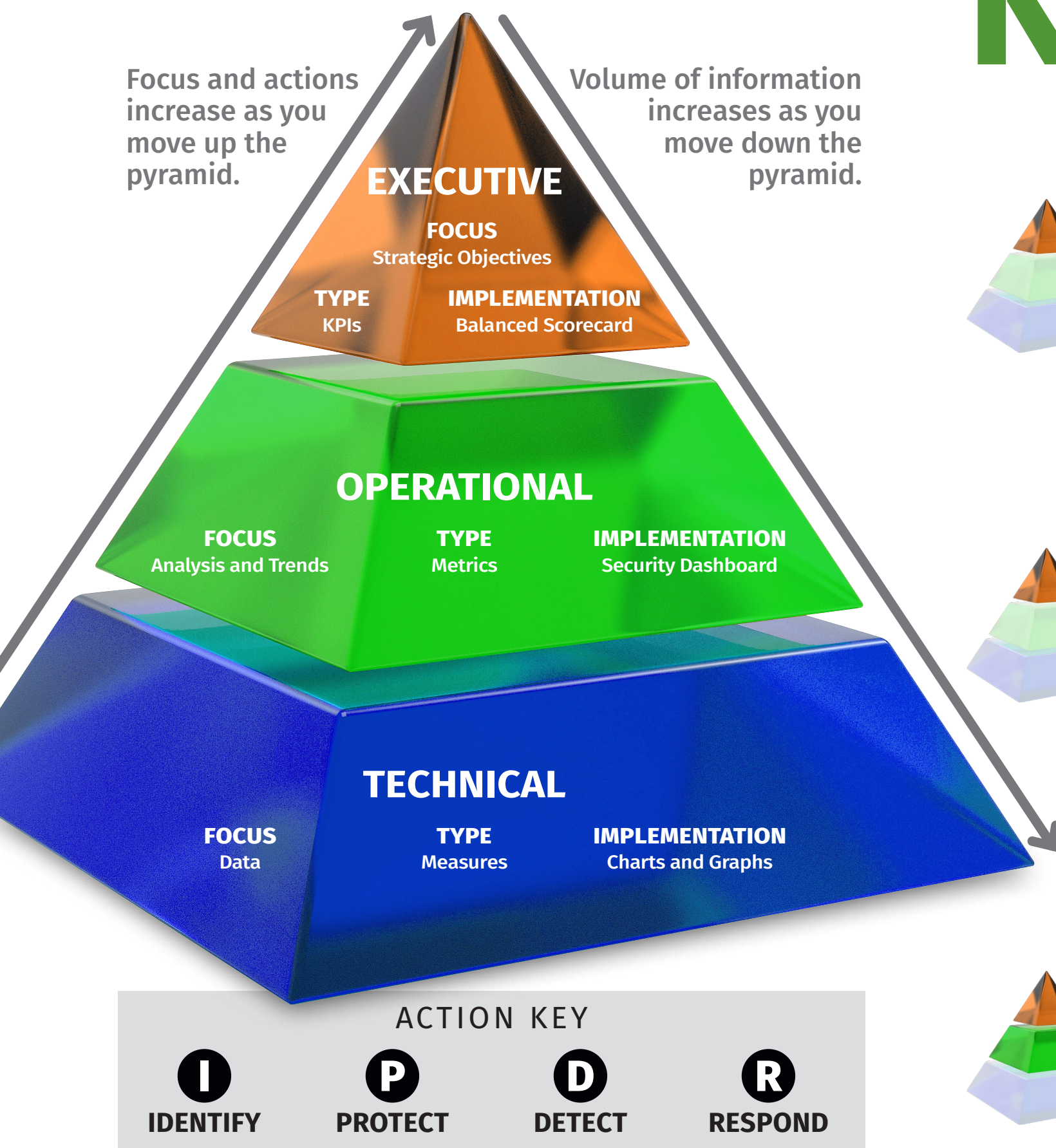
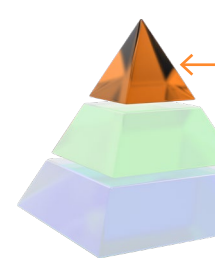


Key Metrics: Cloud and Enterprise

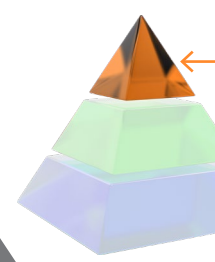


I Average Vendor Security Rating



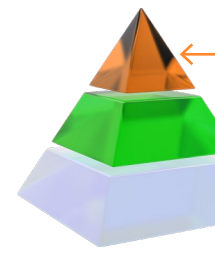
Early stage programs
DESCRIPTION
 This is the average vendor security rating from a solution such as SecurityScorecard, Bitsights, UpGuard or similar tools.
HOW TO CALCULATE
 AVERAGE (SUM of all vendors security rating/total number of vendors rated)
WHAT IT HELPS SHOW/IDENTIFY
 This helps inform the organization of the security posture of vendors that are critical to the organization delivering its services.

P Phishing Attack Success



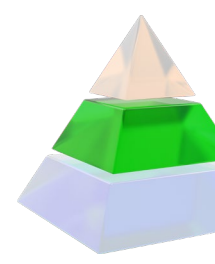
Advanced programs
DESCRIPTION
 Phishing Attack Success is the reported percentage of phishing simulation attacks that were successful over a period of time.
HOW TO CALCULATE
 ABSOLUTE VALUE (Total employees that failed phishing test/Total employees X 100)
WHAT IT HELPS SHOW/IDENTIFY
 This helps inform the organization whether or not users are trained and informed on cybersecurity best practices. incident.

R Vulnerability Remediations Past Due Date



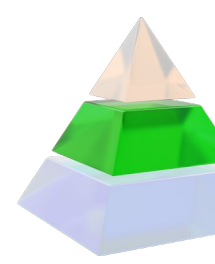
Advanced programs
DESCRIPTION
 The remediations that are not meeting corporate policy requirements for remediation efforts that have not been granted an exception
HOW TO CALCULATE
 (current date - first discovered date) > policy requirement (or if available, leverage due date field)
WHAT IT HELPS SHOW/IDENTIFY
 Any remediation effort not meeting corporate requirements helps to show if there is a problem system or component, or potentially unrealistic remediation timeframes.

I Exclusions



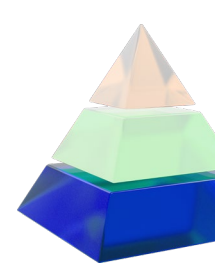
Early stage programs
DESCRIPTION
 Exclusions are the number of exemptions granted and the timeframes associated with the exemptions.
HOW TO CALCULATE
 Number of vulnerabilities being excluded/exempted from remediation efforts
WHAT IT HELPS SHOW/IDENTIFY
 There needs to be a central repository for tracking and managing these exclusions, so stakeholders and VM participants can monitor them over time, and risk managers can determine if any categories of exclusions need to be reported on as a risk finding.

P Administrator's Density



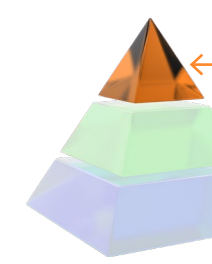
Advanced programs
DESCRIPTION
 Administrator's Density is the percentage of employees with administrator access.
HOW TO CALCULATE
 ABSOLUTE VALUE (Total administrators/Total employees X 100)
WHAT IT HELPS SHOW/IDENTIFY
 This helps inform the organization on whether or not there are a large number of administrators as it relates to the total number of employees in the organization. This metric can prove if the organization is not following a principle of least privilege.

P Patch Velocity



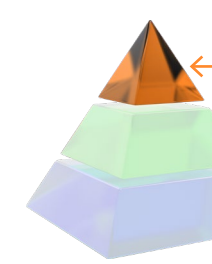
Advanced programs
DESCRIPTION
 Patch Velocity counts patches applied per day.
HOW TO CALCULATE
 ABSOLUTE VALUE (Patches applied on each date when the host was patched)
WHAT IT HELPS SHOW/IDENTIFY
 This helps inform the organization how many patches were applied on each date when the host was patched. It can serve as a way to measure how frequently patching is happening in the environment.

P # of Security Incidents Reported



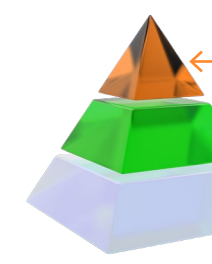
Early stage programs
DESCRIPTION
 # of Security Incidents Reported is the number of security incidents that have been reported over a period of time.
HOW TO CALCULATE
 ABSOLUTE VALUE (Number of security incidents over a period of time)
WHAT IT HELPS SHOW/IDENTIFY
 This helps inform the organization about how many times an attacker breached your information assets or networks. This metric helps inform leadership on the return on investment on cybersecurity tools and processes.

I Cloud Spend Trends



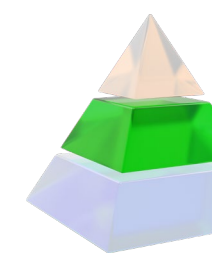
Early stage programs
DESCRIPTION
 Cloud Spend Trends is a report on whether or not cloud resources have increased or decreased over time.
HOW TO CALCULATE
 ABSOLUTE VALUE (Current cloud spend - Past cloud spend [over a period of time])
WHAT IT HELPS SHOW/IDENTIFY
 This helps inform the organization whether or not cloud spending has changed over a period of time which may indicate a potential compromise or development resources that increase the blast radius of a potential incident.

P Vulnerability Churn Rate



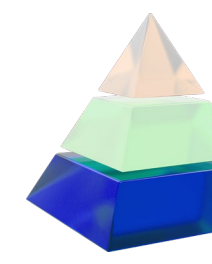
Advanced programs
DESCRIPTION
 Vulnerability Churn Rate is the rate that vulnerabilities are being closed as well as new vulnerabilities being opened
HOW TO CALCULATE
 ABSOLUTE VALUE (New Vulnerabilities - Closed Vulnerabilities [over specific period of time e.g., monthly])
WHAT IT HELPS SHOW/IDENTIFY
 It shows if the vulnerability management program is making headway or is losing the battle.

R Mean Time to Resolve



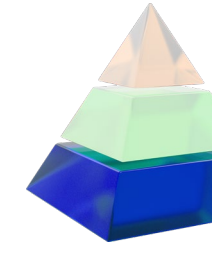
Advanced programs
DESCRIPTION
 Mean Time to Resolve is the average time it takes the organization from discovering a vulnerability until the vulnerability is remediated.
HOW TO CALCULATE
 AVERAGE (Vulnerability Closed date - First Discovered date)
WHAT IT HELPS SHOW/IDENTIFY
 This informs the organization how long it is taking from the time a vulnerability is discovered until it is remediated. It can provide insights when new vulnerabilities arise and/or how long until these are validated findings using normal processes.

I Vulnerability Scanner Coverage



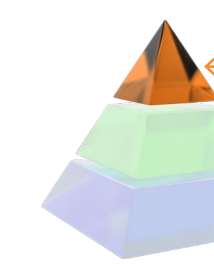
Early stage programs
DESCRIPTION
 Vulnerability Scanner Coverage is the percentage of the system within your organization that is regularly scanned for vulnerabilities.
HOW TO CALCULATE
 Assets being scanned for Vulnerabilities/Total Assets
WHAT IT HELPS SHOW/IDENTIFY
 Knowing if systems are not regularly scanned is crucial to understanding the risk to the business and trend reports will not be as meaningful until coverage is stable.

P Patch Age



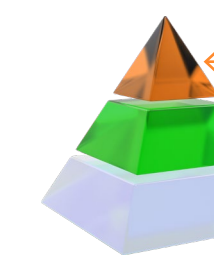
Advanced programs
DESCRIPTION
 Patch Age of a system is the number of days since the last patch was applied.
HOW TO CALCULATE
 ABSOLUTE VALUE (The number of days which have elapsed since the last time a patch was installed on the system)
WHAT IT HELPS SHOW/IDENTIFY
 This helps inform the organization of whether patching has happened recently. Stakeholders can understand the number of days which have elapsed since the last time a patch was installed on the system. A low Patch Age does not necessarily mean that the system is fully patched, but it does indicate that some patching activity has taken place recently.

P # of Vendors with Cyber Incident



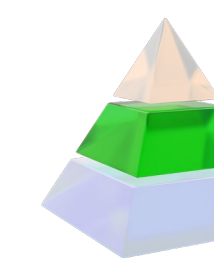
Early stage programs
DESCRIPTION
 This is the number of vendors that have a reported cyber incident over a period of time.
HOW TO CALCULATE
 ABSOLUTE VALUE (Total number of vendors that reported a security incident in a given period)
WHAT IT HELPS SHOW/IDENTIFY
 This helps inform the organization of the number of vendors that have experienced a cyber incident over a period of time which may indicate a weakness within the supply chain.

I Average Exposure Window



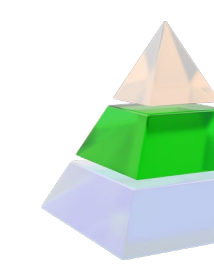
Advanced programs
DESCRIPTION
 The Average Exposure Window is meant to show how long the vulnerabilities are known about prior to them being remediated.
HOW TO CALCULATE
 AVERAGE (Vulnerability Closed date - Vulnerability Published date)
WHAT IT HELPS SHOW/IDENTIFY
 It helps track performance against the policy standards for various vulnerabilities. The goal is to have this as close to Mean Time to Resolve as possible.

D Vulnerability Reopen Rate by XXX



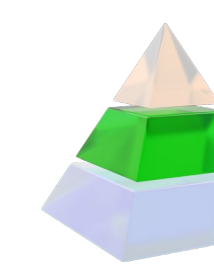
Advanced programs
DESCRIPTION
 Number of vulnerabilities within the environment that are being re-opened for any reason. (XXX can be specific systems, application, business owners, administrators)
HOW TO CALCULATE
 Number of vulnerabilities that were previously closed
WHAT IT HELPS SHOW/IDENTIFY
 Identifies vulnerabilities that were felt to be addressed that no longer are, that normally point to a remediation system problem or a unique system

P Cybersecurity Awareness Training Results



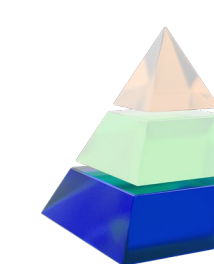
Early stage programs
DESCRIPTION
 This is a percentage of new employees that have completed cybersecurity awareness training within 30 days of hire.
HOW TO CALCULATE
 ABSOLUTE VALUE (Total employees that completed security awareness training/Total employees X 100)
WHAT IT HELPS SHOW/IDENTIFY
 This helps inform the organization whether or not their cybersecurity onboarding and training program is being implemented effectively.

D Mean Time to Detect



Advanced programs
DESCRIPTION
 Mean Time to Detect is the average time it takes the organization to discover a vulnerability from when it is first published, or the asset is added to the network.
HOW TO CALCULATE
 AVERAGE (Vulnerability Publish date - Vulnerability Discovered date)
WHAT IT HELPS SHOW/IDENTIFY
 This metric gives you information on the exposure that the organization has due to vulnerabilities that exist but have not yet been discovered.

D Intrusion Attempts



Advanced programs
DESCRIPTION
 Intrusion Attempts display the number of intrusion attempts over a period of time.
HOW TO CALCULATE
 ABSOLUTE VALUE (The number of intrusion attempts over a period of time)
WHAT IT HELPS SHOW/IDENTIFY
 This helps inform the organization on what the overall number of threats the business faces at any given time. This metric can help prove that cybersecurity threats continue to exist and are growing all the time.



Key Metrics: Cloud and Enterprise

AND

Vulnerability Management Maturity Model

For Cyber Leaders of Today and Tomorrow

sans.org/cybersecurity-leadership

sans.org/cybersecurity-leadership

@secleadership

SANS Security Leadership

Vulnerability Management Maturity Model

	LEVEL 1 Initial	LEVEL 2 Managed	LEVEL 3 Defined	LEVEL 4 Quantitatively Managed	LEVEL 5 Optimizing	
Prepare	Policy & Standards	Policy and standards are undocumented or in a state of change.	Policy and standards are defined in specific areas as a result of a negative impact to the program rather than based on a deliberate selection of best practices or standards from recognized frameworks.	Policy and standards have been carefully selected based on best practices and recognized security frameworks and are updated as needed to fulfill the program's mission. Employees are made aware of standards and training on requirements is available.	Adherence to defined policy and standards is tracked and deviations are highlighted. Training of personnel on requirements is required at least annually.	Automated, proactive controls enforce policy and standards and provide input to regular updates and training requirements.
	Context	Contextual data (e.g., asset details, ownership, relationships) are available from multiple data sources with varying degrees of accuracy.	There is a central repository of contextual data that has some data for most systems and applications.	The central repository requires that certain contextual information be tracked and updated for each system and that it is based on program needs.	Reports show compliance with contextual information requirements and processes are in place to identify non-compliant, missing, or retired systems and applications.	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.
Identify	Automated	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.	The process, configuration, and schedule for scanning infrastructure and applications is defined and followed for certain departments or divisions within the organization. Available technology may vary throughout the organization.	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. Technology is made available throughout the organization through enterprise licensing agreements or as a service.	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.	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.
	Manual	Manual testing or review occurs when specifically required or requested.	Manual testing or review processes are established and some departments and divisions have defined requirements.	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.	Deviations from manual testing or review requirements are tracked and reported.	Manual testing or review processes include focused testing based on historical test data and commonalities or threat intelligence.
	External	External vulnerability reports and disclosures are handled on a case-by-case basis.	Basic vulnerability disclosure policy (VDP) and contact information published, but backend processes and procedures not documented.	More comprehensive VDP in place, along with terms and conditions for external vendors and security researchers, that outlines rules of engagement, tracking, and feedback processes.	Compliance with VDP and terms and conditions is tracked and measured and information is used to streamline processes and evaluate vendors and researchers.	A mature external testing and research program is in place with specific goals and campaigns that may only be available to specific vendors or researchers.
Analyze	Prioritization	Prioritization is performed based on CVSS/Severity designations provided by identification technology or indicated in reports.	Prioritization also includes analysis of other available fields such as whether or not exploits or malware exist or confidence scores.	Prioritization includes correlation with the affected asset, asset group, or application to account for its criticality in addition to the severity designation. This may require light to moderate customization depending on architecture and design.	Generic threat intelligence or other custom data, which may require additional products or services, are leveraged to perform prioritization.	Company-specific threat intelligence, or other information gathered from the operating environment, is leveraged to perform prioritization. This information may require human analysis or more extensive customization.
	Root Cause Analysis	Root cause analysis is performed based on out-of-the-box information such as standard remediation/patch reports or other categorized reports (e.g., OWASP Top 10 category).	Data are lightly customized to apply less granular or more meaningful groupings of data than CVE, CWE, or Top 10 identifiers to facilitate root cause analysis.	Data are also identified, grouped, and/or filtered by department or location to enable identification of location- or group-based deficiencies. This may require light to moderate customization depending on architecture and design.	Data are also identified, grouped, and/or filtered by owner or role. This may require more extensive customization and ongoing maintenance.	An executive dashboard is in place and includes the highest-risk root cause impediments, exclusions, project cost projections, etc. This will require more detailed analysis and customization to become meaningful and should integrate with existing executive business intelligence tools.
Communicate	Metrics & Reporting	Simple, point-in-time operational metrics are available primarily sourced from out-of-the-box reports leveraging minimal customization or filtering.	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.	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.	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.	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.
	Alerting	Alerting is either not available or only available within security-specific technologies.	Integrations exist and alerts are being sent for specific divisions or departments or for users of specific non-security technologies already being leveraged by some stakeholders.	Alerting is available for most stakeholders in their technology of choice.	Visibility and both timing and detail of response to alerts is measured and tracked.	Data are analyzed to develop a standard or automated response to alerts for common issues that can be tied to a common response.
Treat	Change Management	Changes related to vulnerability management activities pass through the same workflow as any other change.	Some changes related to vulnerability management activities have a custom workflow or are treated as standard changes.	Most changes related to vulnerability management activities follow a custom workflow or are treated as standard changes.	Changes related to vulnerability management activities along with success rates are tracked. Timing is also measured for different stages of the change or subtasks related to the change.	Metrics from vulnerability management change activities are used to modify requirements or streamline future change requests. At least some standard changes are automated.
	Patch Management	Patches are applied manually or scheduled by admins and end-users.	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.	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.	Patch management activities are tracked along with compliance with remediation timelines and the success rate.	Data from patch management activities, security incidents, and threat intelligence are used to right-size remediation timelines and identify process or technology changes.
	Configuration Management	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.	Configurations are defined for some divisions or departments or for specific platforms.	Configurations are defined for all supported platforms and technologies are available to automate or validate configuration changes for all platforms.	Deviations from configuration requirements and associated service impacts are measured and tracked.	Data from the configuration process along with security incidents and threat intelligence are leveraged to strengthen or relax requirements as needed.

Contextual Information
Contextual information is key to helping us prioritize our vulnerability backlog and to understand where we might need more focus or help. Some examples of contextual information include:



SEC557: Continuous Automation for Enterprise and Cloud Compliance
Measure what matters, not what's easy. Agile development, DevOps, cloud technologies, and virtualization have enabled organizations to build and deploy systems at a terrifyingly fast rate. The old and cumbersome manual ways to test security and compliance can't keep up. You need to understand and use the same tools and techniques that your developers and engineers are using, and you need to be able to generate results quickly and often - without slowing down your organization. SEC557 teaches professionals tasked with ensuring security and compliance how to stop being a roadblock and work at the speed of the modern enterprise. **30 Hands-On Labs**

MGT516: Managing Security Vulnerabilities: Enterprise and Cloud
Stop treating symptoms. Cure the disease. Vulnerability, patch, and configuration management are not new security topics. In fact, they are some of the oldest security functions. Yet, we still struggle to manage these capabilities effectively. The quantity of outstanding vulnerabilities for most large organizations is overwhelming, and all organizations struggle to keep up with the never-ending onslaught of new vulnerabilities in their infrastructure and applications. When you add in the cloud and the increasing speed with which all organizations must deliver systems, applications, and features to both their internal and external customers, security may seem unachievable. This course will show you the most effective ways to mature your vulnerability management program and move from identifying vulnerabilities to successfully treating them. **16 Cyber42 and lab exercises**