Attack Surface Management/Exposure Management Strategy

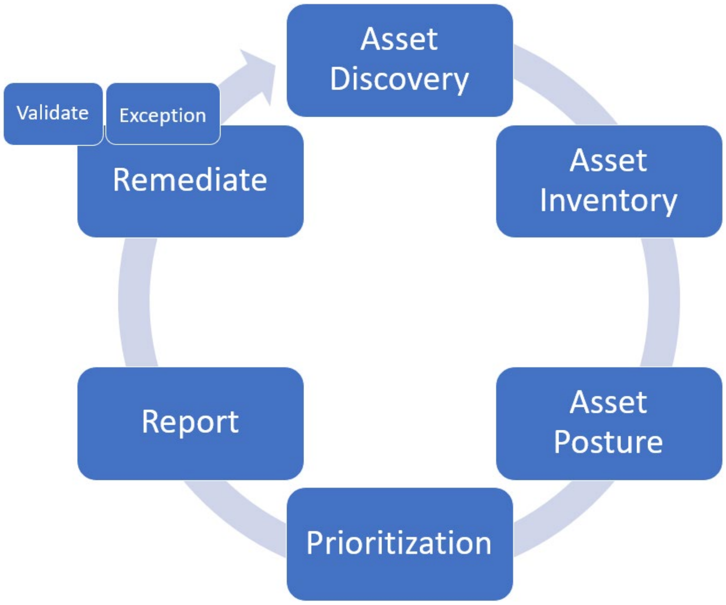
Contents

Overview:

Attack surface management (ASM) is the continuous discovery, analysis, remediation and monitoring of the cybersecurity vulnerabilities and potential attack vectors that make up an organization's attack surface.[1]

This definition includes assets based on availability (internal vs external); organizationally managed (Org owned vs XaaS); type of asset (services, infrastructure, identity, etc.); and the wide variety of activities that would support the NIST CSF functions (Identify, Detect, Protect, Respond & Recover).

ASM is a complex program that incorporates multiple processes; each with their own maturity requirements of staffing, processes, and tooling.



ASM/EM Process

1. Asset Discovery. Ability to "see" all asset types in the ASM scope.
2. Asset Inventory: Method to account for all asset type, owner, location, etc. within the ASM scope.
3. Asset Posture: Ability to scan an asset for misconfigurations and vulnerabilities.
4. Prioritization: Ability to triage findings based on internal or external inputs (i.e., policy or threat intelligence)
5. Report: Ability to notify asset owners of findings and present KPIs, Metrics and Measurements to leadership.
6. Remediate: Process to reduce attack susceptibility.
7. Validate: Process to verify the remediation status and/or overall validity of a finding.
8. Exception: Process to accept risk due to business drivers.

[1] Rule Your Risk™ | CyCognito

Details

1. Major Components

This document focuses on the maturity, effectiveness and strategy pertaining to the 'major' components.

Service	Primary Application
Vulnerability Management	
Cloud Security Posture Management	
AppSec (SCA & SAST)	

2. Advanced Components

As the organization matures in this area the following technology categories can be deployed

Service	Primary Application
Unified ASM Reporting Tool	
Application Security Posture Management	
AppSec (DAST/PAST/MAST)	
Kubernetes Security Posture Management (KSPM)	
SaaS Security Posture Mgmt (SSPM)	
Data Security Posture Management (DSPM)	
Identity Security Posture Management (ISPM)	

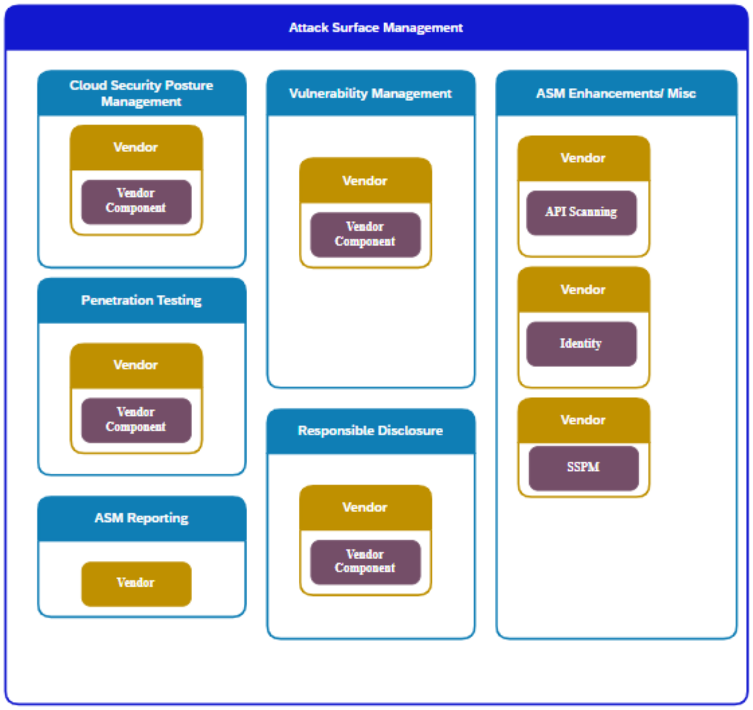
3. Supporting Components

Service	Primary Application
Penetration Testing	
Bug Bounty/ Responsible Disclosure	
Third Party Risk Management	
Certificate Management	
Access Management	
Compliance Management	
Threat Intelligence	

4. Tool Rationalization

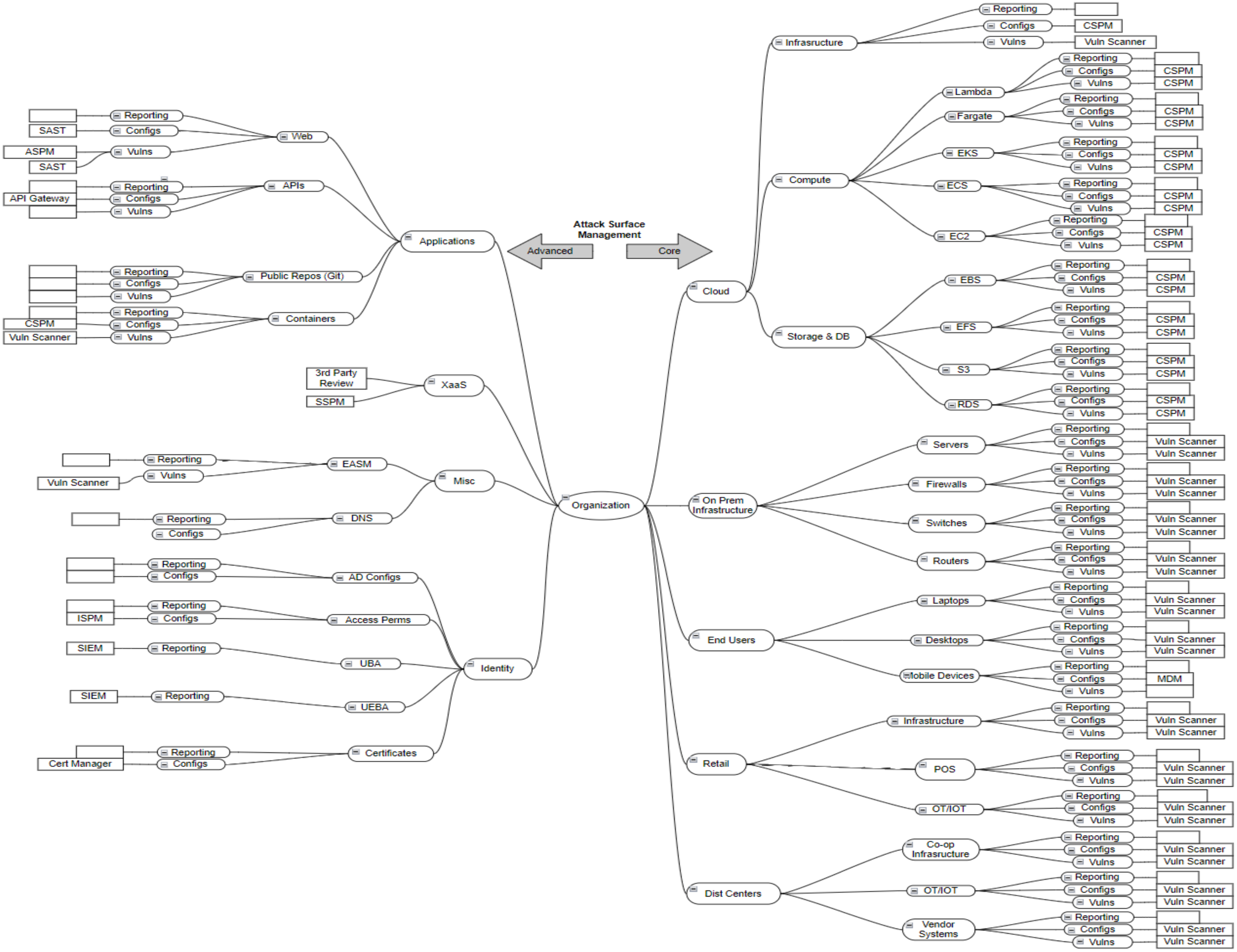
Many of our security applications provide coverage in numerous service areas. This can either be viewed as a hinderance (e.g., misreporting or misrepresentation of # of findings) or a complimentary service (overlapping coverage). In either case, each application should be mapped to its core and auxiliary service functions.

Legend	
Business Capability	Business Supporting Capabilities
Service	Security Services
Provider	Providers/Vendors
Component/Tool	Application



Example Service-to-Tool Mapping

5. ASM/EM Coverage Mind Map



6. Maturity & Effectiveness Criteria

Maturity

Maturity Levels	Roles and Responsibilities	Policy/Procedure Management	Audit and Monitoring	Reporting	Supporting Platforms and Applications
Level 0 (Does Not Exist) **Ad-hoc**					
Level 1 (Initial) *Process unpredictable, poorly controlled and reactive*	No cybersecurity representative assigned or support structure in place for the business. Information cybersecurity issues are not identified mitigated by qualified resources using the defined processes	Minimal or no cybersecurity policies, procedures, or guidelines exist. Documentation is not stored in a central location	Business does not conduct any self-assessments; No controls in place to ensure information (e.g., PII, intellectual property) is protected according to information security policy	Business does not collect or report on information security metrics	No formalized cadence to review application health and maintenance. Maintenance focus is to patch application vulnerabilities only
Level 2 (Repeatable) *Process characterized for the project and is often reactive*	No cybersecurity representative assigned within the business. Alternative support structure may exist. Information cybersecurity issues are identified in an ad-hoc fashion. Limited consistency in the process.	Cybersecurity policies, procedures, and guidelines for major areas are documented and available in a central location. Policy owners and key stakeholders approve policies.	Self-assessment criteria are documented and is known. Business conducts self-assessments but is not a formalized process.	Metrics are identified and scorecard is created.	Process defined for reviewing application health and maintenance. Process is followed infrequently and/or when problems are identified
Level 3 (Defined) *Process characterized for the organization and is proactive*	Cybersecurity lead/SME assigned; Roles and Responsibilities for the lead is understood.	Cybersecurity policies, procedures, and guidelines for all areas are documented. Clearly define information cybersecurity responsibilities and expected behaviors. New employees are briefed on company and business unit cybersecurity policies.	Self-assessment criteria are documented, and monitoring tools are available to automate the process. Self-assessments are performed regularly and is integrated into existing business activities.	Metrics are approved by management and procedural documentation is created and documented.	Process defined for reviewing application health and maintenance. Process is followed on a scheduled cadence. Meetings are recurring and relevant stakeholders (i.e. responsible platform engineer) are required.

Maturity Levels	Roles and Responsibilities	Policy/Procedure Management	Audit and Monitoring	Reporting	Supporting Platforms and Applications
Level 4 (Managed) *Process measured and controlled*	Cybersecurity Lead/SME assigned, Established integration with the cybersecurity community. Representative is a cybersecurity advocate and an influencer. Roles and responsibilities are defined and followed.	Procedures are communicated to individuals who are required to follow them. Information security procedures and controls are implemented in a consistent manner everywhere that the procedure applies and are reinforced through training. Initial testing is performed to ensure controls are operating as intended.	Self-assessment criteria are regularly evaluated and updated to mitigate against newly identified risks. Self-assessment and/or monitoring results are correlated and used to identify mitigating controls and metrics.	Metrics are being tracked and reported to management.	Process defined for reviewing application health and maintenance. Some portions of this process are automated (either through vendor or Org - e.g., Splunk) Process is followed on a scheduled cadence. Meetings are recurring and relevant stakeholders (i.e., responsible platform engineer) are required. Validation of these meetings and process fulfillment is sent to GRC; and reviewed for compliance
Level 5 (Optimized) *Focus on continuous process improvements*	Cybersecurity role hierarchy exists; Responsibilities are defined based on the cybersecurity needs and advancements; Roles are defined to provide the highest level of support.	Effective implementation of information security controls is second nature. Policies, procedures, implementations, and tests are continually reviewed, and improvements are made. Information security is an integrated practice. Threats are continually reevaluated, and controls adapted to changing IT security environment.	Self-assessment/monitoring program is fully operational. Status metrics for self-assessment program are established and met. Comprehensive self-assessment/monitoring program is an integral part of the culture.	Metrics are fully operational and reported to management. Trends are identified and areas that need to be addressed are prioritized.	Process defined for reviewing application health and maintenance. All available portions of this process are automated (either through vendor or Org - e.g., Splunk) Process is followed on a scheduled cadence. Meetings are recurring and relevant stakeholders (i.e., responsible platform engineer) are required. Validation of these meetings and process fulfillment is sent to GRC; and reviewed for compliance"

Effectiveness

Effectiveness Levels	Asset Discovery & Inventory	Asset Posture	Analysis and Prioritization	Reporting	Validation	Remediation/Exception
1	Basic contextual data (e.g., asset details, ownership, relationships) are available from multiple data sources with varying degrees of accuracy.	Infrastructure and applications are scanned ad-hoc or irregularly for vulnerability details, or vulnerability details are acquired from existing data repositories or from the systems themselves as time permits.	Prioritization is performed based on CVSS/Severity designations provided by identification technology or indicated in reports.	Simple, point-in-time operational metrics are available primarily sourced from out-of-box reports leveraging minimal customization or filtering.	Manual testing or review occurs when specifically required or requested.	Patches are applied manually or scheduled by admins and end-users. Configuration requirements are not well-defined, and changes are either applied manually or the automatic application of configurations is only available for a subset of platforms.
2	There is a central repository of contextual data that has some data for most systems and applications	The process, configuration, and schedule for scanning infrastructure and applications is defined and followed for certain departments or divisions within the organization.	Prioritization also includes analysis of other available fields such as whether or not exploits or malware exist or confidence scores.	Filtered reports are created to target specific groups or prioritize findings. Specific divisions or departments have defined their own reporting requirements, including both program and operational metrics, and generate and release the corresponding reports at a defined interval.	Manual testing or review processes are established, and some departments and divisions have defined requirements.	There is a standard schedule defined and technology is available for some divisions or departments or for some platforms to automate patch testing and deployment. Configurations are defined for some divisions or departments or for specific platforms.
3	The central repository requires that certain contextual information be tracked and updated for each system and that it is based on program needs.	There are defined and mandated organization wide scanning requirements and configurations for infrastructure and applications that set a minimum threshold for all departments or divisions.	Prioritization includes correlation with the affected asset, asset group, or application to account for it's criticality in addition to the severity designation. This may require light to moderate customization depending on architecture and design.	Reporting requirements, including all required program, operational, and executive metrics and trends, are well-defined and baseline reports are consistent throughout the organization and tailored or filtered to the individual departments or stakeholders.	Manual testing or review occurs based on reasonable policy-defined requirements that apply to the entire organization and is available as a service where not specifically required by policy.	All departments are required to patch within a certain timeframe and technologies are available to assist with testing and applying patches for all approved platforms. Configurations are defined for all supported platforms and technologies are available to automate or validate configuration changes for all platforms.

Effectiveness Levels	**Asset Discovery & Inventory**	**Asset Posture**	**Analysis and Prioritization**	**Reporting**	**Validation**	**Remediation/Exception**
4	Reports show compliance with contextual information requirements and processes are in place to identify non-compliant, missing, or retired systems and applications.	Scanning coverage is measured and includes the measurement of authenticated vs. unauthenticated scanning (where applicable), the types of automated testing employed, false positive rates, and vulnerability escape rates.	Generic threat intelligence or other custom data, which may require additional products or services, are leveraged to perform prioritization.	Reports and metrics include an indication of compliance with defined policy and standards, treatment timelines, and bug bars. Correlation with other security or contextual data sources allows for more meaningful grouping, improves accuracy, and allows for identification of faulty or inefficient design patterns.	Deviations from manual testing or review requirements are tracked and reported.	Patch management activities are tracked along with compliance with remediation timelines and the success rate. Deviations from configuration requirements and associated service impacts are measured and tracked.
5	Automated or technology-assisted processes and procedures exist to both create and remove systems and applications and associated attributes from the central repository, or data are correlated and reconciled with other systems that contain information about tracked systems and applications.	Scanning is integrated into build-and-release processes and procedures and happens automatically in accordance with requirements. Scanning configurations and rules are updated based on previous measurements.	Company-specific threat intelligence, or other information gathered from the operating environment, is leveraged to preform prioritization. This information may require human analysis or more extensive customization.	Custom reporting is available as a service or via self-service options, or feedback is regularly solicited and reports are updated to reflect changing needs. Automated outlier and trend analysis along with exclusion tracking is performed to identify high/low performers and highlight systemic issues/successes.	Manual testing or review processes include focused testing based on historical test data and commonalities or threat intelligence.	Metrics from vulnerability management change activities are used to modify requirements or streamline future change requests. At least some standard changes are automated. Data from the configuration process along with security incidents and threat intelligence are leveraged to strengthen or relax requirements as needed.

Road Map

1. **Phase 1: Goals and Milestones**
    a. Reporting. Deploy a reporting capability that meets the following requirements:
        - □ Aggregates findings from VM, CSPM and AppSec platforms
        - □ Produces reports by organizational hierarchy based on asset ownership.
        - □ Continue to work on refining the Remediation Tracking Process.
        - □ Create and utilize measurements and metrics.

    b. Application Rationalization. Without duplication, identify the appropriate application to meet the objectives of the ASM Service.
        - □ Review ASM Coverage Mind Map and catalog current and proposed applications that can provide coverage.
        - □ Review proposed technology. Conduct a cost/benefit analysis for 3-yr road mapping service; consider additional headcount requirements.

    c. Review planed 2023 tooling and how to utilize it to enrich data for ASM
2. **Phase 2: Goals and Milestones**
    a. Staffing.
        - □ Onboard additional analyst.
            - Remediation tracking
            - Vulnerability analysis
            - Risk reclassing

    b. Prioritization.
        - □ Utilize enriched data to prioritize remediations. Data enrichment will give us the ability to prioritize remediations outside of merely following policy requirements. For example, using MITRE ATT&CK for attack path analysis would show us remediations that are needed to disrupt a threat actor attack cycle. Some examples of enriched data are the following:
            - Tenable.AD, Wiz.io, Threat Intelligence, Vulnerability Intelligence, Attack Simulation tools
        - □ Prioritization of the deployment of these enrichments will come from the application rationalization list created in 2023.
3. **Phase 3+: Goals and Milestones**
    a. Continue to monitor coverage effectiveness, program maturity, and threat actor trends. Evaluate and invest as needed to drive the required improvements.