From Zero to Hero: aumentando a maturidade em gestão de vulnerabilidades

Eduardo Santos

@edusantos33

Quem sou eu?

- Tech Manager - Red Team | AppSec
- Mestre e Doutorando em Eng. da Computação (UFRN)
- EC-Council CEH Practical | Microsoft AZ-900
- CompTIA Security+ e Pentest+
  - *CompTIA* Network Vulnerability Assessment Professional (*CNVP*)
- {um} Chapter Leader do capítulo OWASP em Natal-RN
- Palestrante em diversos eventos (YSTS, GTS, Campus Party, WTR PoP-RN, OSDFCon, BSides João Pessoa, OWASP@Home, MVS ...)
- Professor em cursos livres e de pós-graduação
- @edusantos.official

How Data Breaches Occur

1 Research

Attacker looks for weaknesses he can exploit

2 Stage Attack

SOCIAL ENGINEERING

Phishing email, spam with malware, phone call, dress like the night janitor, etc.

INFRASTRUCTURE WEAKNESS

FIREWALL WEBSITE WEB SERVER

SQL injection, vulnerability exploitation, session hijacking, etc.

Attacker may need to keep staging attacks until the desired information is obtained or the desired access to the network is achieved

3 Exfiltrate

DATABASE AND FILE SERVERS

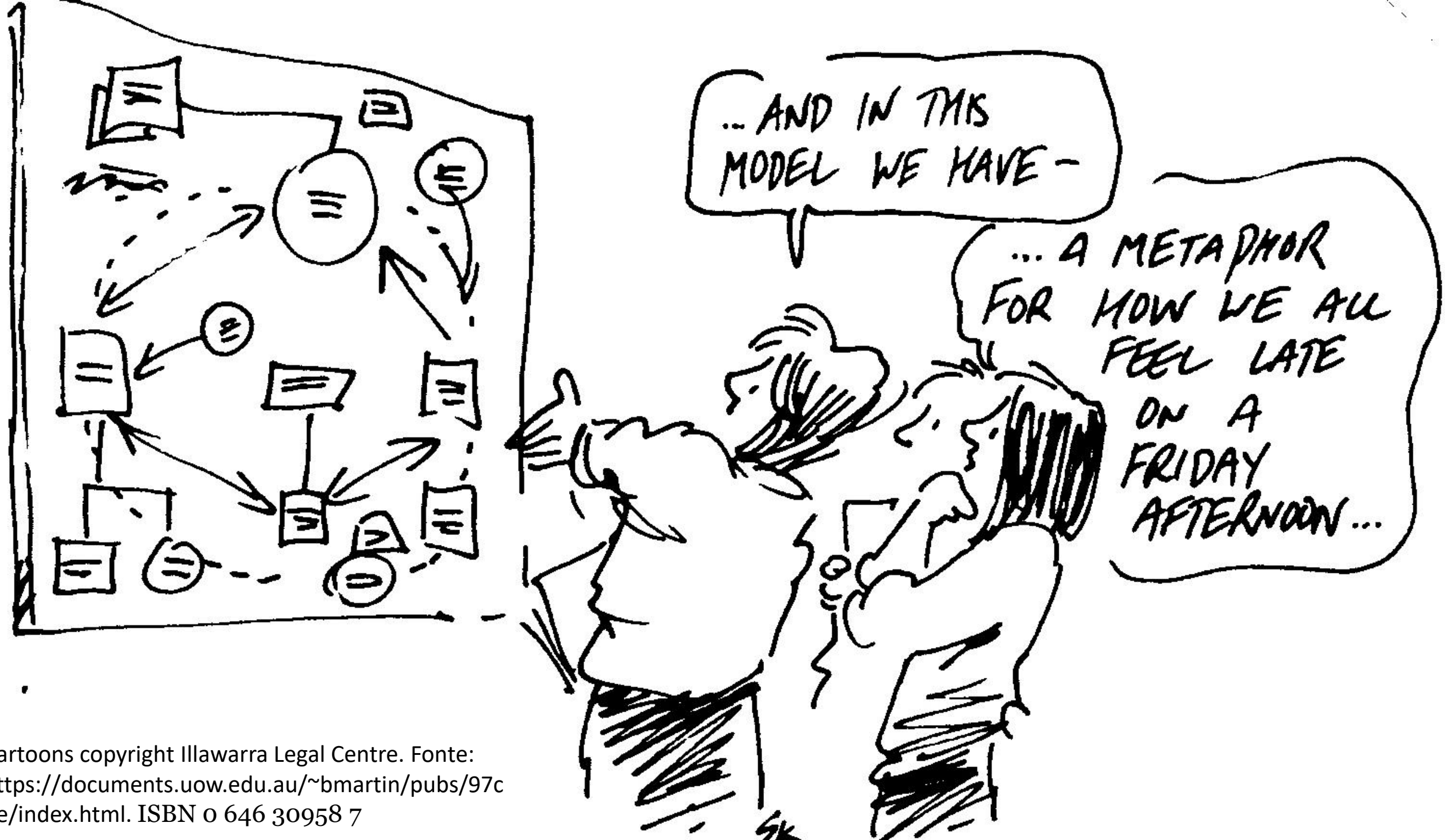
Personally identifiable information (PII), credit card numbers, email addresses, other social details, etc.

Once the attacker maintains acess to the system, exfiltration can indefinitely proceed

HTTP-based path, FTP, email, etc.

Accessed data is exfiltrated back to attacker

Fonte: https://www.trendmicro.com/vinfo/dk/security/definition/data-breach



O que é Vulnerabilidade?

?

“Uma fraqueza de um ativo ou grupo de ativos que pode ser explorado por uma ou mais ameaças.” (ISO 27002)

O que é Gestão de Vulnerabilidades?

??

- Processo no qual as vulnerabilidades em TI são identificadas e os riscos dessas vulnerabilidades são avaliados.
- A avaliação leva a corrigir as vulnerabilidades e remover ou aceitar do risco.

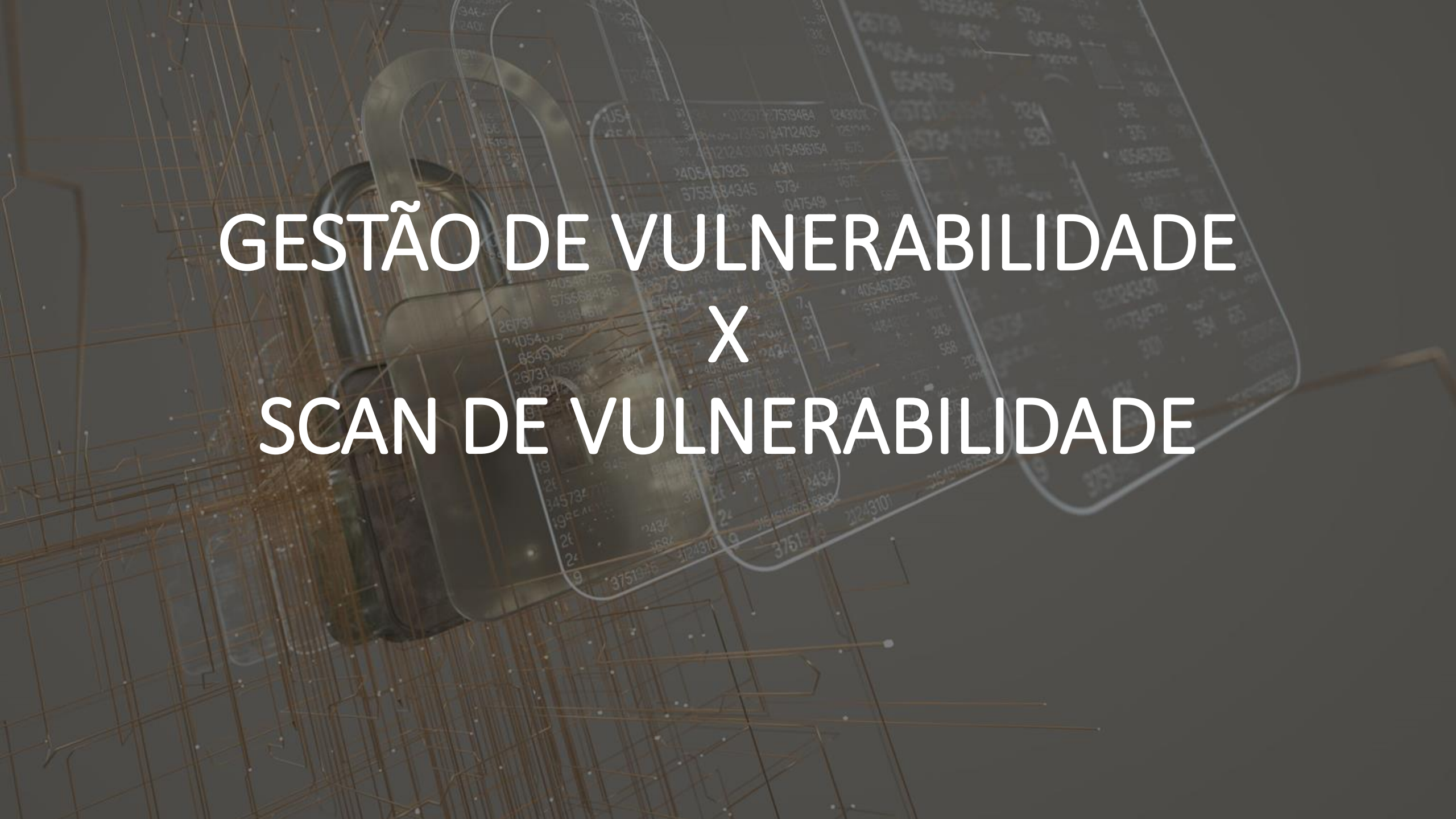
Fonte: PALMAERS, Tom. Implementing a Vulnerability Management Process. GIAC (GSEC) Gold Certification. SANS. 2013 updated in 2021.

Por quê Gestão de Vulnerabilidades?

???

- Permite uma visão geral e contínua das vulnerabilidades e dos riscos no ambiente de TI.
- “Identificar e mitigar vulnerabilidades pode impedir invasão na rede e o roubo de informações” (Williams e Nicollet, 2005).

Fonte: Williams, A and Nicollet, M: Improve IT Security With Vulnerability Management, Gartner ID Number: G00127481, May 2005



GESTÃO DE VULNERABILIDADE
X
SCAN DE VULNERABILIDADE

Vulnerability Management Tools Market

ERPScan

QUALYS® CONTINUOUS SECURITY

Nessus® vulnerability scanner

MAXPATROL

CORE SECURITY

BeyondTrust™

nexpose®

Сканер-ВС анализ защищенности

BEYOND security

DIGITAL DEFENSE INCORPORATED

OpenVAS Open Vulnerability Assessment System

Red Check

SAINT®

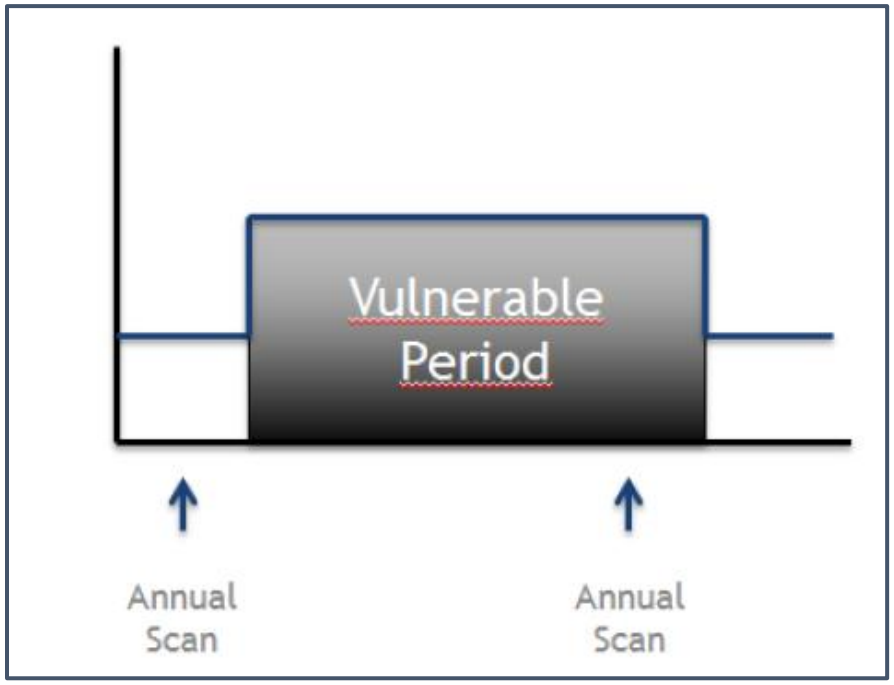
F-Secure.

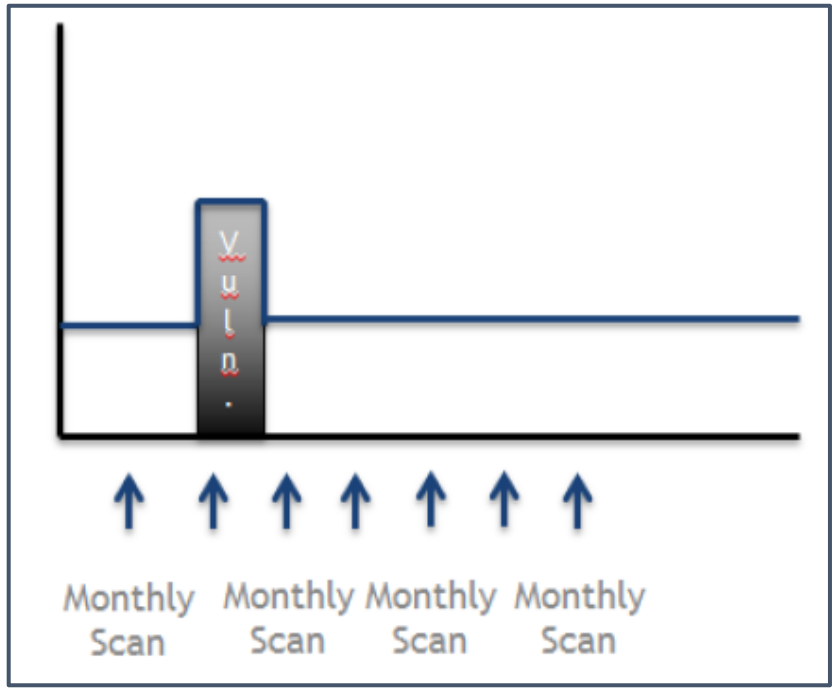
tripwire

secpod Expose the Unknown

Qual o objetivo de um processo de GVuln?

- Detectar e remediar vulnerabilidades em tempo hábil (Qualys, 2008).





Fonte: PALMAERS, Tom. Implementing a Vulnerability Management Process. GIAC (GSEC) Gold Certification. SANS. 2013 updated in 2021.

Papéis e Responsabilidades

Líder do time de GVuln

Analista de GVuln

Líder do time afetado pela vulnerabilidade

Analista, Dev, SRE

SANS

Security Leadership

POSTER

CISO Mind Map

Version 2.5

AND

Vulnerability Management Maturity Model

For Cyber Leaders of Today and Tomorrow

sans.org/cybersecurity-leadership

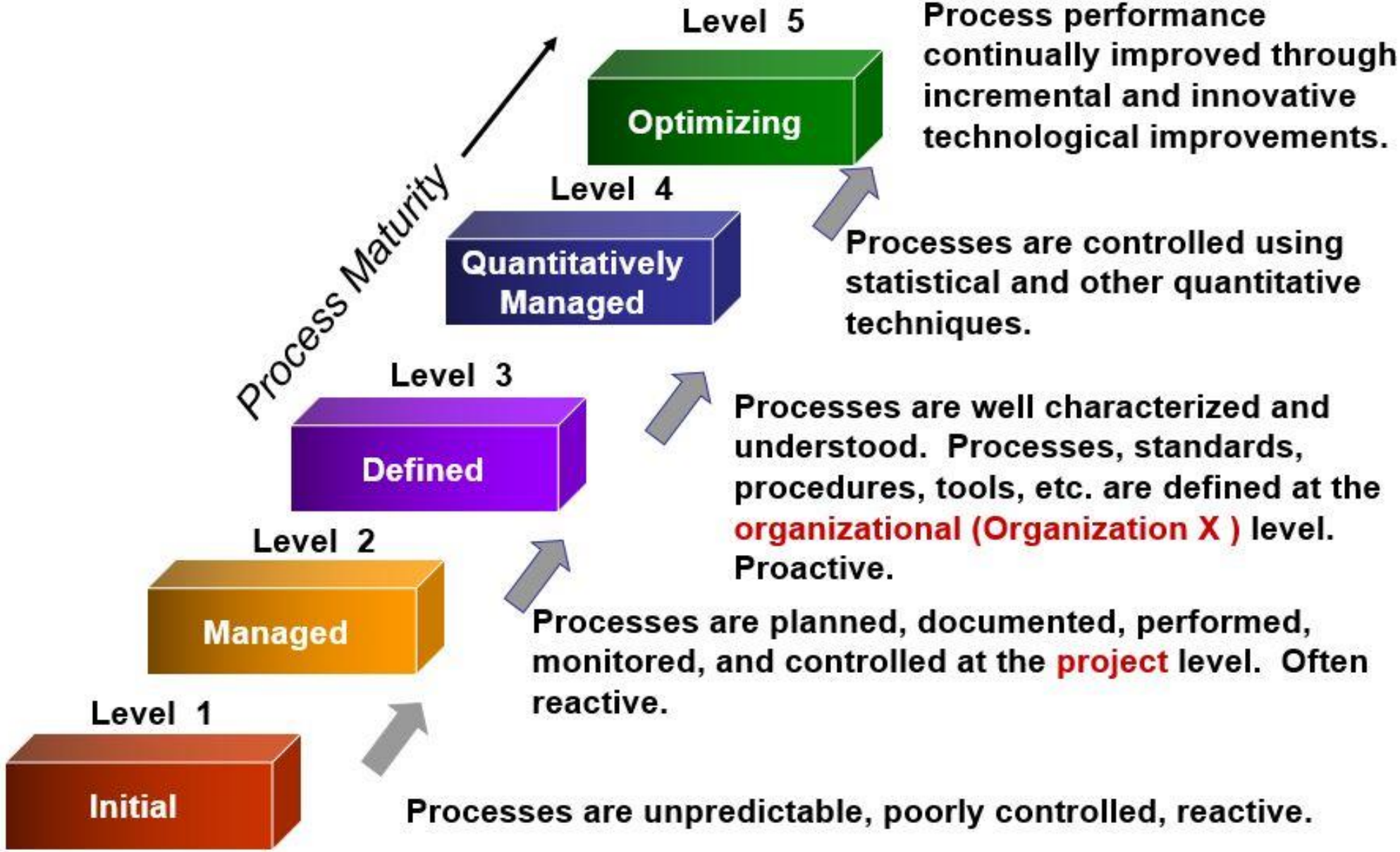
MGTPS_CISO-VM_v2.5_2021

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 it's 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 preform 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.

PIACT


Preparação
Política e Padrões
Contexto
Identificação
Automatizado
Manual
Externo
Análise
Priorização
Análise de Causa Raíz
Comunicação
Métricas e Informes
Alertas
Tratamento
Gerenciamento de Mudanças
Gerenciamento de Patches
Gerenciamento de Configuração

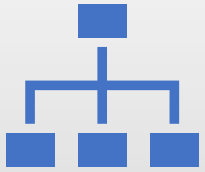


Fonte: https://www.umsl.edu/~sauterv/analysis/Fall2013Papers/Lanjewar/CMMI.html


HEROES
HEROES EVERYWHERE

Como implementar, então?

Preparação



Defina o escopo

Toda Empresa?

Alguma unid. de negócio ou projeto específico?

Identifique os stakeholders

Eles precisarão te dar apoio no processo

Espalhe a palavra

Informe a importância da gestão de vulnerabilidades

Avaliação

Identificar e entender o atual nível de maturidade

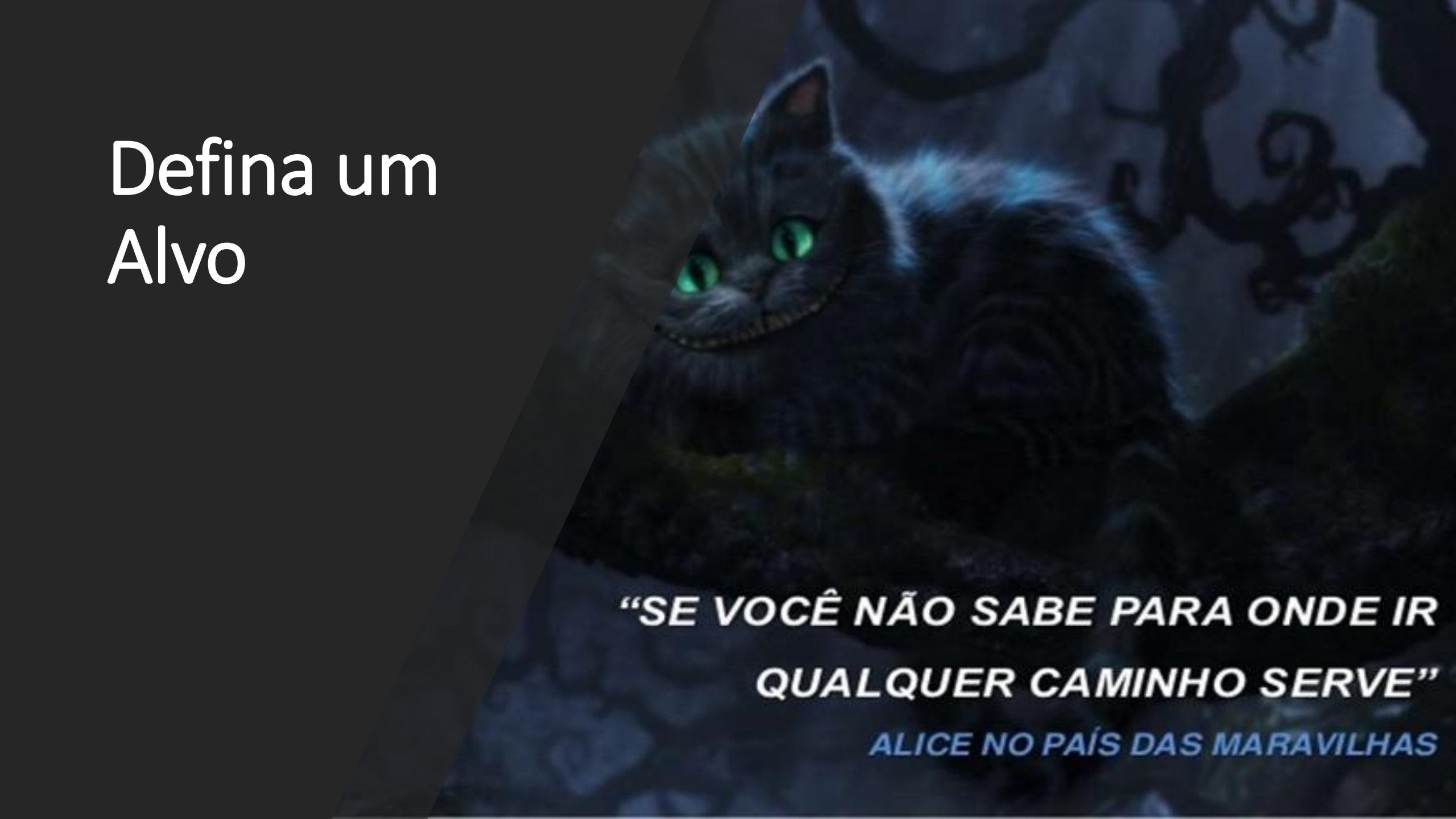
Avaliar as práticas atuais

- O que já está sendo feito?
- Será que não há nada mesmo?

Determine o nível de maturidade

- Dica: criar uma planilha no excel ☺

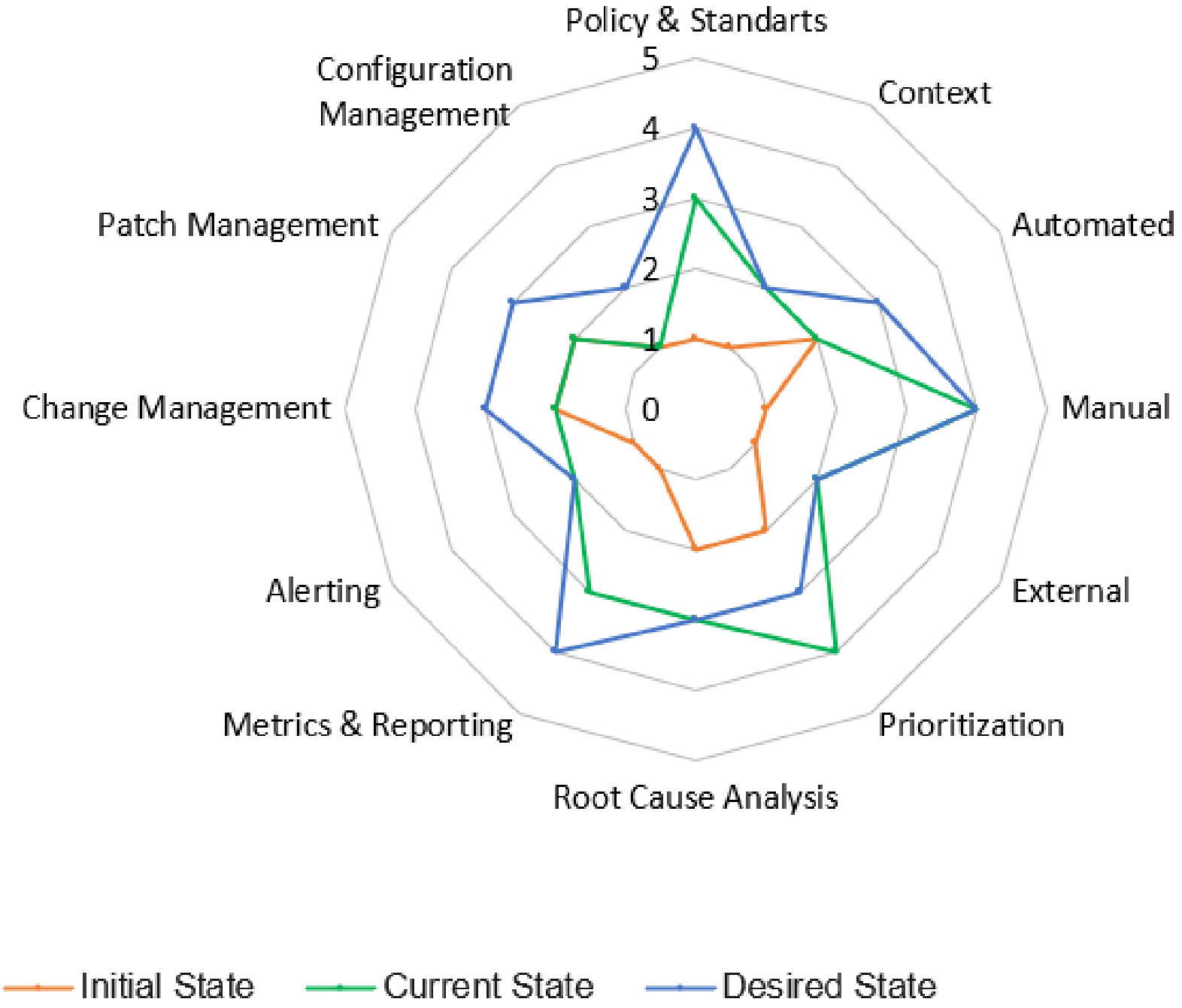
Defina um Alvo



Defina um Alvo

Defina aonde deseja chegar no nível de maturidade em cada domínio do processo **PIACT**

Process	Sub Process	Initial State Maturity Level (Select a Level)	Current State Description	Desired State Maturity Level (Select a Level)	Desired State Description
Prepare	Policy & Standarts	3	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.	4	Adherence to defined policy and standards is tracked and deviations are highlighted. Training of personnel on requirements is required at least annually.
	Context	1	Contextual data (e.g., asset details, ownership, relationships) are available from multiple data sources with varying degrees of accuracy.	2	There is a central repository of contextual data that has some data for most systems and applications.

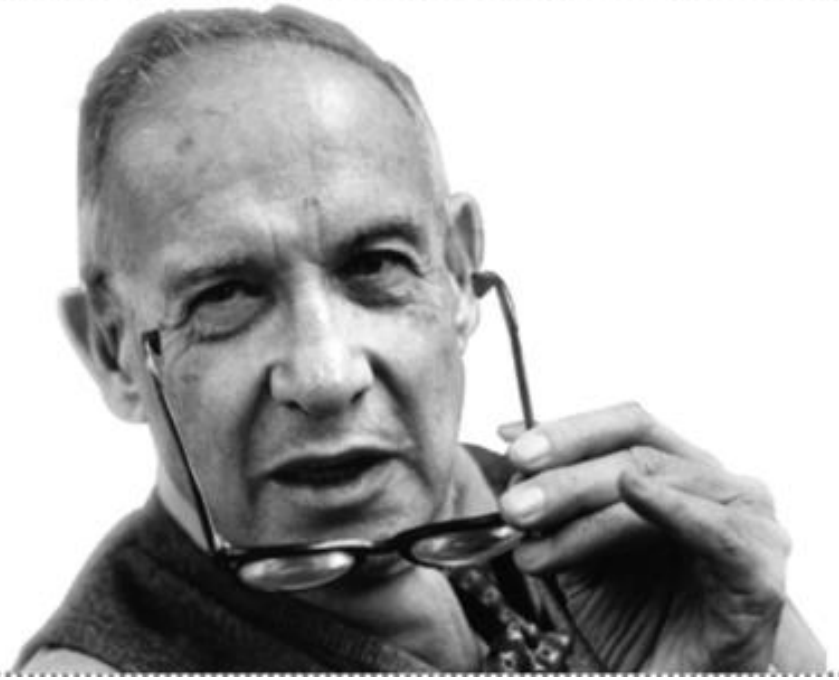

Policy & Standarts
Context
Automated
Manual
External
Prioritization
Root Cause Analysis
Metrics & Reporting
Alerting
Change Management
Patch Management
Configuration Management
5
4
3
2
1
0
Initial State
Current State
Desired State

Bora, que eu Quero é mão na massa!!!

Preparação: Políticas e Padronizações

- Escreve tudo que você está fazendo...
  - Desde o início em conversar com os stakeholders
- Explica as pessoas o que é gestão de vulnerabilidades
  - Treina, faz palestras
  - Periodicamente
- Aplica o **PDCA** em tudo aqui

Preparação: Contexto



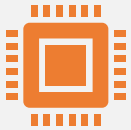
"Se você não pode medir, não pode gerenciar."

Peter Drucker

Preparação: Contexto

- Está relacionado com o escopo definido
- CIS Controls v8
- Utilize ferramentas de gestão de inventário ou de scan de vulnerabilidades

Identificação: Automatizado



ML1: A infraestrutura e os aplicativos são verificados isoladamente ou irregularmente para detalhes de vulnerabilidade…

Escolhe uma ferramenta de scan de vulnerabilidade

Infraestrutura

Aplicações

Scan periódico

Autenticado e não autenticado

Automatiza esse processo para qualquer “coisa” que vá ser utilizado

Identificação: Manual

ML1: Testes manuais ou revisões ocorrem quando solicitados

Testes manuais são feitos em todo o escopo definido

Os testes devem ser trackeados e reportados

Faça testes novos baseado no histórico dos anteriores e focados em Threat Intelligence

Identificação: Externa

ML1: Divulgações de vulnerabilidades externas são tratados caso a caso

Definir uma política de descoberta de vulnerabilidades (VDP)

Publicar informações de contatos Secure.txt

Utilizar plataformas de bug bounty

Análise: Priorização

ML1: Geralmente baseados em CVSS

Existe exploit público ou malware?

Correlacione a vuln com os ativos, grupos de ativos e aplicações

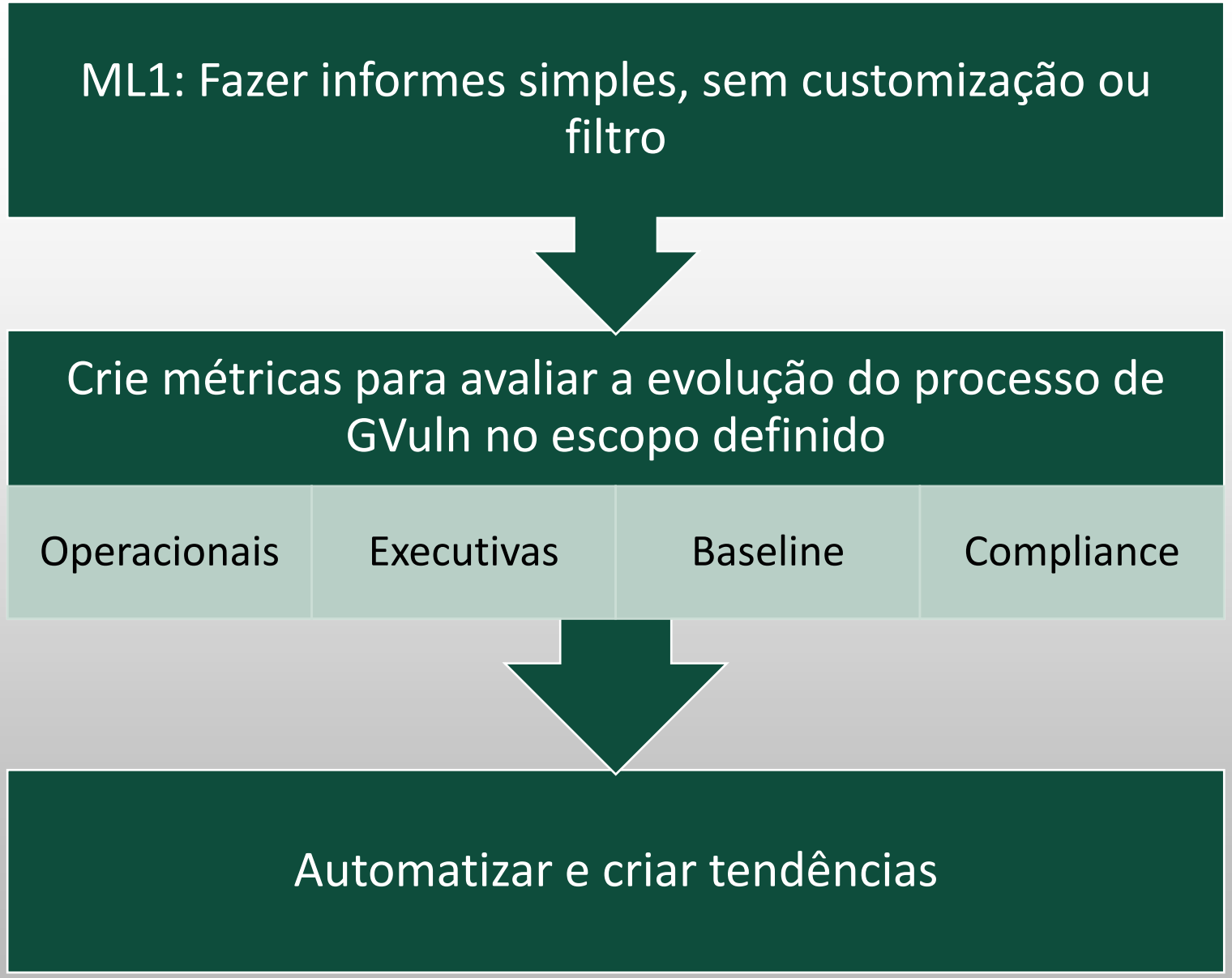
Faça Threat Intelligence

- Básica
- Manual
- Empresa parceira

Análise: Causa Raiz

- ML1: baseada em relatórios padrão de correção ou de categorização com o OWASP Top 10.
- As classificações podem ser avançadas para
  - CVE
  - CWE
  - Agrupadas por grupos semelhantes de aplicações e infra
- Automatizadas
- Análise de tendências

Comunicação: métrica e informe



Comunicação: alertas

- ML1: O alerta não está disponível ou está disponível apenas em tecnologias específicas de segurança
- Crie grupos de pessoas responsáveis pelas partes da infraestrutura e das aplicações
- Alerte aos stakeholders

Comunicação: alertas

- Informações que ajudam a tomar decisões (métricas)
- Crie formas de respostas automatizadas com possíveis soluções
- Ferramentas:
  - Integrações com Slack, Github, ELK...
  - Elastalert

Tratamento: Gestão de mudanças

ML1: As vulnerabilidades passam pelo mesmo fluxo de mudança de outros ativos de TI

Aos poucos crie atividades específicas para vulnerabilidades

Crie métricas

Automatize

Tratamento: Gestão de patch

ML1: Os patches são aplicados manualmente ou agendados por administradores e usuários finais.

Crie escopos de testes de novos patches

- Depois propague isso para todos da organização

Automatize as entregas

Crie métricas

Ferramentas

- WSUS
- Intune
- Repositórios específicos para ambientes *nix

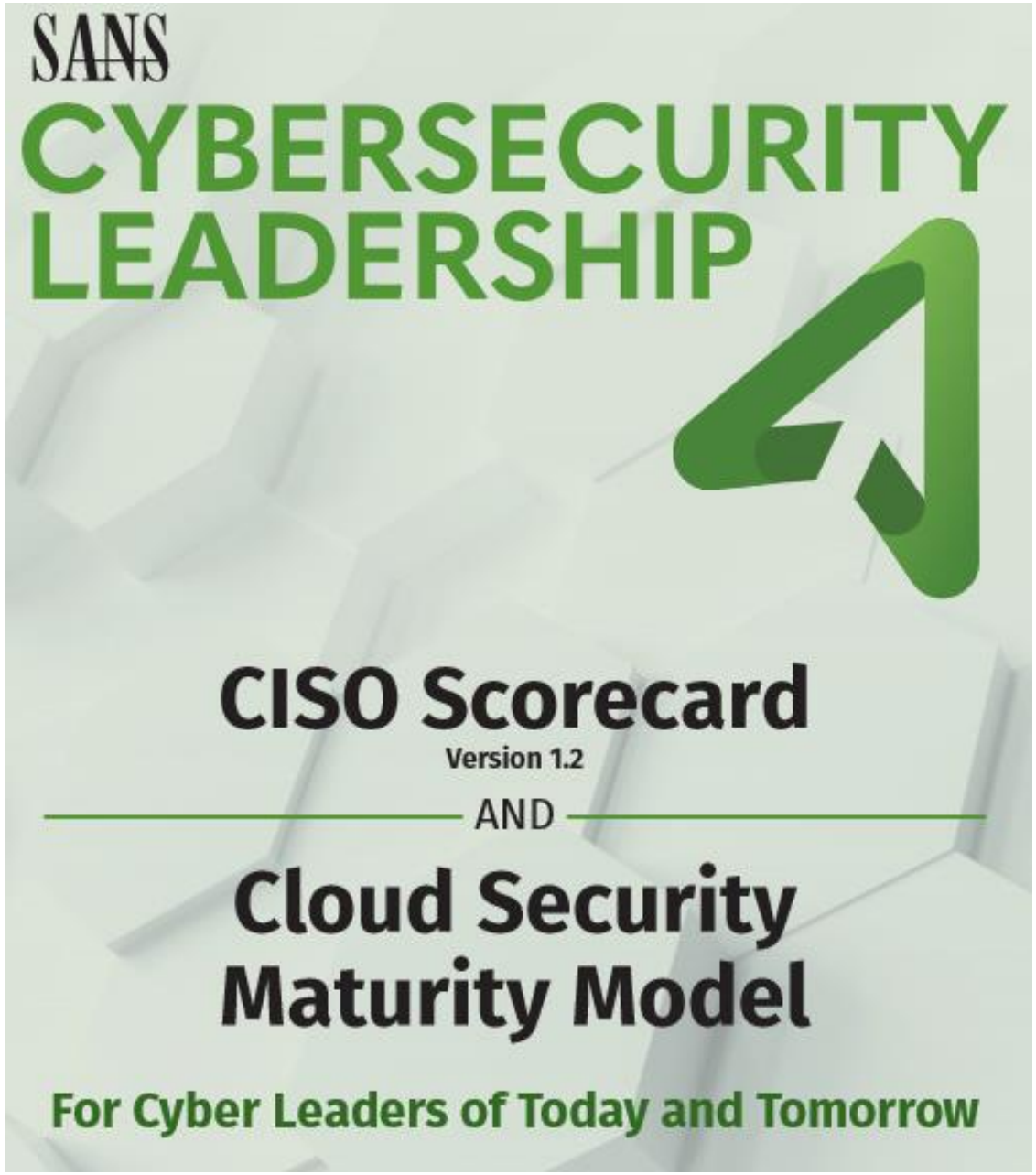
Tratamento: Gestão de Configuração

- ML1: Os requisitos de configuração não estão bem definidos e as alterações são aplicadas manualmente ou a aplicação automática de configurações está disponível apenas para um subconjunto de plataformas.

Tratamento: Gestão de Configuração

- Aplicar gestão de configuração em todo escopo do processo de gestão de vulnerabilidades
  - Suportando tecnologias e plataformas
- Utilizar métricas e analise os impactos das configurações


YOU'RE A HERO, YOU'RE A HERO
YOU'RE ALL HEROES
makeameme.org



https://www.sans.org/posters/ciso-scorecard-cloud-maturity-model/

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

https://www.sans.org/posters/ciso-scorecard-cloud-maturity-model/

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 security 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 ACLs.
- 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 connectivity for the resource access.

Security Governance

Cost Management

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

Managed
- Cost management principles 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 rhythm 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 priorities, 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 measuring 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 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 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

IAM

Infrastructure Architecture and Protection

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 ACLs.
- 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.

Muito Obrigado!!!

@edusantos.oficial

@edusantos33