are configured. Cloud to onpremise communication is routed over a secure encrypted channel

Defined
- Existing applications that use encryption in transit
- Components are migrated to Cloud native options.

Quantatively Managed
- Automated enforcement of the encryption policy

Optimizing
- Encryption configurations are periodically reviewed in Cloud to ensure the latest up-to-date best practices are adopted.

Data Classification and Protection

Initial
- Manual and limited automated inventory exists of locations where sensitive data is stored and SaaS services are used.

Managed
- Native CSP rules are used to run discovery scans. 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 to scan contents to find and respond to sensitive data patterns as well as threats like cloud malware.

Data Backup

Initial
- Business continuity and disaster recovery
- Requirements are identified and documented.

Managed
- Cloud environment is configured on best effort basis to match availability requirements.
- Configuration guardrails for configuration are updated to include backup configurations.

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

Quantatively Managed
- Tags and resource IDs are used to automatically identify resources that store data for business-critical applications and protect data using immutable backups (eg., AWS Backup Vault Lock).

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

Key Management

Initial
- The level of trust required has been determined with regards to Key management (eg., compliance). Usage of the default CSP managed is key for encryption usage.

Managed
- Key management service is used to manage keys. Disaster recovery requirements for keys have been established.

Defined
- Key management service and customer managed keys are leveraged for 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.

Optimizing
- Periodic validation that all keys in the Cloud environment managed by key management service. Exercises on the recovery actions on disaster affecting keys.

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.
- Review the baseline security posture report from the service providers

Managed
- Organizational use cases in the cloud have been analyzed and the current cloud security posture has been established.
- Identify the benchmark standards appropriate for measuing the organization's cloud security posture.
- Remediate the top findings 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 reports the results back to the key stakeholders.
- Publish key metrics on the overall performance of the posture validation effort

Optimizing
- Tools are adopted to streamline and improve, such as GRC tools or CASB to automate them into workstreams of day-to-day tasks

Regulatory Compliance

Initial
- Gather information on the workload to be put in the cloud. Type of data records involved, nature of the workload and geographic locations of the cloud service are probably the most crucial information to collect.
- Identify the relevant regulatory requirements with regards to using cloud service providers for hosting workload
- Leverage CSP-provided regulatory compliarce 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 of legal compliance requirements based on the cloud setup changes, possibly due to new service adoption or new workload architecture

Quantatively Managed
- For the compliance requirements that require recurring monitoring, automate the process in the cloud environment so the reports are generated automatically. Regularly review the reports generated to validate compliance.

Optimizing
- Compliance validation process largely rolled into the assurance automated processes with automation and monitoring

Security Testing

Initial
- Perform vulnerability assessment with traditional remote scanning ability to detect known vulnerabilities.
- Perform penetration testing exercises with basic threat assumptions such as external attacker attempting to breach the cloud environment.
- Use CSP's security validation services to generate report of commonly known misconfiguration and vulnerabilities.

Managed
- Leverage cloud-native or third-party assessment tools focused in configured validation area to detect misconfiguration
- Pentest is conducted on regular intervals
- Consolidate the vulnerability views across on-premise and cloud for holistic view

Defined
- Penetration testing is based on specific compromise scenarios that would reflect real-world attacker. The scenario 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 timeline and both validated for remediation and engineered to avoid future recurrance.

Quantatively Managed
- Threat model of the cloud environment and common access to use-cases are developed and these use-cases are used to develop penetration or purple team scenarios.

Optimizing
- Conduct regular attack simulations to gain better understanding of the blast radius and also validate the effectivenss of in-control technology and processes.

Detection and Response

Security Intelligence

Initial
- Subscribe to intelligence feed available to organization. The feed can be industry aligned.

Managed
- Analyze Cloud environment setup and generate original detection logic for the Cloud environment in use.
- Refine industry intelligence feed to attain better detection

Defined
- Recurring generation of new detection logic through the learnings from incidents or threat hunting activities in the environment.

Quantatively Managed
- Perform threat modeling and purple team exercise to determine the abuse cases for monitoring. Continue to evaluate additional threat feeds to be integrated

Optimizing
- Integrate metrics into the security intelligence evaluation process.

Analysis and Monitoring

Initial
- Turn on cloud native platform monitoring capability. Use default monitoring use-cases for monitoring

Managed
- Cloud platform logs are collected for analysis. Integration with self generated intelligence.

Defined
- Start consolidating cloud platform logs and enterprise platform logs into SIEM
- Collect and analyze Network flow/traffic-based logs
- Maintain the alert at expected false positive ratio
- Normalizing events across different sources

Quantatively Managed
- Logs across on-prem and cloud enviornment consolidated into single analysis technology for single pane of glass view

Optimizing
- Consolidate either the logs of multi-cloud platforms into a single technology or analyze in native cloud environment then consolidate the relevant alerts and logs together for analysis.

Response

Initial
- Start documenting playbooks for common tasks for response.
- Start with Responding on critical detection by the native cloud platform security monitoring technology

Managed
- Establish containment and eradication workflow in cloud environment and define the playbooks to support these operations

Defined
- Use tabletop walkthrough/exercise to help refine the incident response playbooks
- Automate the most frequently used playbooks
- Focus on automating passive response tasks to gain confidence

Quantatively Managed
- Conduct purple team exercise to validate detection and repsonse capabilities

Optimizing
- Automated most playbooks. Recurring process to review playbooks' effectiveness and efficiency

Log Management

Initial
- May send logs to on-prem log collection for analysis.
- Define plans for logs storage, with considerations for cost of storage, ingestion and transfer.

Managed
- Established logging standards for Cloud native components. Config to be integrated to automatic resource provisioning

Defined
- Cloud platform and resource logs consolidated in cloud

Quantatively Managed
- Enterprise logs consolidated. Event logging requirements and config aligned enterprise wide

Optimizing
- Multicloud logs consolidation and log configuation normalization

Workforce Transformation

Skill Readiness

Initial
- Focus the training the "pioneer" group of core users and members who are working directly on and responsible for setting up the cloud environment.

Managed
- Map job functions to skill requirements to align with training.
- Develop security-specific training and certification paths for main groups of enterprise users. The key roles would consist of developers, infrastructure, engineering, security, management and operational teams.

Defined
- Establish on-the-job training, hands-on and/or job-shadow training in additional to classroom and certification programs.

Quantatively Managed
- Make security-related cloud training open to general IT team members to expand talent pool.
- Conduct validation with teams via a survey on the relevance of training and job functions. Refine training scope to align with job requirements.

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

Organizational Alignment

Initial
- Each team within the organization supports the cloud transformation 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
- Map and document the required security functions to support the cloud environment. The requirements are then mapped to teams or departments to support in RACI (responsible, accountable, consulted, and informed) charts. Initial focus could be in the engineering aspect of cloud security. This estabalishes the accountability and collaboration across the organization.

Defined
- Review the organization's reporting structure and/or virtual-team setup to align with the cloud support functions
- Determine the organization's alignment to support the DevSecOps movement.
- Establish the RACI for the cloud operations as it relates to security

Quantatively Managed
- By reviewing funding, resources and operational metrics establish the effectiveness of each key area of alignment. This enables the organization to adjust its supporting model for cloud

Optimizing
- Taking in business, audit, and external review factors into adjusting the organization's alignment from RACI, resources, and strategic angles.

SANS training:
MGT520: Leading Cloud Security Design and Implementation
sans.org/mgt520

IAM

Segregation

Initial
- Mandate the use of approved cloud environment/accounts. Isolate functional area (e.g., Dev,Test, Prod) where possible and different projects for isolation to reduce blast radius

Managed
- Established the enterprise resources permission segregation model in alignment with CSP's best practices. Determine the level of separation necessary (e.g., multi-account, multi-subscription) The segregation model should have taken enterprise security variations into account (e.g., department or subsidary differences)

Defined
- Update the enterprise IaC templates with the segregation model.

Quantatively Managed
- Align the segregation model to multicloud environment, logical seperation should maintain consistently across CSPs but the technical implementation can be different.
- Leverage automation to periodically identify the discrepency to the segregation model.

Optimizing
- Using configuration management solutions, prevent segregation mis-aligned resource/objects from being created.

Identity Management

Initial
- Accounts maybe 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. The usage of the single authentication system span to all cloud based data and control panes.
- Use user templates for consistent provisioning and deprovisioning of accounts and implement account security policies.

Defined
- Build centralized access request, provision and de-provisioning workflow that is automated and with proper approval and visibility built in.
- Established the third-party and client-identity stategy for access to cloud environment and whether integration of identity directory is necessary.

Quantatively Managed
- Align the user management practice to multicloud environment. Single directory system should serve across all leveraged cloud environments.
- Customers identity are consolidated on one directory and may be consolidated to the enterprise system with proper segregation.
- Expand the scope of MFA/passwordless usage to more general users.

Optimizing
- Eliminate weak authentication usage in the environment.

Access Management

Initial
- Establish roles in the organization that have access requirements and start mapping out access in relation to cloud environment.
- Apply the access permission required for each role types to the best extend, it is possible at this stage to leverage default permission configuration provided by the CSP
- Secure leadership and organizational buy-ins to transform the traditional rigor in network perimeter management to managing access controls.

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

Defined
- Use Just-In-Time or temporary access management for privileged access for as-needed privilege usage.
- Review adopted cloud services individually and validate the permission granted based on least-privilege principle – refining the permission from the CSP's default role
- Expand the dimensions of access-control policies to incorporate telemetry data of endpoint, network, data, and application – enabling for Zerotrust model.

Quantatively Managed
- Limit administrative account access to certain isolated endpoint assets that are dedicated for such use.
- Enforce consistent approaches and workflow to multicloud environment.

Optimizing
- Leverage the use of attack simulations to identify the full extension of a breach situation and drive access reduction.

Application and Workload Protection

Security Protection Services

Initial
- Cloud native security components are leveraged by applications in ad-hoc manner or follow 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 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
- The enterprise protection profile extended to assist with fine tuning of protection profiles. Allowing application to further secure the environment beyond the basic protection. Gudelines provided on 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 exercise are validated and fine tuned.

Assessment

Initial
- Pentest or other end-of-development cycle testing are performed with most critical workloads. Other forms of testing maybe 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 deploy phases.

Quantatively Managed
- The testing pipeline applies to all applications and related resources running in the cloud environment.
- Threat modeling is performed for applications in 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 of the threat model 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.
- Update enterprise coding standard to reflect on cloud native environment

Defined
- Application design and architecture patterns are established for cloud native solutions.
- The patterns are aligned with the enterprise's cloud architecture decision and considered 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 distributed as code for adoption by teams enterprise wide.
- Development teams are confident in automated development and deployment capability, teams 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 also able to adopt new cloud capabilities and new architecture within a very short period of time and in quick succession.