SBSeg24 SÃO JOSÉ DOS CAMPOS

24º Simpósio Brasileiro em Segurança da Informação
e de Sistemas Computacionais

MAV

Metodologia de Análise de Ameaças e Vulnerabilidades em um framework integrado multiplataforma

Ariel M. Silva, João Pedro Pereira, Raissa S de Moura e Sérgio Ribeiro

16 - 19 de Setembro de 2024, São José dos Campos, Brasil

Hoje, realizamos **o maior programa de pesquisa e desenvolvimento da América Latina.**

Centro de Pesquisa e Desenvolvimento em Telecomunicações

Em 2023, ocupamos **a primeira posição no ranking** de registro de softwares no Brasil.

449 Processos de patentes nacionais.

213 Processos de patentes internacionais.

+600 clientes

telecom, agronegócio, financeiro, utilities, indústrias, cidades, varejo e serviços de defesa e segurança.

APOIO:

FUNTTEL

FUNDO PARA O DESENVOLVIMENTO TECNOLÓGICO DAS TELECOMUNICAÇÕES

Finep

INOVAÇÃO E PESQUISA

EMPRESA PÚBLICA DO MCTI

TecSEG

Desenvolvimento de tecnologias e metodologia de avaliação e investigação de segurança para redes e aplicações de governo digital.

Redução do risco de vazamento de dados.

Diferentes cenários de aplicação suportados por tecnologias distintas.

Gartner®

Até 2024

80%

das organizações de infraestrutura crítica abandonarão seus provedores de soluções de segurança existentes e isoladas, adotando soluções hiperconvergentes para unir riscos ciberfísicos e de TI.

Principais desafios existentes:

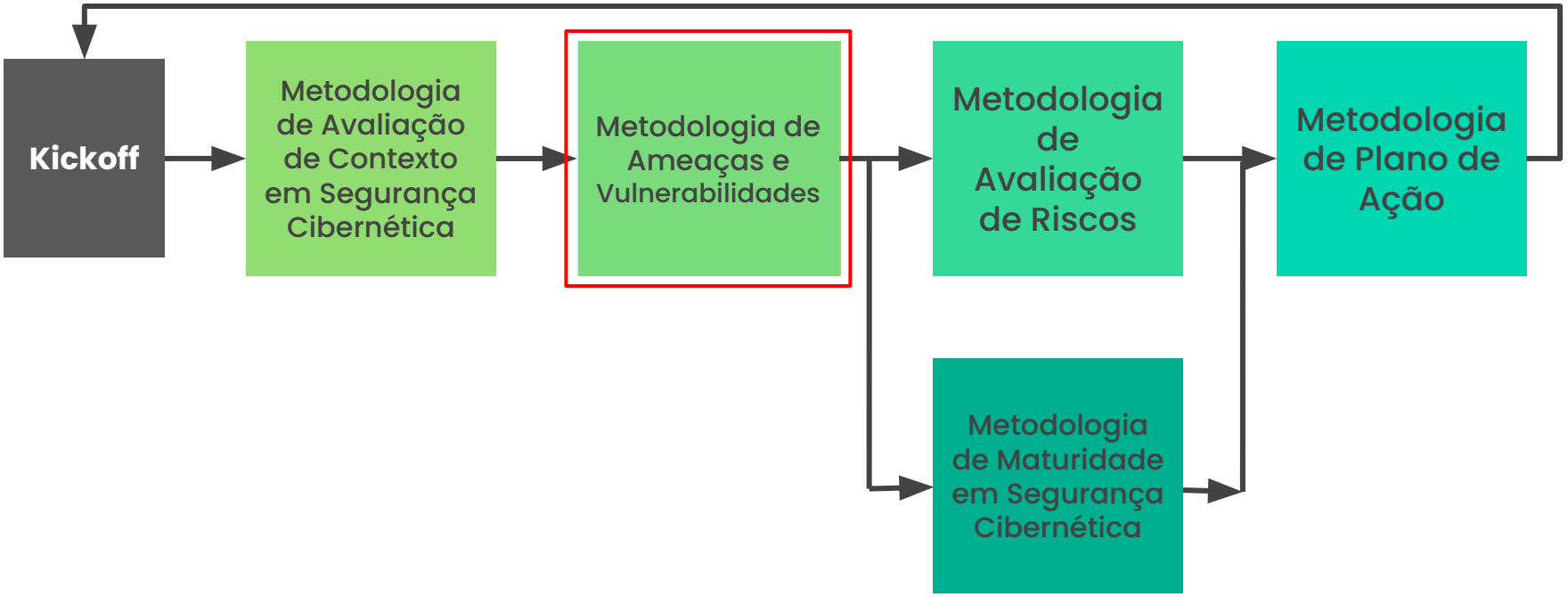
- **Rastreabilidade completa** - Mapeamento de todos os cenários possíveis dentro do fluxo de dados da aplicação.

- **Atualização** - Identificação de novas ameaças a cada versão do sistema.

Threat Assessment & Remediation Analysis (TARA) (2011)

FIASM

Framework Integrado de Avaliação de Segurança em Multiplataforma para Gestão de Segurança ***em Tempo Real***



No FIASM propõe-se a realização de cinco metodologias com objetivos distintos, onde cada metodologia possui diferentes insumos e o resultado, de cada uma, é considerado como insumo para outras, mas também é previsto e possibilitando a liberdade de que insumos externos possam ser utilizados

FIASM

Framework Integrado de Avaliação de Segurança em Multiplataforma para Gestão de Segurança em Tempo Real.

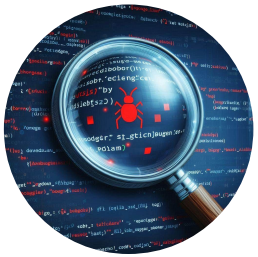
Entradas

Dados do Avaliador

Fontes Externas

Dados de monitoramento

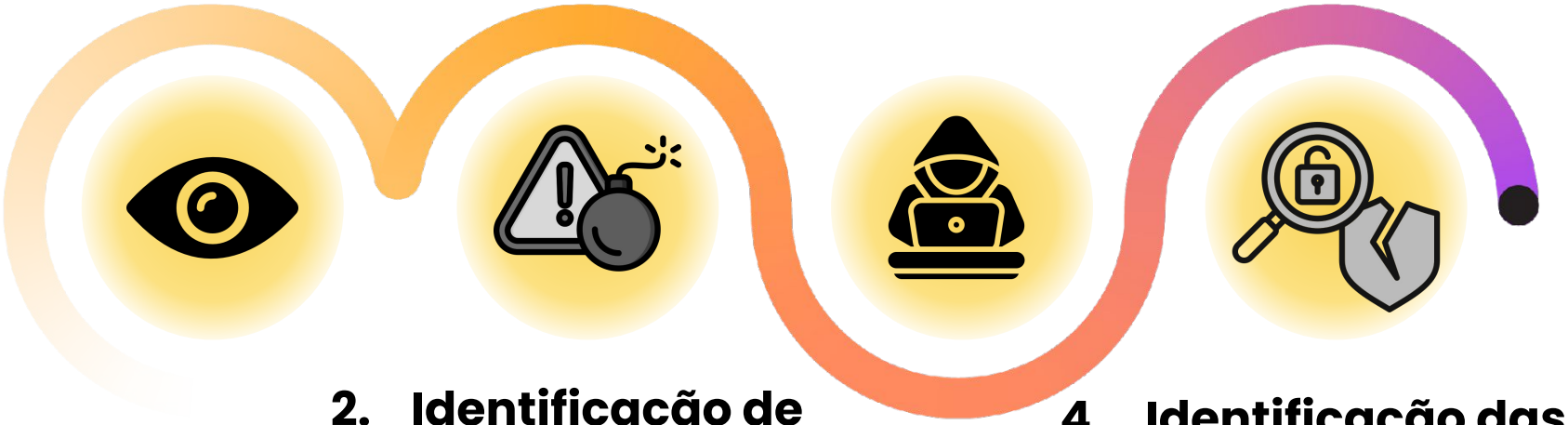
Leis e Normas



Análises de código

1. **Identificação da Condição Final de Ameaça**

3. **Identificação do Agente de Ameaças**

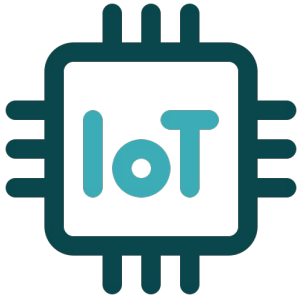


2. **Identificação de Ameaças**

4. **Identificação das Vulnerabilidades**

Fases da **metodologia - MAV**

Caso de **teste**



Onde: Software de gerenciamento, controle e monitoramento de dispositivos IoT.

Objetivos: Proteger a confidencialidade, integridade e a disponibilidade da operação e do processo produtivo.

1. Identificação da Condição Final de Ameaça

Objetivos: Proteger a operação e do processo produtivo.

Entender a necessidade

O que: Dados da operação e funcionamento.

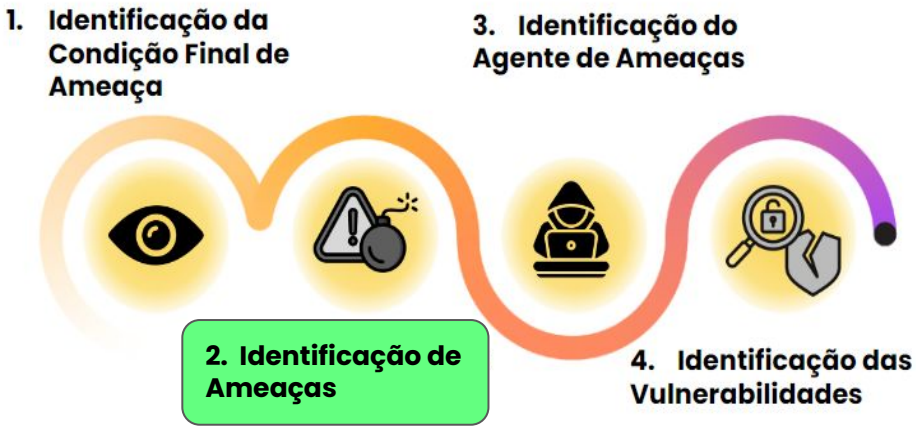
Identificar o que proteger

O que pode acontecer com o que devo proteger

Variável de Contexto

- Exposição de dados
- Processo atrasado
- Processo não executado

Operação	Condição	Variável de Contexto	Condição Final de Ameaça
Enviar Comandos	A operação não é executada	**Processo não executado**	**O comando do ativo origem não chega ao ativo destino**



CF: O comando do ativo origem não chega no ativo de destino					
Ativo	**STRIDE**	**Ameaça**	**Vulnerabilidade**	**Vetor de Ataque**	**Agente de Ameaça**
Ativo origem	T (Adulteração)	Ativo origem é alterado comprometendo seu funcionamento			
	D (Negação de Serviço)	Um agente interrompe o funcionamento do ativo de origem			

Categoria	Motivação	Capacidade	Agente	Descrição
Nações	Interesses Geopolíticos	Muito alta	Allanite	Suposto grupo russo de espionagem cibernética, que tem como alvo principal o setor elétrico nos Estados Unidos e no Reino Unido. Tem sido sugerido que o grupo mantenha uma presença no ICS com o objetivo de obter compreensão dos processos e manter a persistência.
			Dragonfly	Grupo de espionagem cibernética atribuído ao Centro 16 do Serviço Federal de Segurança (FSB) da Rússia. Ativo desde pelo menos 2010, o Dragonfly tem como alvo empresas de defesa e aviação, entidades governamentais, empresas relacionadas a sistemas de controle industrial e setores críticos de infraestrutura em todo o mundo.

CF: O comando do ativo origem não chega no ativo de destino					
Ativo	**STRIDE**	**Ameaça**	**Vulnerabilidade**	**Vetor de Ataque**	**Agente de Ameaça**
Ativo origem	T (Adulteração)	Ativo origem é alterado comprometendo seu funcionamento	Injeção de payload permitindo que invasores executem comandos	Injeção de inúmeros processos no ativo	Grupos Hackers mapeados (Allanite e Drangonfly)
	D (Negação de Serviço)	Um agente interrompe o funcionamento do ativo de origem			

Conclusão

Identificação da condição final de ameaça

Suprir as lacunas de outras metodologias existentes no mercado

Monitoramento em tempo real

Da ideia à realidade. Do planejamento à concretização. Do futuro ao presente. Do simples ao extraordinário. Agora é a hora.

JUNTOS, FAZEMOS ACONTECER!

Muito **Obrigado!**

Ariel Moreira
ariels@cpqd.com.br

João Pedro Pereira
joaolc@cpqd.com.br

Raissa S. de Moura
raissak@cpqd.com.br

Sérgio Ribeiro
sribeiro@cpqd.com.br

/in/ariel-moreira

SBSeg2024
16 - 19 de Setembro de 2024,
São José dos Campos, Brasil

www.cpqd.com.br