Governança aliada a operações de segurança

Daniel Bortolazo
dbortolazo@paloaltonetworks.com

November de 2020

Zero Trust - John Kindervag

- Creator of Zero Trust.
- Field CTO at Palo Alto Networks
- Board Advisor at Strong Salt
- Ex-Forrester

5:40 pm - 6:10 pm | By John Kindervag,

Palestra: Zero Trust - Mitigando os riscos de amanhã

NETOPS, SECOPS, WHATOPS?

SecOps - Lidar com ameaças que não são evitadas de outra forma.

Operações de segurança

1 IDENTIFICAR

2 INVESTIGAR

3 MITIGAR

4 MELHORIA CONTÍNUA

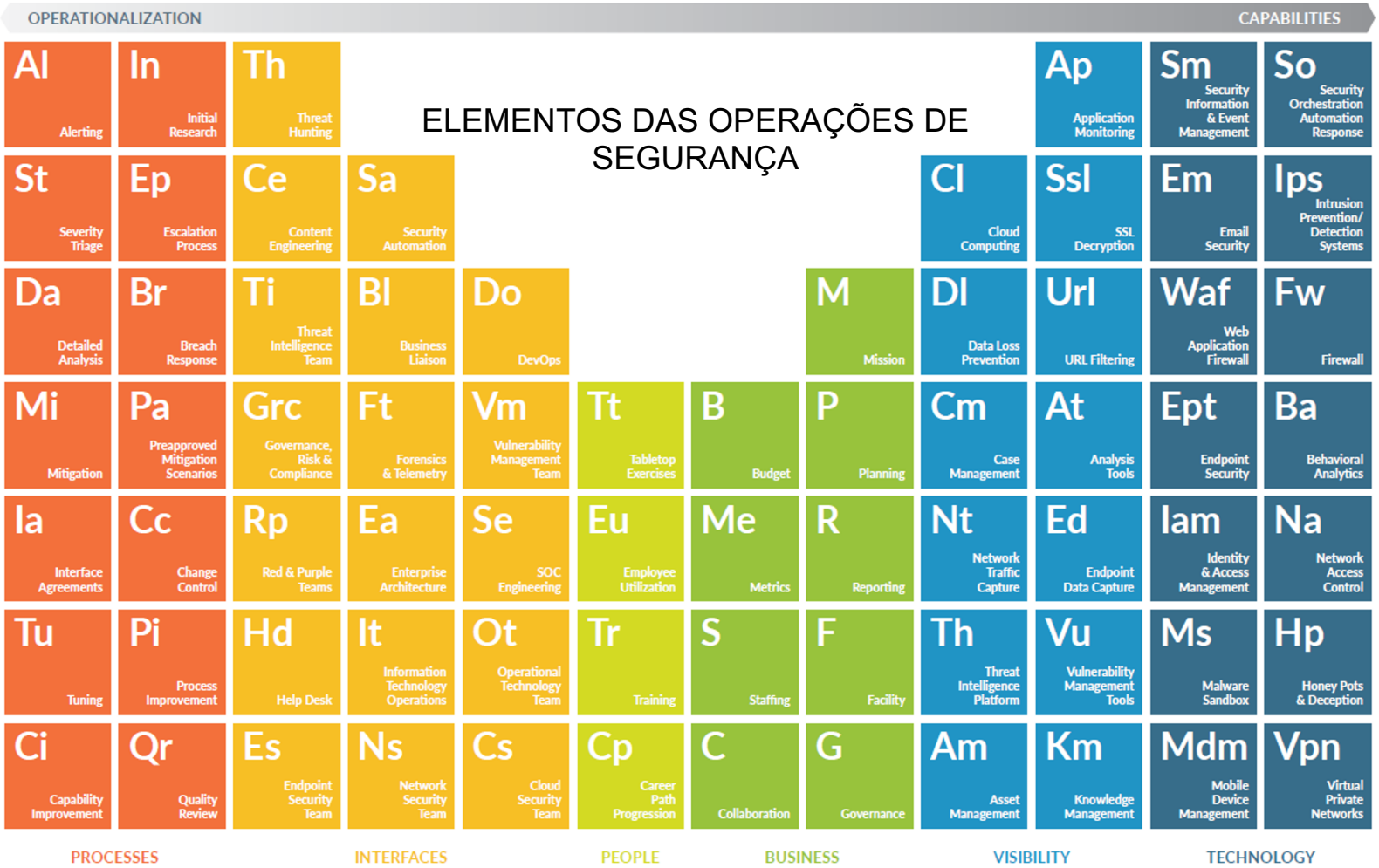
Feedback sobre os controles de prevenção

Desafios de uma operação de segurança

- Processos excessivamente complexos ou insuficientes
- Muitos alertas
  - Falta de conhecimento sobre a capacidade atual
  - Automação mínima de tarefas repetitivas
  - Negligência na melhoria contínua
- Muitas atividades / Priorização
- Métricas in-suficientemente significativas
- Focado em IOCs individuais

Governança aliada às operações de segurança

- Ter uma estrategia comun (Zero Trust)
- Construir políticas, processos e arquitetura baseada em prevenção
- Melhoria contínua
- Automação
  - Identificação
  - Resposta
  - Aprendizado
- Colaboração (Ferramentas e pessoas)
- Acordos operacionais/SLAs com as áreas de interfaces
- Plano modular de respostas a incidentes


OPERATIONALIZATION
CAPABILITIES
ELEMENTOS DAS OPERAÇÕES DE SEGURANÇA
Al Alerting
In Initial Research
Th Threat Hunting
Ap Application Monitoring
Sm Security Information & Event Management
So Security Orchestration Automation Response
St Severity Triage
Ep Escalation Process
Ce Content Engineering
Sa Security Automation
Cl Cloud Computing
Ssl SSL Decryption
Em Email Security
Ips Intrusion Prevention/ Detection Systems
Da Detailed Analysis
Br Breach Response
Ti Threat Intelligence Team
Bl Business Liaison
Do DevOps
M Mission
Dl Data Loss Prevention
Url URL Filtering
Waf Web Application Firewall
Fw Firewall
Mi Mitigation
Pa Preapproved Mitigation Scenarios
Grc Governance, Risk & Compliance
Ft Forensics & Telemetry
Vm Vulnerability Management Team
Tt Tabletop Exercises
B Budget
P Planning
Cm Case Management
At Analysis Tools
Ept Endpoint Security
Ba Behavioral Analytics
Ia Interface Agreements
Cc Change Control
Rp Red & Purple Teams
Ea Enterprise Architecture
Se SOC Engineering
Eu Employee Utilization
Me Metrics
R Reporting
Nt Network Traffic Capture
Ed Endpoint Data Capture
Iam Identity & Access Management
Na Network Access Control
Tu Tuning
Pi Process Improvement
Hd Help Desk
It Information Technology Operations
Ot Operational Technology Team
Tr Training
S Staffing
F Facility
Th Threat Intelligence Platform
Vu Vulnerability Management Tools
Ms Malware Sandbox
Hp Honey Pots & Deception
Ci Capability Improvement
Qr Quality Review
Es Endpoint Security Team
Ns Network Security Team
Cs Cloud Security Team
Cp Career Path Progression
C Collaboration
G Governance
Am Asset Management
Km Knowledge Management
Mdm Mobile Device Management
Vpn Virtual Private Networks
PROCESSES
INTERFACES
PEOPLE
BUSINESS
VISIBILITY
TECHNOLOGY

Business *(goals and outcomes)*

Mission: What are we doing?

Planning: How are we going to do it?

Governance: How are we going to manage what we are doing?

Staffing: Who do we need to do this?

Facility: Where are we going to do this?

Budget: What will it cost to do this?

Metrics: How do we know it is working effectively?

Reporting: How will we track activity and provide updates?

Collaboration: How will we communicate and track issues with the rest of the business?

People *(who will do the work)*

How will we find staff and train them to fulfill their roles?

What will we do to retain them?

How will we manage the workloads of the staff?

How will we validate the actions of the staff for efficacy?

Visibility *(information needed to accomplish goals)*

What primary security data is needed?

What contextual data is needed?

How often does this data need to be refreshed?

What knowledge base information needs to be accessed?

How will the security operations team see activity in the SOC?

How will external teams see activity in the SOC?

Technology *(capabilities needed to provide visibility and enable people)*

What capabilities are required to achieve the necessary visibility?

What technology will be used to provide these capabilities?

Who will be responsible for the licensing, implementation, and maintenance of the technology?

How will technology and content updates be requested and performed?

What updates will be carried out automatically and at what interval?

Processes *(tactical steps needed to execute on goals)*

What processes need to be defined?

Where will the processes and procedures be documented?

How will this documentation be accessed and socialized?

Who will have responsibilities for keeping this documentation updated?

How often will the processes need to be reviewed and updated?

Interfaces *(external functions to help achieve goals)*

What other functions of the business impact security operations?

What other functions of the business does security operations impact?

How will the security operations team work alongside these other functions?

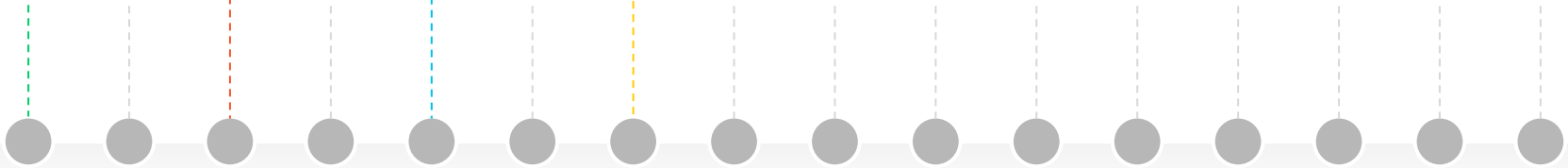
Who has ownership of responsibilities and are there SLAs that need to be documented?

At what interval will these interfaces be reviewed and updated?

Aplicando governança as operações de segurança

Governança

1. **Criar a fundação:** Explorar os elementos de operações de segurança, identificar GAPs e criar um roadmap para atingir os objetivos.
2. **Configurar as melhores práticas e estabelecer processos:** Garantir que a utilização e configuração das melhores práticas estão aplicadas as capacidades. Desenvolver um plano de resposta a Incidente (modular) para crescer a sua segurança.
3. **Integrar capacidades avançadas:** Integrar processos específicos de uma plataforma ao SOC, incluindo automação, EDR (endpoint detection and response), threat intelligence e next generation firewall.
4. **Medir progressos e melhora contínua:** Mensurar as capacidades, reajustar roadmap, melhoria contínua das operações.



Fase 1: Fundação

M

Missão

Missão

Objetivos da organização para operações de segurança e as metas a serem alcançadas para o negócio

Questões

- Por que existirá/existe a equipe SecOps? Ex: Crescente número de fraudes.
- Quais são os objetivos para o negócio ? Ex: Reduzir o risco operacional em 15%
- Quais são as metas ? Ex: Solucionar 80% do número de alertas/incidentes
- Quais são as métricas? Ex: Diminuição de 90% dos alertas comparado ao trimestre anterior

Objetivos

- A missão define nossos objetivos gerais e deve ser compartilhada com a equipe para fornecer uma direção clara
- A missão deve incluir as funções principais do time SecOps
- Governança tem um papel fundamental nestas funções

Itens de ação

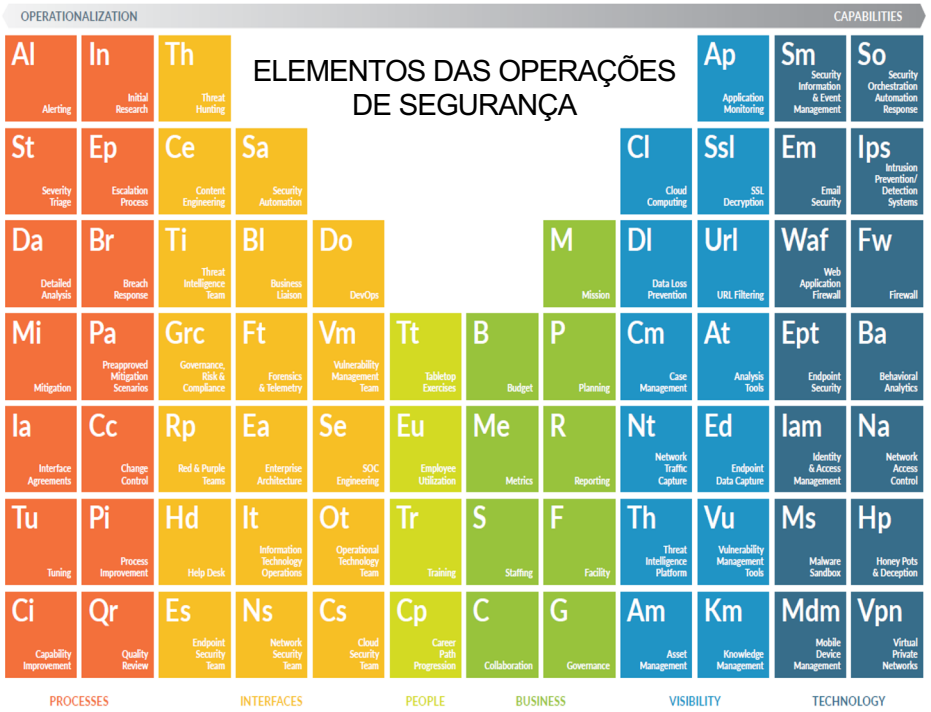
- Definir a missão
- Socializar a missão

Fundamentos

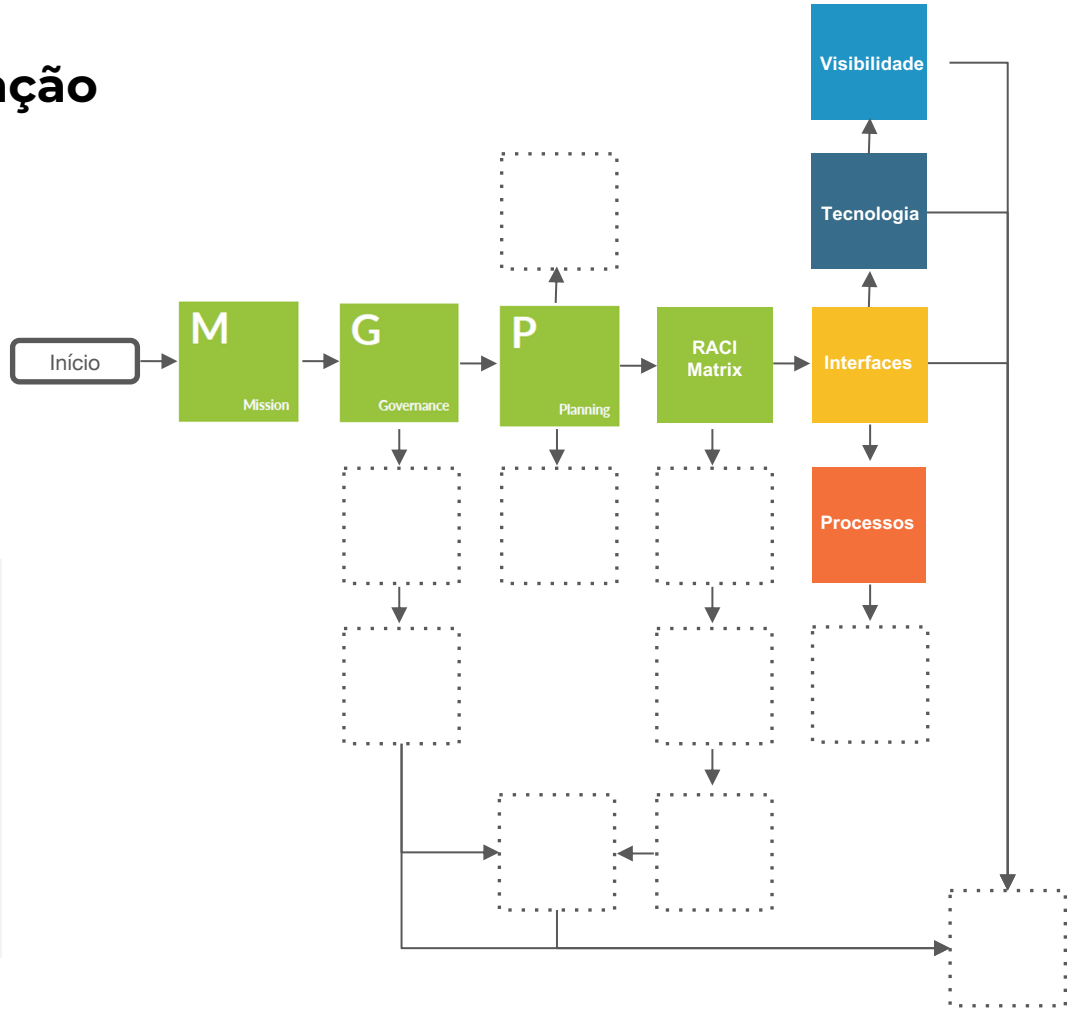
Como funciona

Agnóstico a produtos

- Discutir os elementos da operação de segurança:
  - Definir a necessidade de cada elemento
  - Como os elementos interagem entre si.
- Criar:
  - Definir os requisitos da área de segurança.
  - Criar documento aplicável ao time de segurança.
  - Criar uma matrix RACI para todas as funções que impactam o time de segurança
- Revisar:
  - Requisitos para acordos e SLAs das interfaces.
  - Necessidades de tecnologia de segurança.
  - Arquitetura e infraestrutura do SOC.
- Entregas:
  - Apresentação do planejamento para as áreas de interface
  - Ações para próximos passos, engajamentos



Arquitetura da fundação



Elementos bases

 |

Fase 2: Processos

Definição dos processos

- Criar um plano de resposta a incidentes que incluem:
  - Pesquisa inicial
  - Triagem de severidade
  - Processo de escalação
  - Análise detalhada
  - Processos de mitigação
  - Aumentar prevenção
  - Melhoria em tempo real
  - Revisar qualidade
- Guia:
  - Fluxo de trabalho para a plataforma de segurança
  - Triagem das operações de segurança (5W1H)
  - Caminho e requisitos para escalação
  - Caminhar através de casos de usos específicos
  - Importância do plano de resposta a incidentes

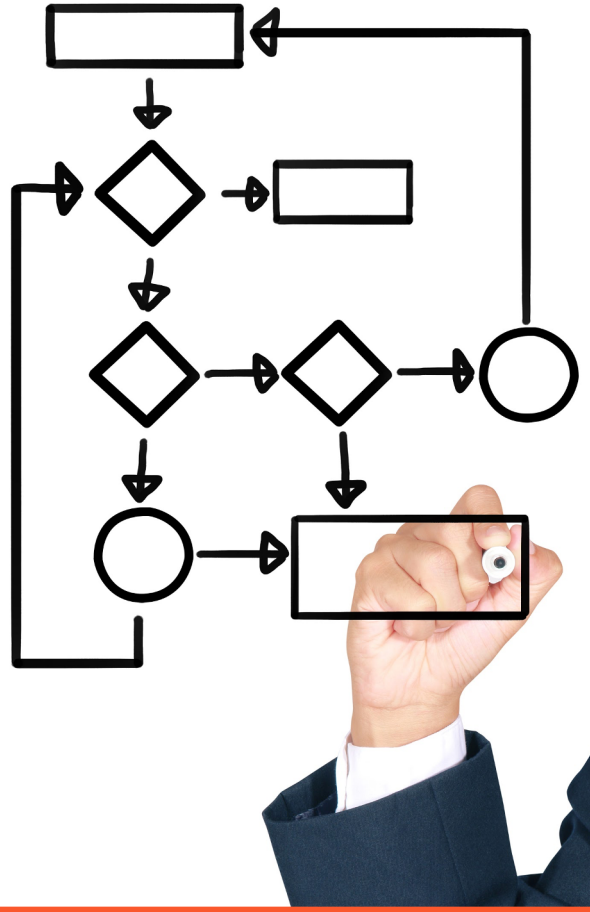
Operações de segurança

1 IDENTIFICAR

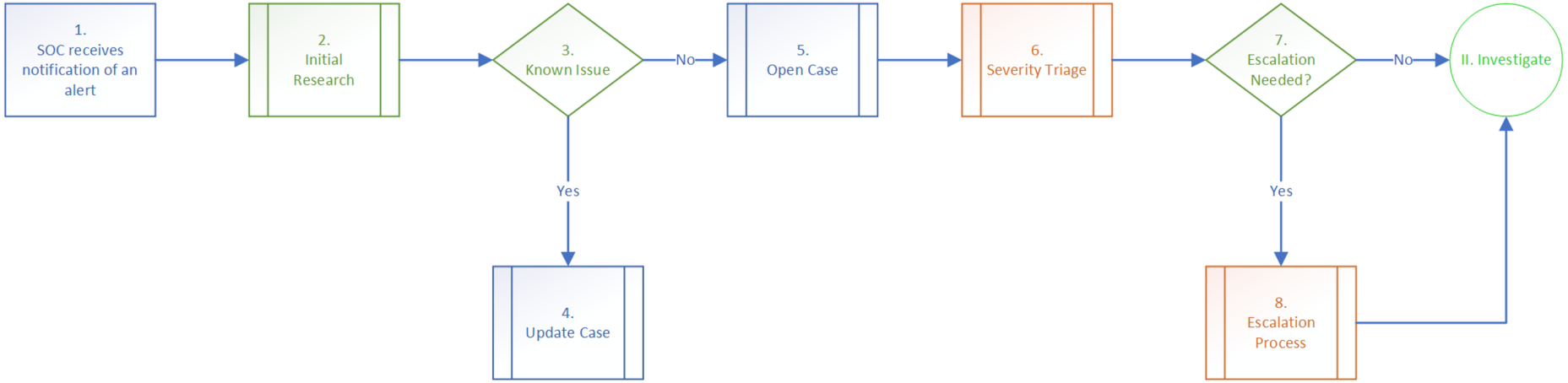
2 INVESTIGAR

3 MITIGAR

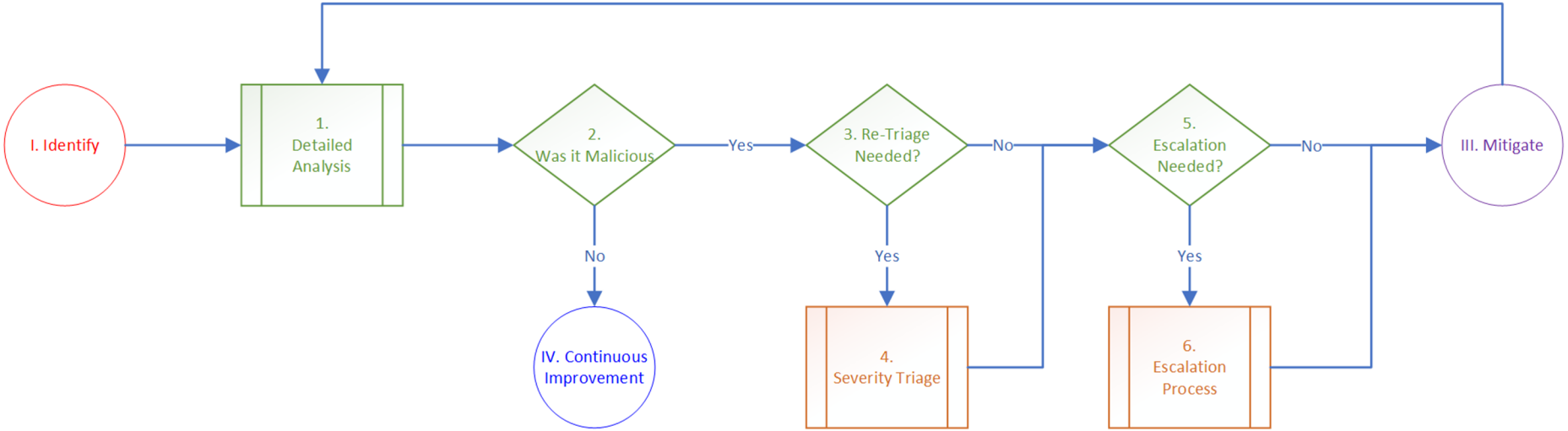
4 MELHORIA CONTÍNUA



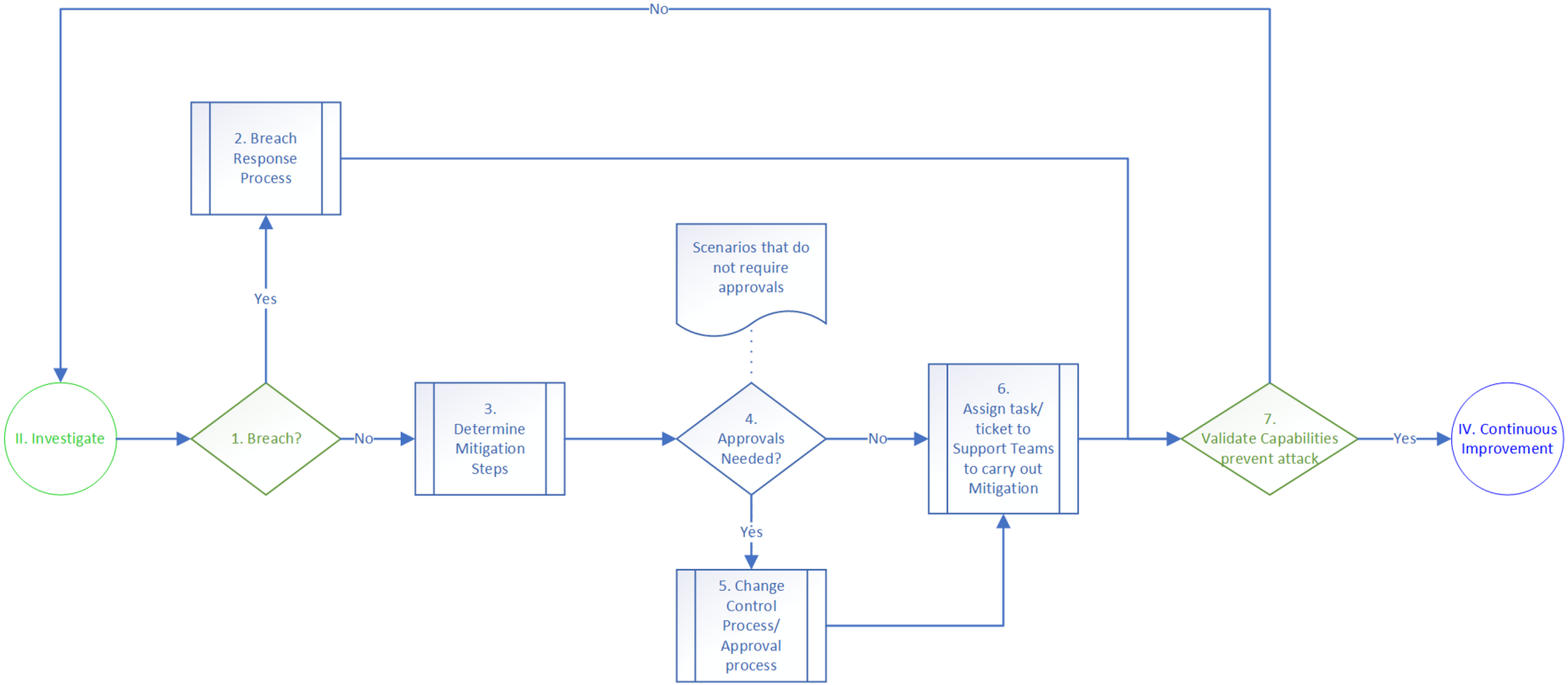
I. IDENTIFICAR



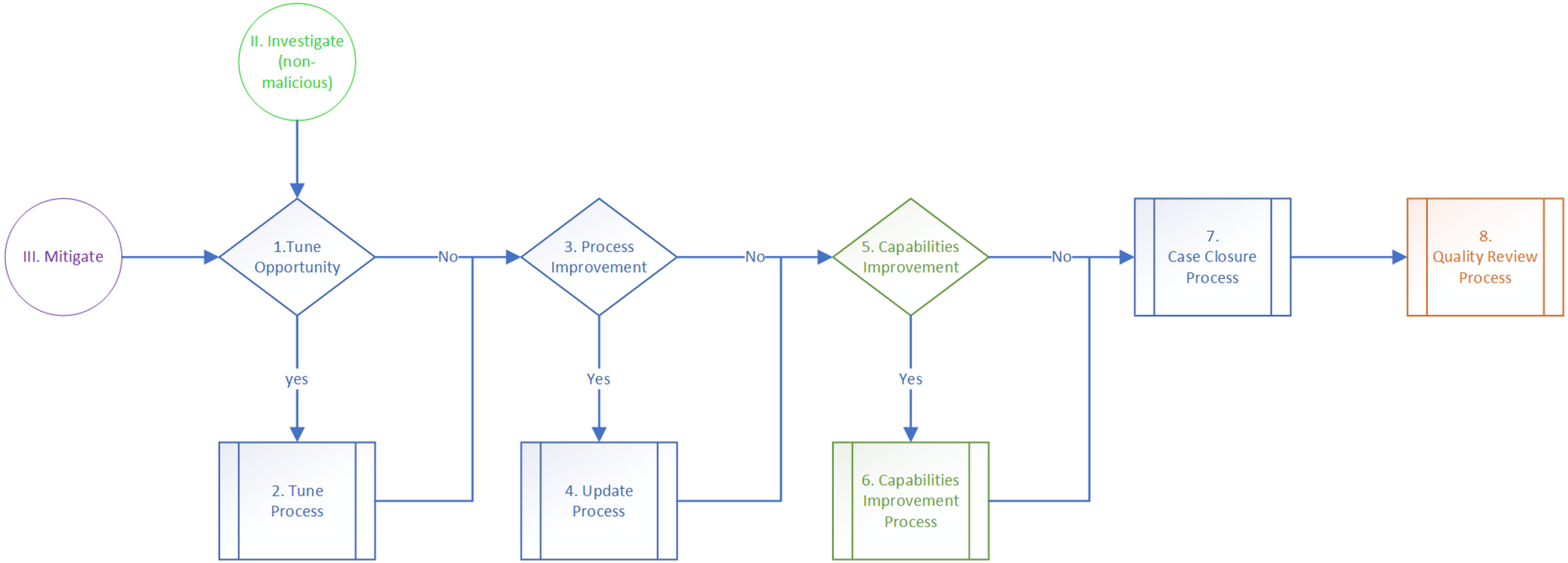
II. INVESTIGAR



III. MITIGAR

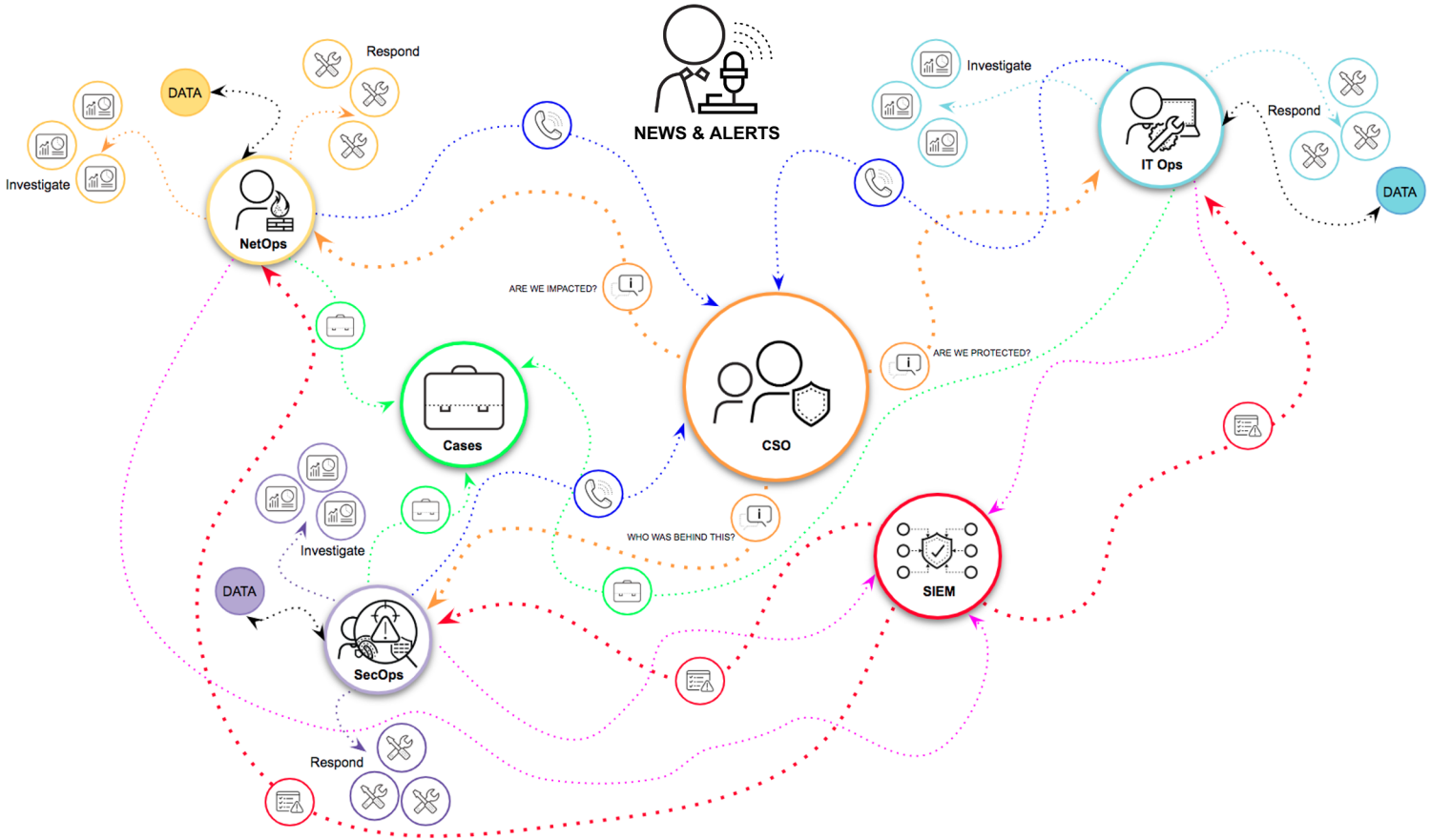

No
2. Breach Response Process
Yes
Scenarios that do not require approvals
II. Investigate
1. Breach?
No
3. Determine Mitigation Steps
4. Approvals Needed?
No
6. Assign task/ ticket to Support Teams to carry out Mitigation
7. Validate Capabilities prevent attack
Yes
IV. Continuous Improvement
Yes
5. Change Control Process/ Approval process

IV. MELHORIA CONTINUA



Fase 3: Integração

Simplificar a complexidade de integração



paloalto NETWORKS

Plataforma para conectar de forma segura qualquer lugar

Consistente

Integrado

Best-in-class

 |

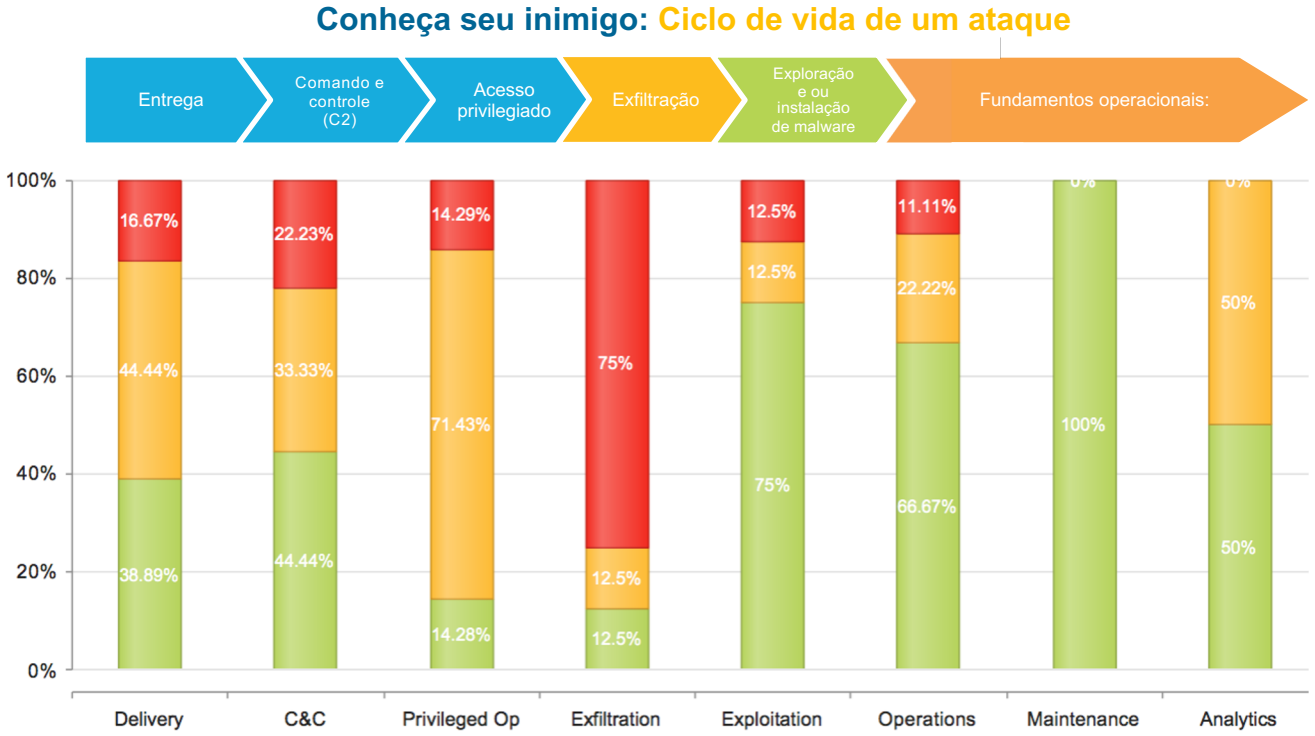
Simplificar a complexidade de integração

Capacidades (examples)	Estado atual	Plataforma
Firewall	Solução vendor A	
IPS	Solução vendor A	
Filtro de conteúdo WEB	Solução vendor B	
Detecção malware desconhecido	Solução vendor A	
Acesso remote a usuários	Solução vendor C	
Proteção de endpoint e detecção e resposta	Solução vendor D	
Proteção de nuvem pública e privada	Solução vendor G	
Acesso web seguro	Solução vendor C	
Automação e orchestração	Solução vendor E	
SD-WAN	Solução vendor F	

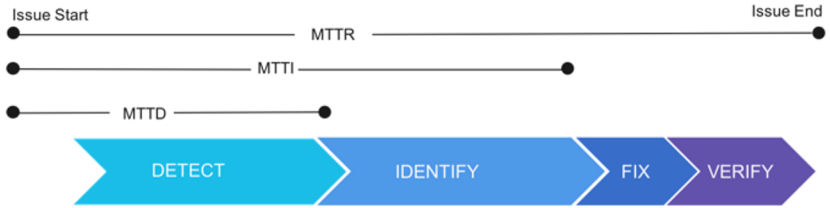
Fase 4: Assessment

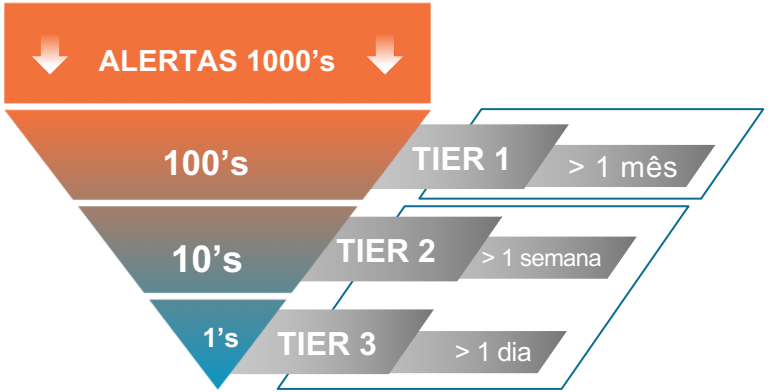
Melhoria contínua

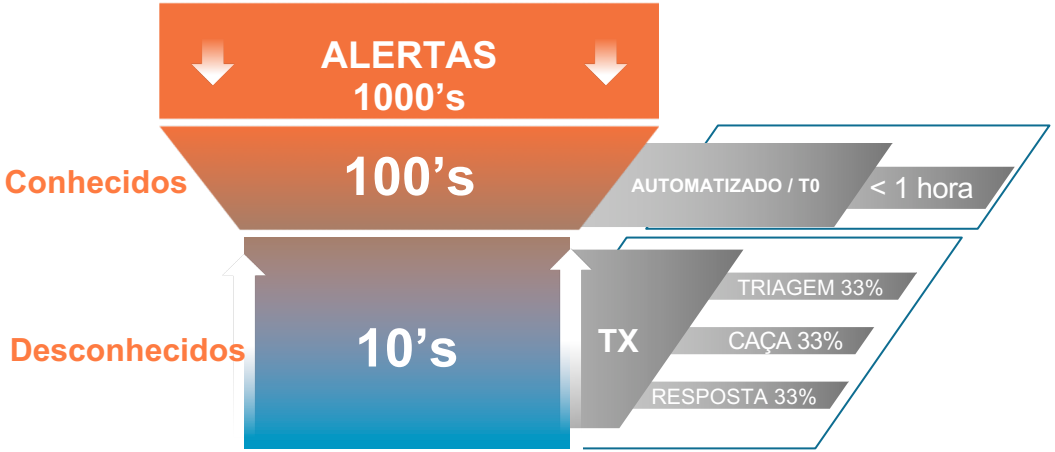
- *Exemplos: Postura de prevenção é forte nos estágios de entrega (delivery) e comando e controle (C2) no ciclo de ataque.*
- *Exemplo: Boa segmentação do perímetro. Sem segmentação interna/datacenter permitindo acesso privilegiado e facilidade de exfiltração de dados.*
- *Exemplo: Sem visibilidade sobre o uso e controle de aplicac'ões SaaS.*
- *Exemplo: Estações em fase de exploração de vulnerabilidade estãos vulneráveis sem prevenção a exploits ou controle de executáveis desconhecidos.*
- *Exemplo: Postura operacional é boa porém melhorias precisam ser feitas em X áreas.*



Medir progressos

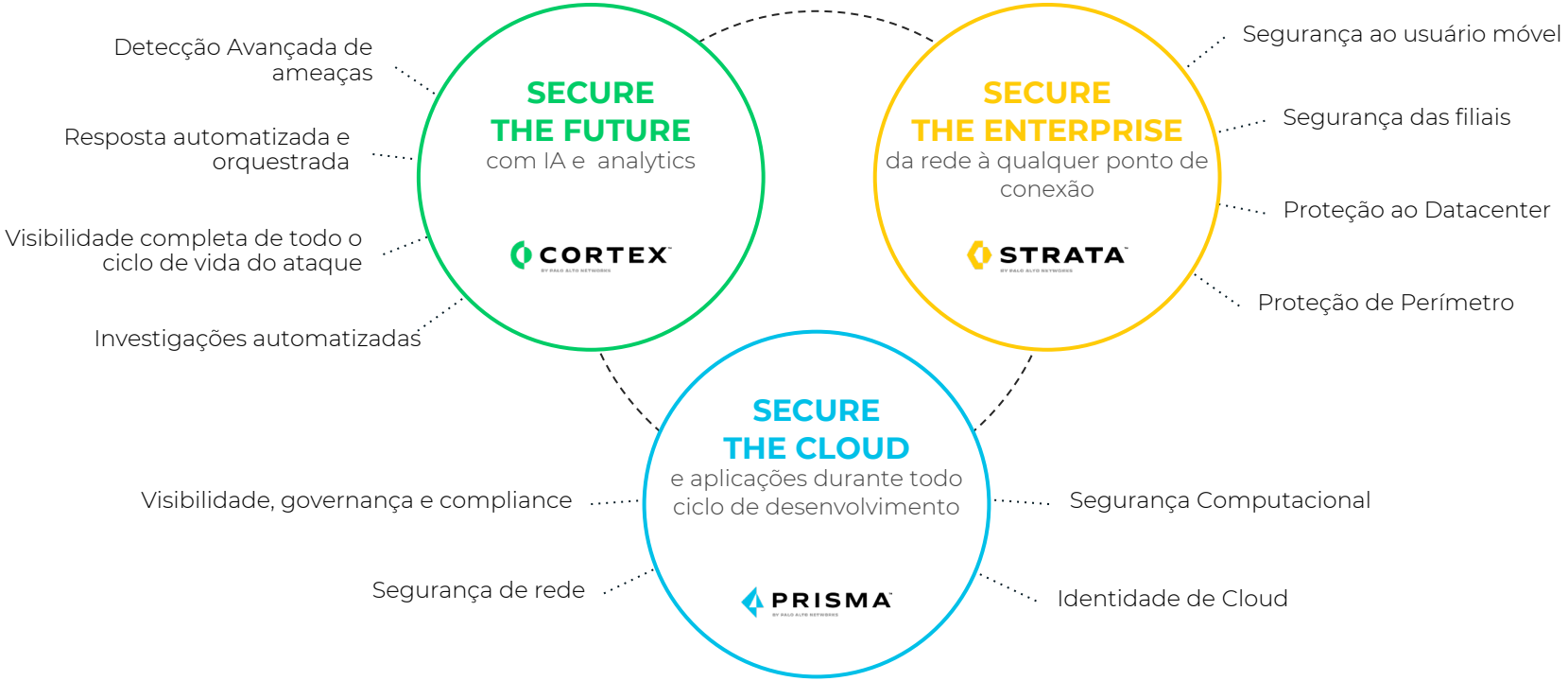




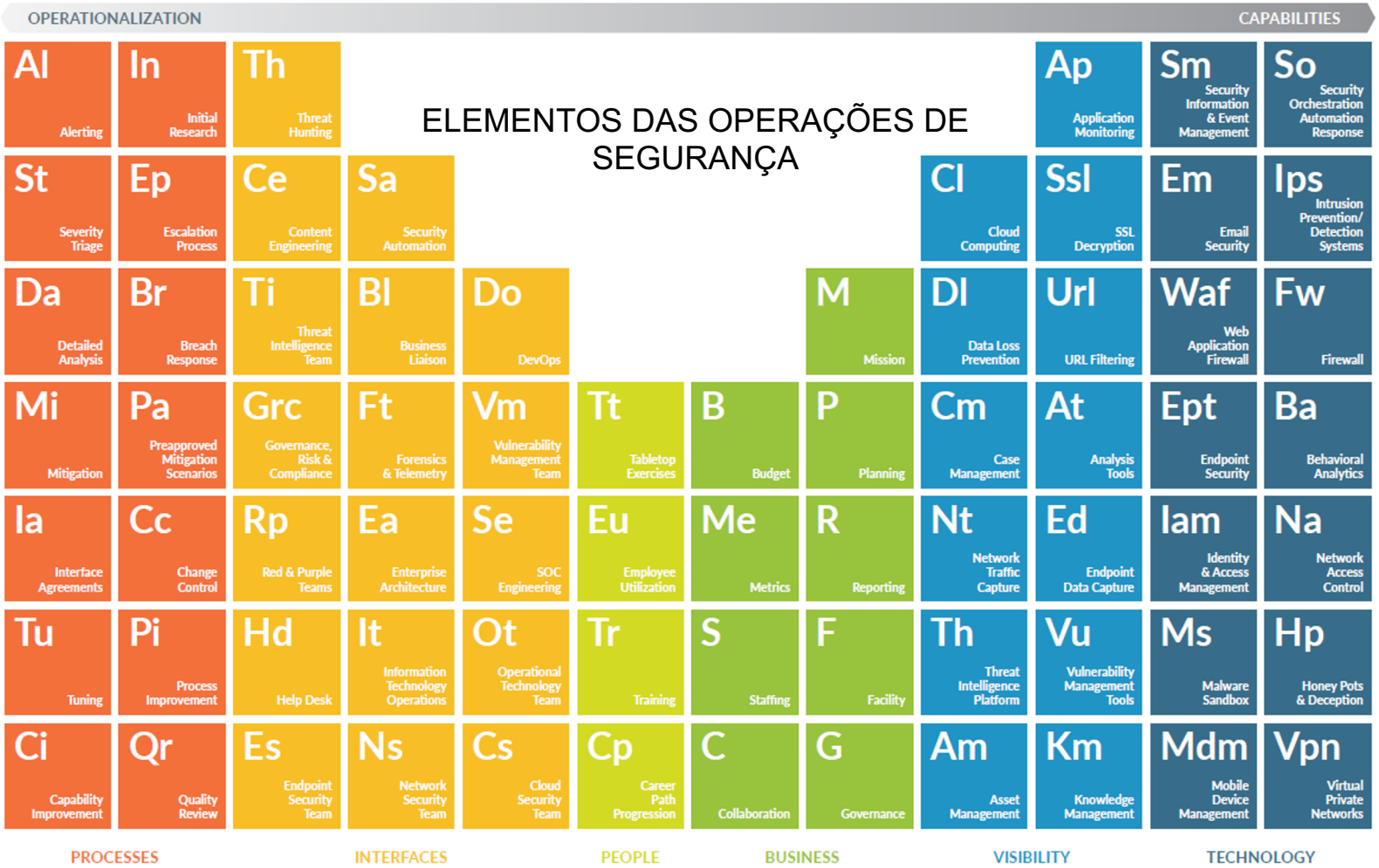


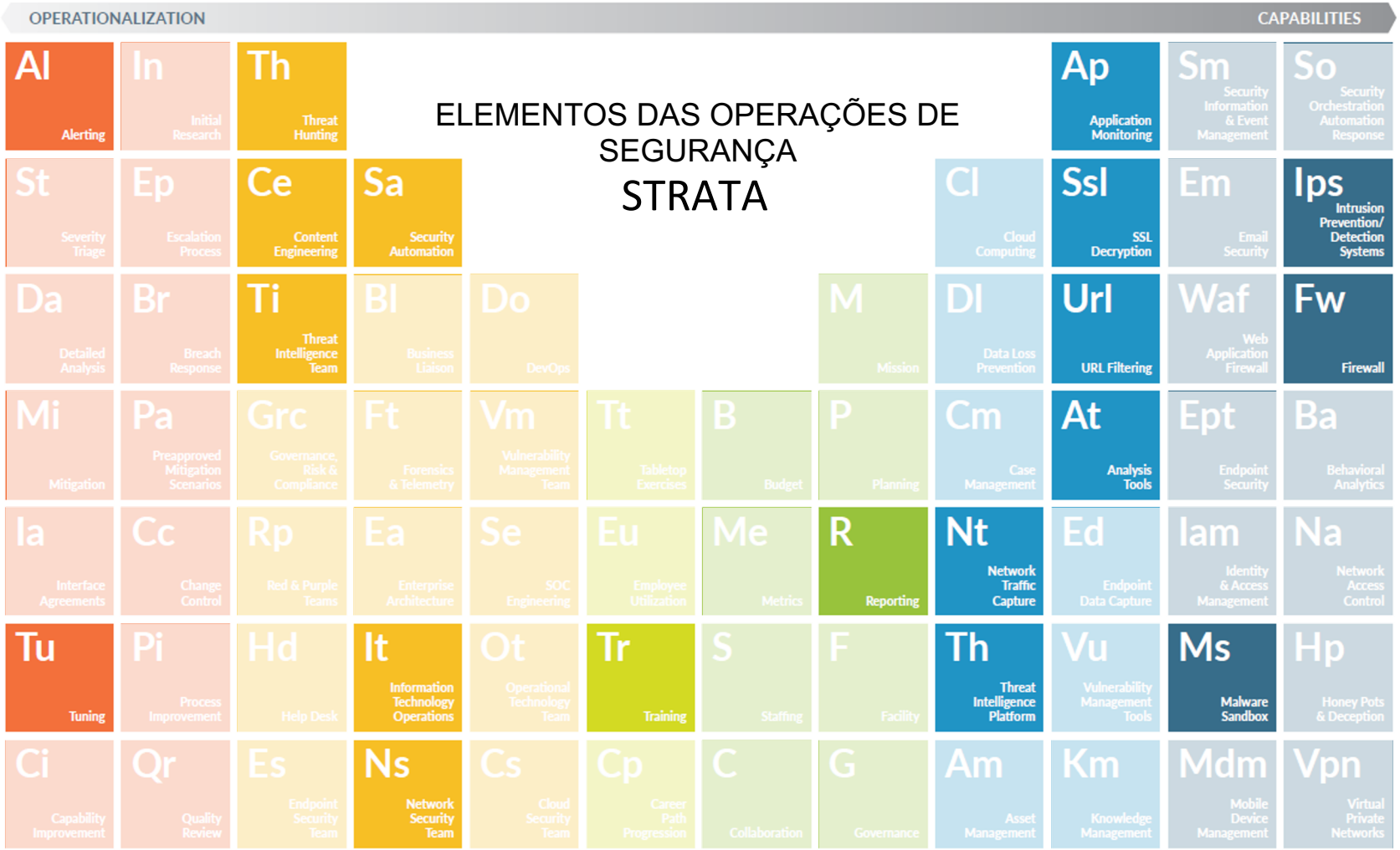
Como podemos ajudar?

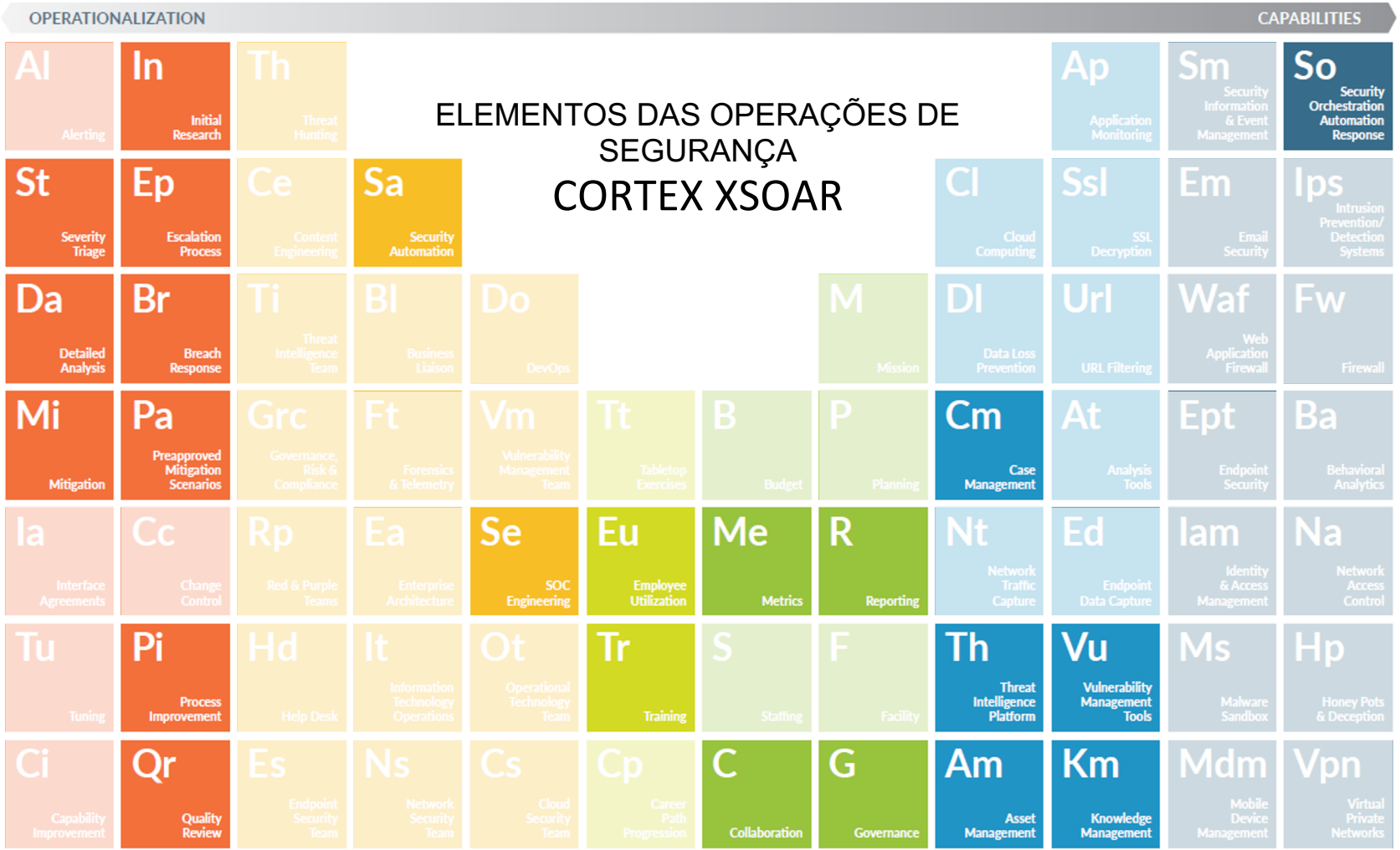
Palo Alto Networks é o Líder mais Abrangente e Integrado de Cybersecurity

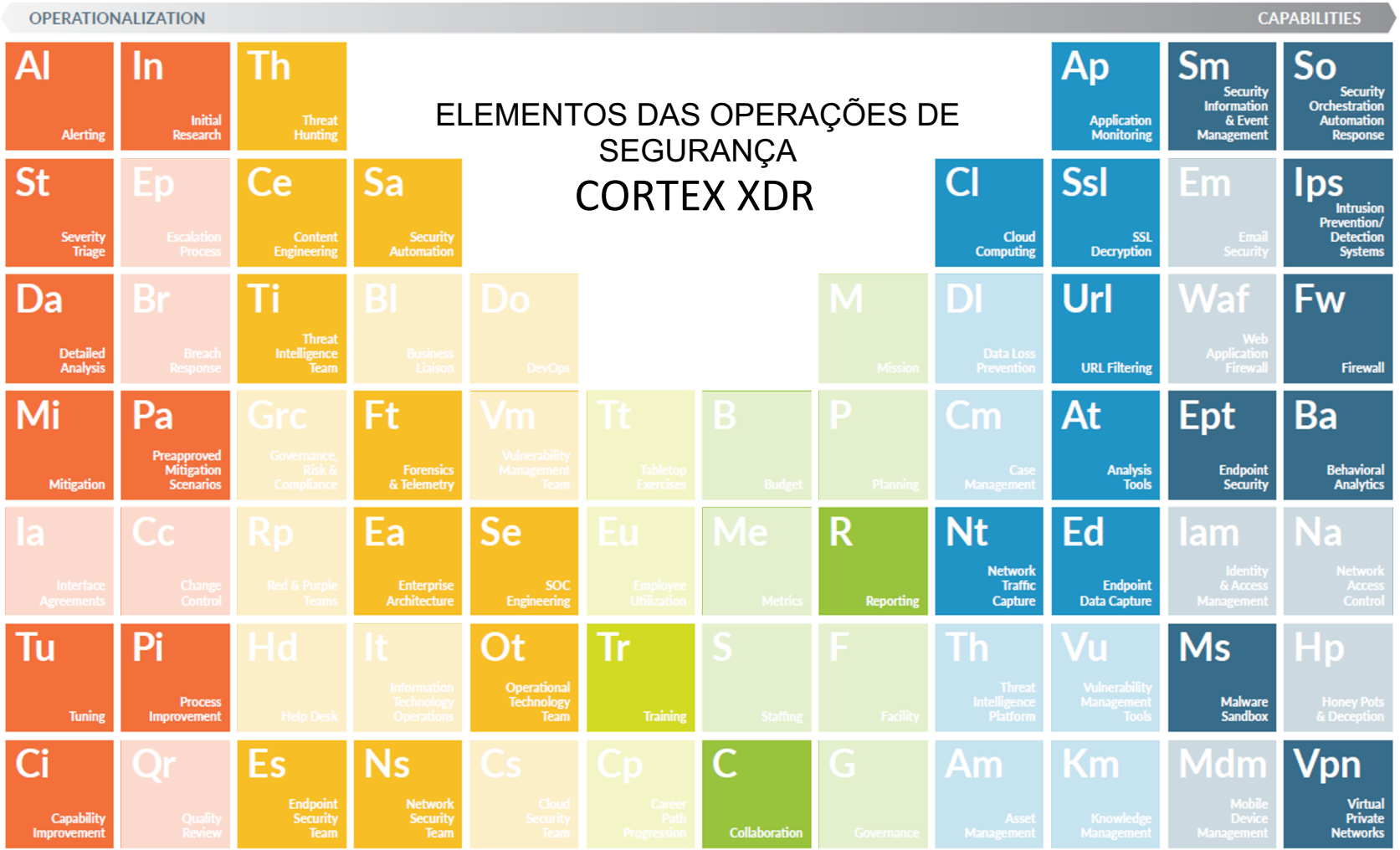


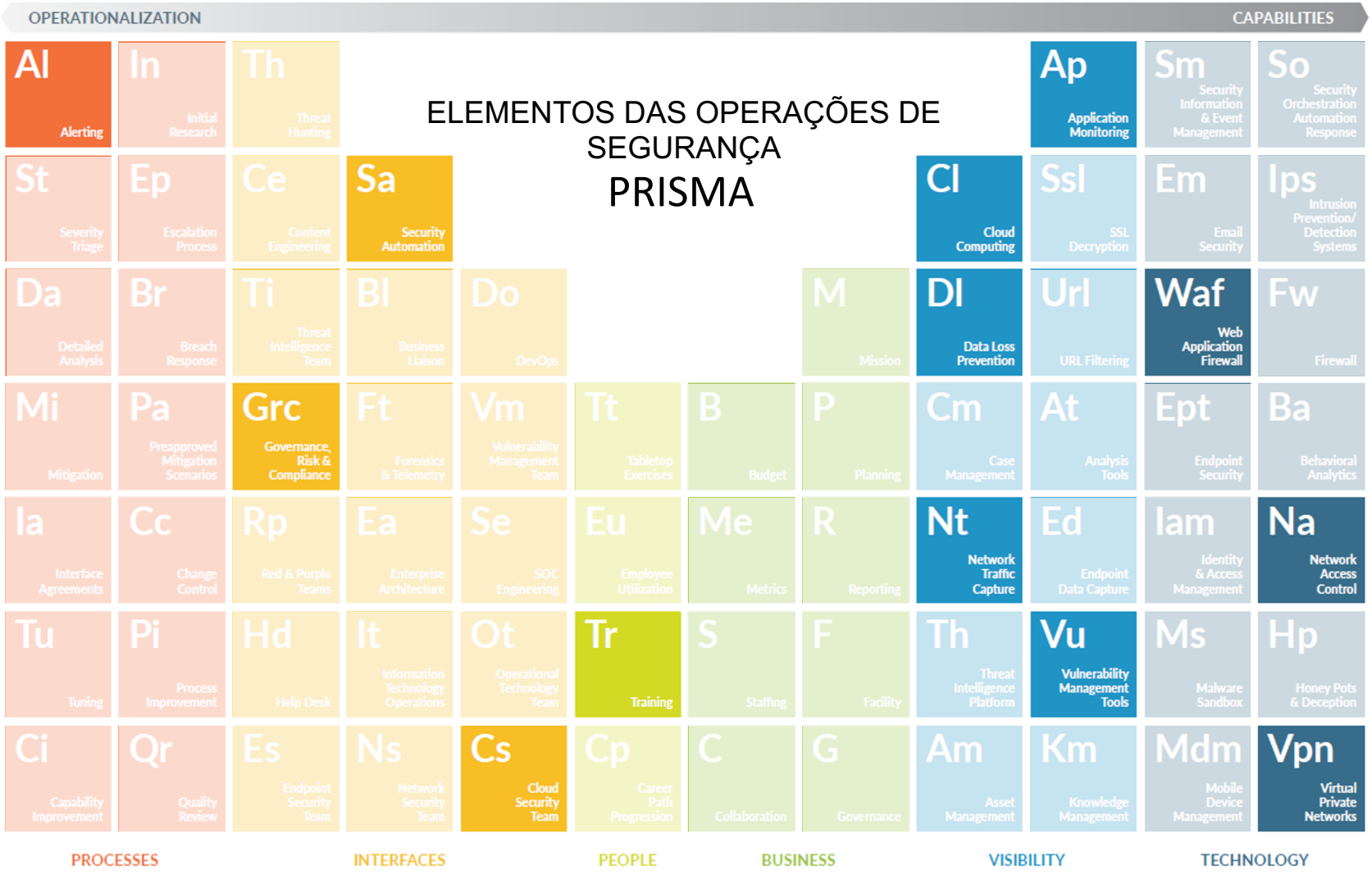
 |

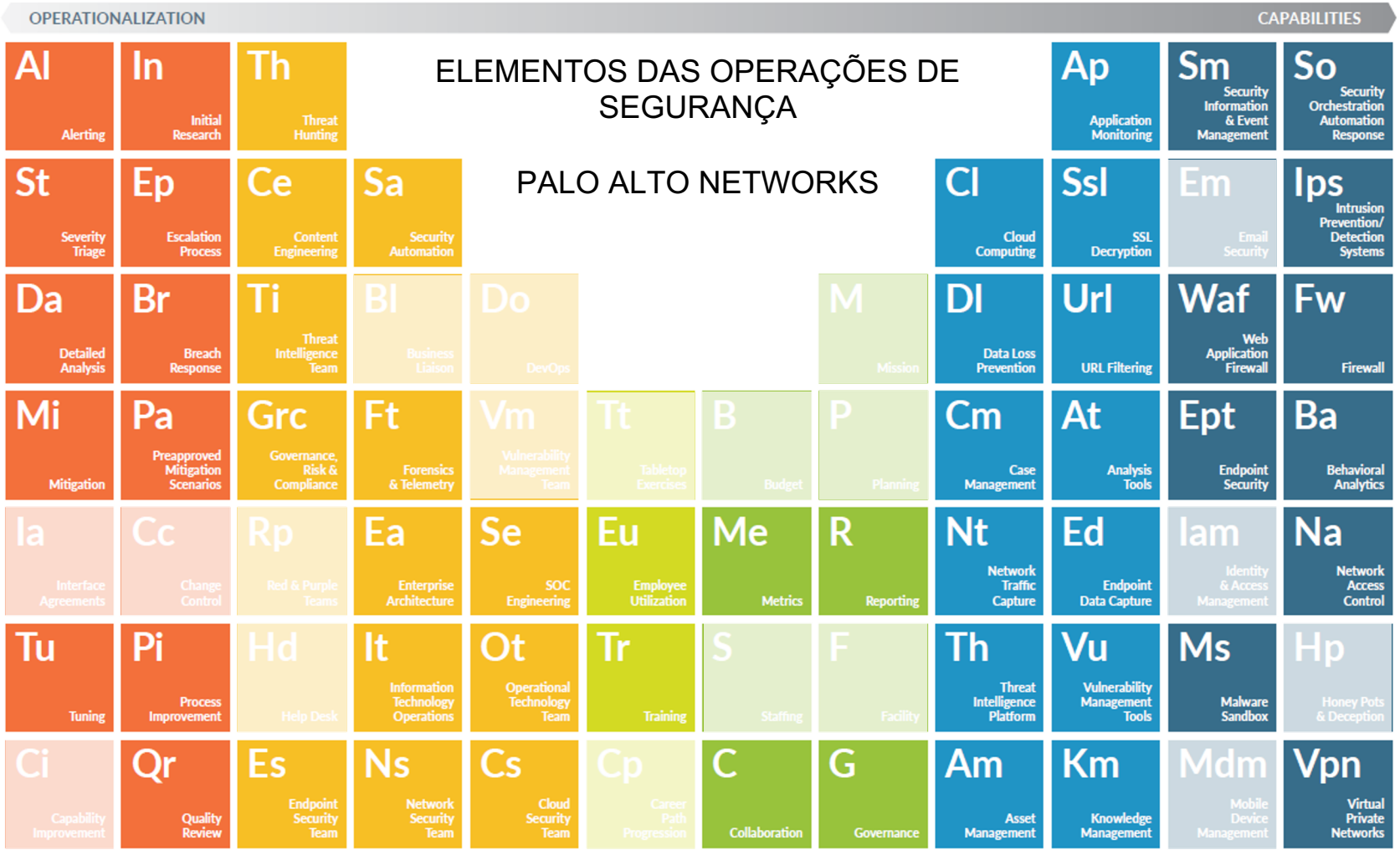

OPERATIONALIZATION
CAPABILITIES
ELEMENTOS DAS OPERAÇÕES DE SEGURANÇA
Al Alerting
In Initial Research
Th Threat Hunting
Ap Application Monitoring
Sm Security Information & Event Management
So Security Orchestration Automation Response
St Severity Triage
Ep Escalation Process
Ce Content Engineering
Sa Security Automation
Cl Cloud Computing
Ssl SSL Decryption
Em Email Security
Ips Intrusion Prevention/ Detection Systems
Da Detailed Analysis
Br Breach Response
Ti Threat Intelligence Team
Bl Business Liaison
Do DevOps
M Mission
Dl Data Loss Prevention
Url URL Filtering
Waf Web Application Firewall
Fw Firewall
Mi Mitigation
Pa Preapproved Mitigation Scenarios
Grc Governance, Risk & Compliance
Ft Forensics & Telemetry
Vm Vulnerability Management Team
Tt Tabletop Exercises
B Budget
P Planning
Cm Case Management
At Analysis Tools
Ept Endpoint Security
Ba Behavioral Analytics
Ia Interface Agreements
Cc Change Control
Rp Red & Purple Teams
Ea Enterprise Architecture
Se SOC Engineering
Eu Employee Utilization
Me Metrics
R Reporting
Nt Network Traffic Capture
Ed Endpoint Data Capture
Iam Identity & Access Management
Na Network Access Control
Tu Tuning
Pi Process Improvement
Hd Help Desk
It Information Technology Operations
Ot Operational Technology Team
Tr Training
S Staffing
F Facility
Th Threat Intelligence Platform
Vu Vulnerability Management Tools
Ms Malware Sandbox
Hp Honey Pots & Deception
Ci Capability Improvement
Qr Quality Review
Es Endpoint Security Team
Ns Network Security Team
Cs Cloud Security Team
Cp Career Path Progression
C Collaboration
G Governance
Am Asset Management
Km Knowledge Management
Mdm Mobile Device Management
Vpn Virtual Private Networks
PROCESSES
INTERFACES
PEOPLE
BUSINESS
VISIBILITY
TECHNOLOGY



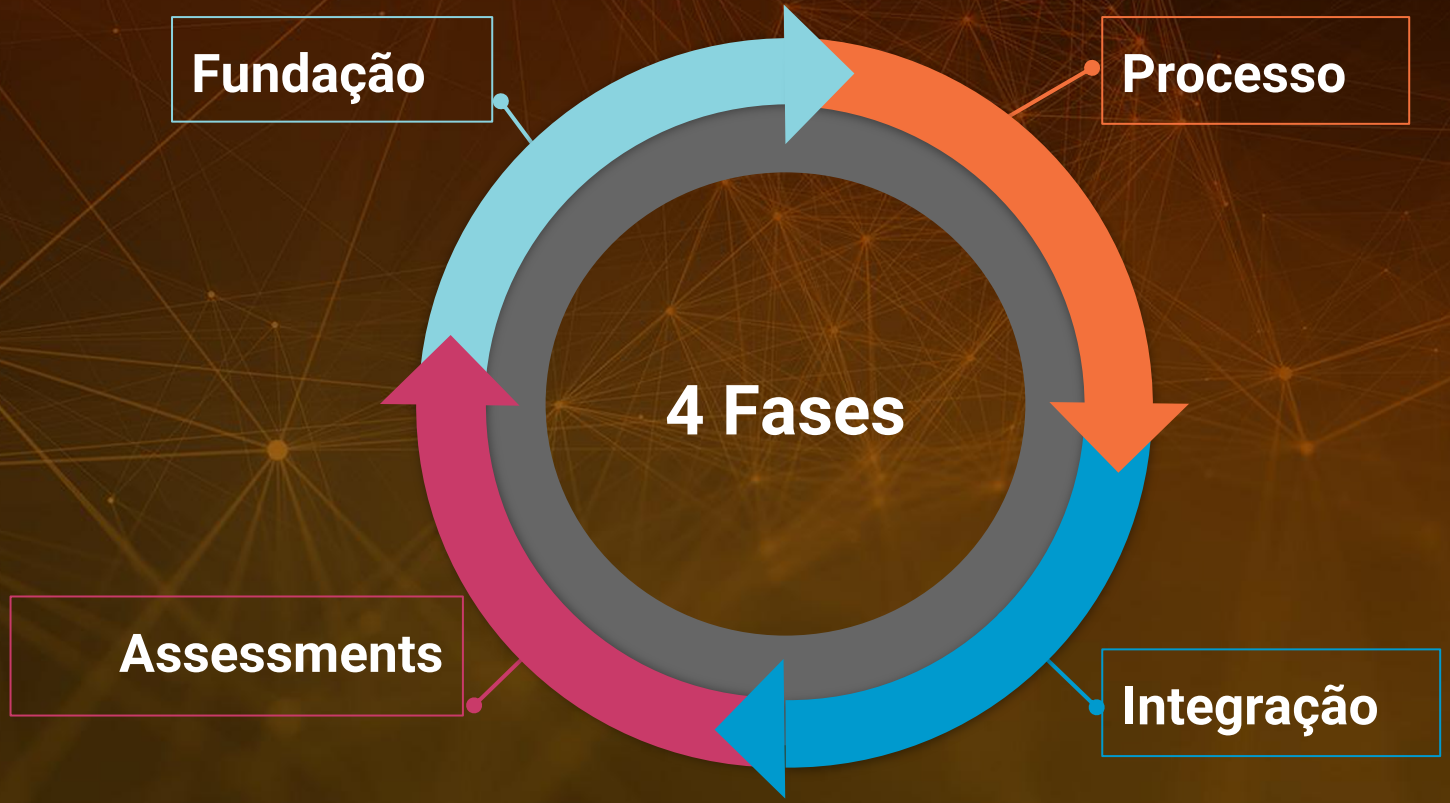








As 4 Fases para aplicar Governança às operações de segurança



Obrigado