Construindo Inteligência de Ameaças Cibernéticas

Pessoas, Processos e Maturidade em um Time de CTI

14º Fórum Brasileiro de CSIRTs

Agenda

Marlon Fabro

- Analista de Inteligência - Globo

ESPECIALIZAÇÃO

- Cyber Threat Intelligence (CTI)
- Análise de Malware
- Resposta a Incidentes (DFIR)

DIA A DIA

- Investigação de ameaças e threat hunting
- Análise de ameaças - malwares/phishings
- Mapeamento de TTPs - MITRE ATT&CK
- Engenharia de Detecção
- Produção de inteligência acionável

CERTIFICAÇÕES E FORMAÇÃO TÉCNICA

- SANS FOR610 - Reverse-Engineering Malware
- SANS FOR500 - Windows Forensic Analysis
- EC-Council CTIA
- Mandiant - Malware Analysis, Caça a APTs, OSINT & Threat Intelligence
- Kaspersky - Caça a APTs / YARA
- Magnet AXIOM AX200 - Forensics
- CompTIA Security+

Dados, Informação e Inteligência

DADOS

IPs · Hashes · URLs · Domínios

Fatos discretos sem análise. Feeds de IOCs brutos. Não informam ação isoladamente.

INFORMAÇÃO

Relatórios de vendors · Logs correlacionados

Múltiplos dados combinados que respondem perguntas específicas. Ainda não é acionável.

INTELIGÊNCIA

Análise contextual · Atribuição · COAs

Insight factual que correlaciona dados, descobre padrões e habilita decisões concretas para audiência específica.

"A inteligência deve apontar para decisões ou ações específicas e ser adaptada para facilitar o uso por uma pessoa ou sistema específico." - Intelligence Handbook

Definição e Escopo da CTI

É UMA DISCIPLINA FOCADA EM COMPREENDER AS CAPACIDADES, INTENÇÕES, MOTIVAÇÕES E OPORTUNIDADES DE ADVERSÁRIOS CIBERNÉTICOS RELEVANTES E SUAS TTPS. SEUS INSIGHTS E RECOMENDAÇÕES ARMAM OS STAKEHOLDERS ENCARREGADOS DE PROTEGER A ORGANIZAÇÃO E REDUZIR RISCOS A TECNOLOGIAS, INFRAESTRUTURA E ÀS PESSOAS QUE DEPENDEM DELAS.

- CTI-CMM v1.3

CTI é os "olhos e ouvidos" de uma estratégia de defesa proativa.

OSINT	SOCMINT	HUMINT	TECHINT	FININT
Open Source Intelligence	Social Media Intelligence	Human Intelligence	Technical Intelligence	Financial Intelligence

Cobertura contínua em níveis Estratégico, Operacional e Tático

Preparando os talentos de hoje para as ameaças de amanhã

INTELLIGENCE AND NATIONAL SECURITY ALLIANCE - CYBER INTELLIGENCE TASK FORCE 2015

- Trilhas de formação para analistas de CTI eram inconsistentes ou simplesmente inexistentes.
- Programas de cybersecurity proliferavam, mas quase nenhum ensinava inteligência de forma sistemática.
- Não havia corpo de conhecimento comum, trilhas de carreira claras nem padrão de certificação para a área.
- A força de trabalho era formada por "cross-training" informal entre técnicos e analistas, sem estrutura deliberada.
- CTI era tratada como componente de cybersecurity, não como disciplina própria com competências definidas.

TLP:CLEAR

Os 4 Pilares do Analista de CTI

01

Problem Solving

- Pensamento Crítico - linguagem probabilística, hipóteses concorrentes
- Pesquisa e Análise - coleta estruturada, pivot em datasets
- Pensamento Investigativo - padrões, fingerprints humanos em TTPs

02

Professional Effectiveness

- Comunicação - BLUF, sumário executivo, relatórios por audiência
- Trabalho em Equipe e Inteligencia Emocional - diversidade, mentoria, engajamento de stakeholders
- Visão de Negócios - ROI, risco de negócio, alinhamento organizacional

03

Technical Literacy

- Tecnologia Corporativa - AD, IAM, cloud híbrido, infra virtualizada
- Ecosistema Cibernético - NIST CSF, 800-53, higiene cibernética
- Roles & Responsibilities - RACI, SLAs, interplay entre times

04

Cyber Threat Proficiency

- Drivers Ofensivos - nação-estado, eCrime, hacktivismo, motivações
- Conceitos de Ameaças - Kill Chain, Diamond Model, MITRE ATT&CK
- Malwares & TTPs - execução, C2, evasão, atribuição, infra de adversários

TLP:CLEAR

Quem se Beneficia do CTI?

SecOps / IR

Triagem de alertas, redução de falsos positivos, contexto para resposta mais rápida

Vulnerability Mgmt

Priorização por exploitabilidade real, não apenas CVSS score

Red & Purple Team

TTPs realistas para emular adversários relevantes ao ambiente

Brand Protection

Monitoramento de dark web, typosquatting, impersonação e vazamentos

Third-Party Risk

Postura de segurança de fornecedores, cadeia de suprimentos e parceiros

Risco Geopolítico

Alertas sobre ameaças físicas e cibernéticas por região e país

Liderança Executiva

Priorização de investimento, contexto de risco de negócio, ROI

Threat Analysts

Motivações, TTPs e tendências de atores e conhecimento mais profundo

"CTI não é apenas pesquisa, atua como uma função transversal na organização"

O Universo de Papéis em CTI

↑ Estratégico

- Strategic Threat Analyst
- Threat Analyst
- Threat Context Analyst

↔ Operacional

- Threat Researcher
- Technical Threat Analyst
- Intrusion Analyst

⚙ Técnico/Eng.

- Intelligence Engineer
- Detection Engineer
- Hunt Analyst

⬡ Especialistas

- Vulnerability Intel Analyst
- eCrime Analyst
- Cyber Espionage Analyst

"Analistas 'unicórnio' existem, mas são raros. A ausência de nomenclaturas padronizadas para os cargos gera confusão." – Doyle, J.

Comparativo de Perfis

STRATEGIC / THREAT ANALYST

Executivos · Risk Mgmt · CISO

- Adapta comunicação para audiência sênior
- Visão sistêmica de ameaças, tendências e tech
- Correlaciona objetivos geopolíticos
- Identifica sinais de mudança (indicators & warnings)
- Alinha motivações com mandatos de int. de estados

Threat Landscape Report · Strategic Briefing · Risk Assessment

TECHNICAL / THREAT RESEARCHER

SOC · NOC · IR · Forensics · Red Team

- Extrai IOCs de relatórios de malware e IR
- Desenvolve IOCs de alta fidelidade
- Constrói detecções: YARA, Sigma, Snort, Suricata
- Faz pivot em datasets comerciais para padrões
- Entende TTPs e fingerprints humanos de adversários

IOC Feed · YARA Rules · Adversary Playbook · Hunt Package

INTELLIGENCE ENGINEER

Toda a equipe de CTI · Ferramentas e plataformas

- Automatiza coleta e processamento de inteligência
- Mantém plataformas: MISP, OpenCTI, TheHive
- Cuida de pipelines STIX/TAXII/JSON
- Avalia e cura threat feeds externos
- Integra CTI com SIEM, SOAR e EDR

Automation Pipelines · Feed Management · Platform Ops

Alocação de Pessoas por Tamanho do Time

TIME PEQUENO

1-3 pessoas

Generalistas com prioridades claras

- 1× Analista generalista (Strategic + Tactical)
- Foco: stakeholders críticos primeiro (IR, SOC)
- Ferramentas simples: MISP + feeds curados

TIME MÉDIO

5-8 pessoas

Especialização emergente

- 1× Strategic Analyst
- 2-3× Threat/Technical Analysts
- 1× Intel Engineer (pode ser part-time)
- Divisão por audiência (Tático vs. Estratégico)

TIME MADURO

10+ pessoas

Funções dedicadas por domínio

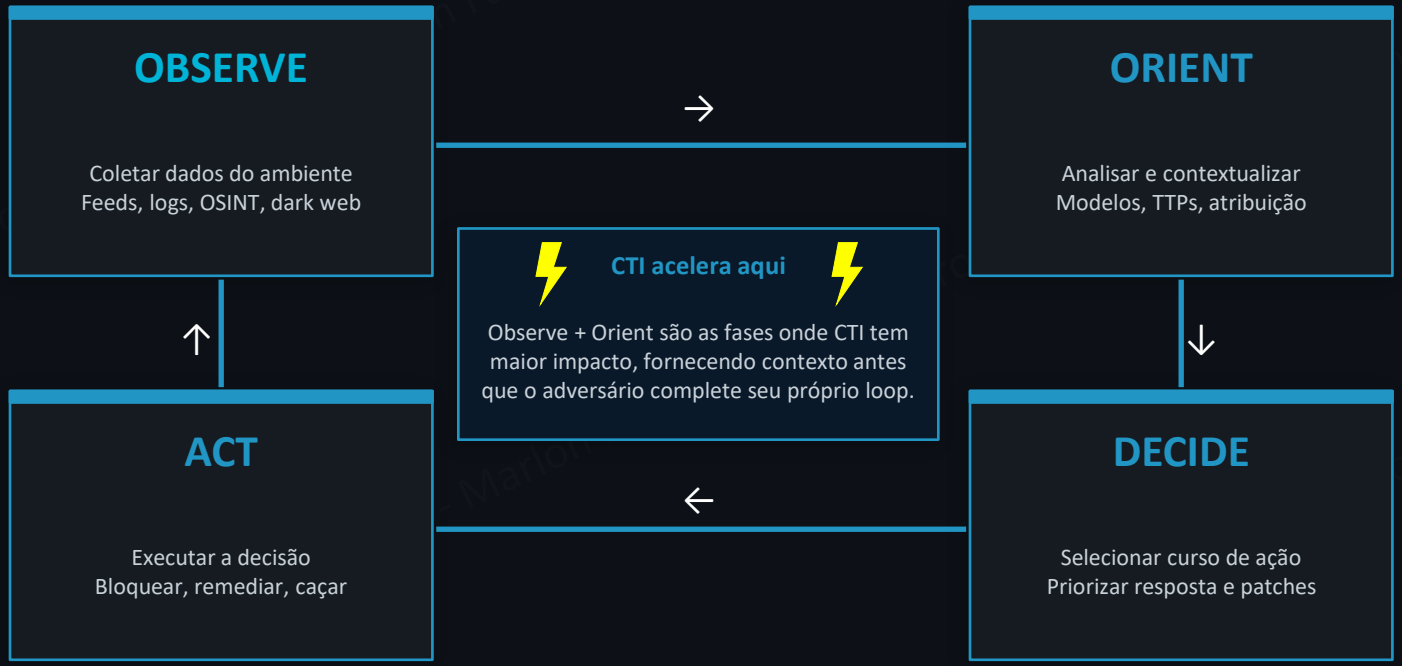
- Strategic Intel Function (1-2)
- Fusion/Operational Function (2-4)
- Tactical Intel Function (2-3)
- DevOps / Intel Engineering (1-2)
- Threat Researcher dedicado (1-2)

TLP:CLEAR

“Existem expectativas não ditas de ambos os lados. Sessões de 'dia a dia no trabalho' e encontros informais de alinhamento são ferramentas valiosas para esse alinhamento." - J. Doyle

OODA Loop e o Papel da CTI

Defensores e atacantes operam em velocidades variadas. A inteligência acelera o ciclo OODA do defensor.



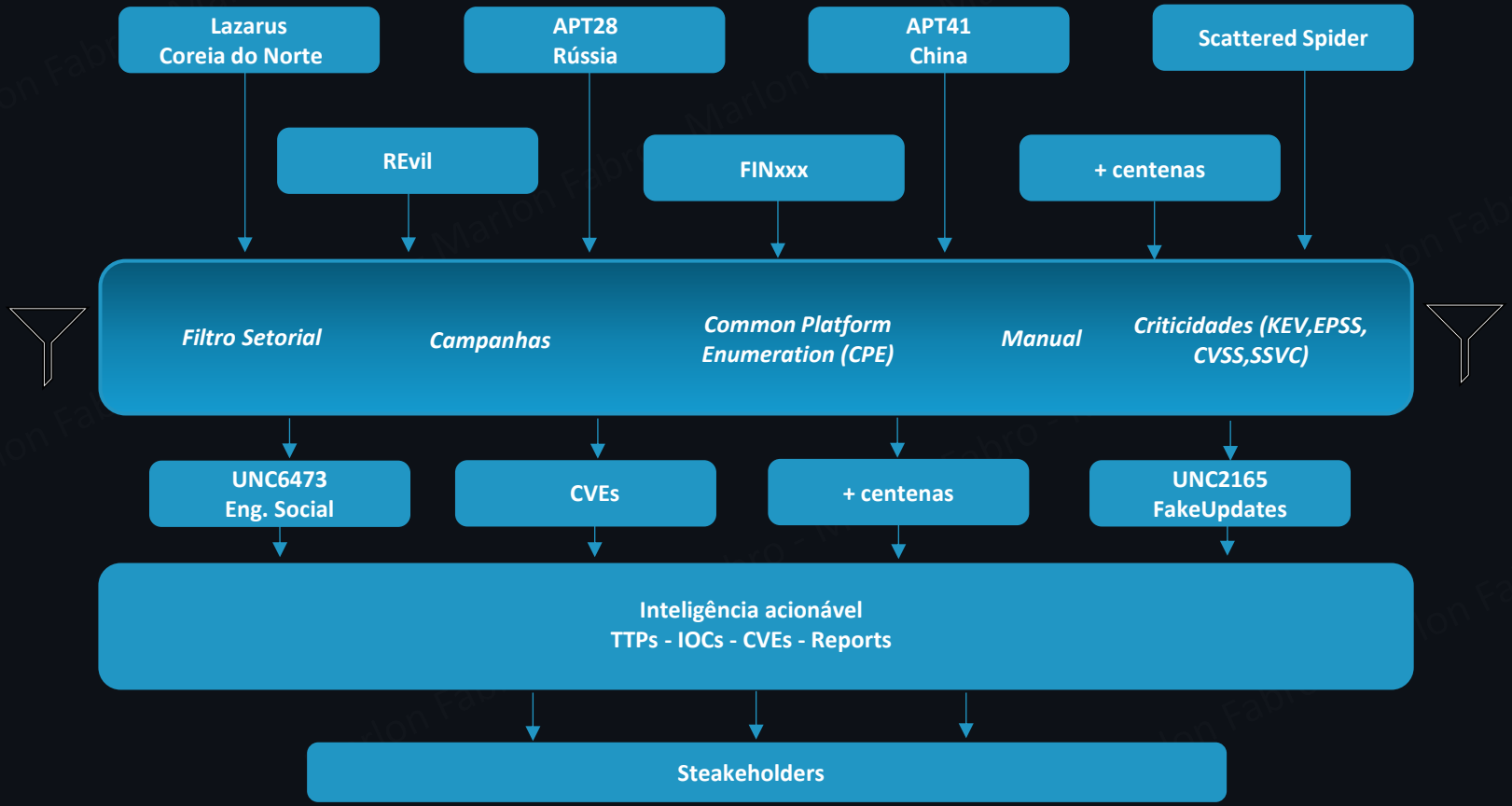
TLP:CLEAR

Mapa de Stakeholders e Produtos de CTI

	Produto	Audiência	Frequência	Formato
ESTRATÉGICO	**Strategic Briefing**	CISO · Executivos	Trimestral	Slides + Executive Summary
	Annual Threat Report	Risk Management	Anual	Relatório formal PDF
OPERACIONAL	**Monthly Threat Report**	Sec. Management · IR Lead	Mensal	PDF + Dashboard
	Adversary Playbook	IR · Forensics · Red Team	Por campanha	Wiki / Documento técnico
	Vuln. Dashboard	Vuln. Management	Semanal	Dashboard SIEM/Portal
TÁTICO	**Flash Report / Alert**	SOC · NOC · IR	Ad hoc / imediato	Email / Ticket / Chat
	IOC / Indicator Feed	Ferramentas (SIEM, EDR)	Contínuo	STIX/TAXII · JSON · CSV
	Weekly Threat Digest	SOC Leads · SecOps	Semanal	Email newsletter

CTI não é para CTI, é para alguém que toma decisão que nos fornece um requisito.

TLP:CLEAR


Lazarus
Coreia do Norte
APT28
Rússia
APT41
China
Scattered Spider
REvil
FINxxx
+ centenas
Filtro Setorial
Campanhas
Common Platform Enumeration (CPE)
Manual
Criticidades (KEV,EPSS, CVSS,SSVC)
UNC6473
Eng. Social
CVEs
+ centenas
UNC2165
FakeUpdates
Inteligência acionável
TTPs - IOCs - CVEs - Reports
Steakeholders

Modelo de Maturidade de Capacidade de CTI

CTI 0 PRE-FOUNDATIONAL	■ Nenhuma prática executada ■ Sem programa formal de CTI	**???**
CTI 1 FOUNDATIONAL	■ Práticas básicas, ad hoc e não documentadas ■ Foco em inteligência reativa ■ Resultados de curto prazo com valor limitado	**Reativa** Curto prazo
CTI 2 ADVANCED	■ Práticas documentadas, planejadas e padronizadas ■ Inteligência proativa e preditiva ■ Métricas com componente qualitativo	**Proativa / Preditiva** Médio prazo
CTI 3 LEADING	■ Práticas de referência ■ Inteligência prescritiva com recomendações ■ Mensuradas e alinhadas aos resultados do negócio ■ Resultados estratégicos de longo prazo	**Prescritiva** Longo prazo / Negócio

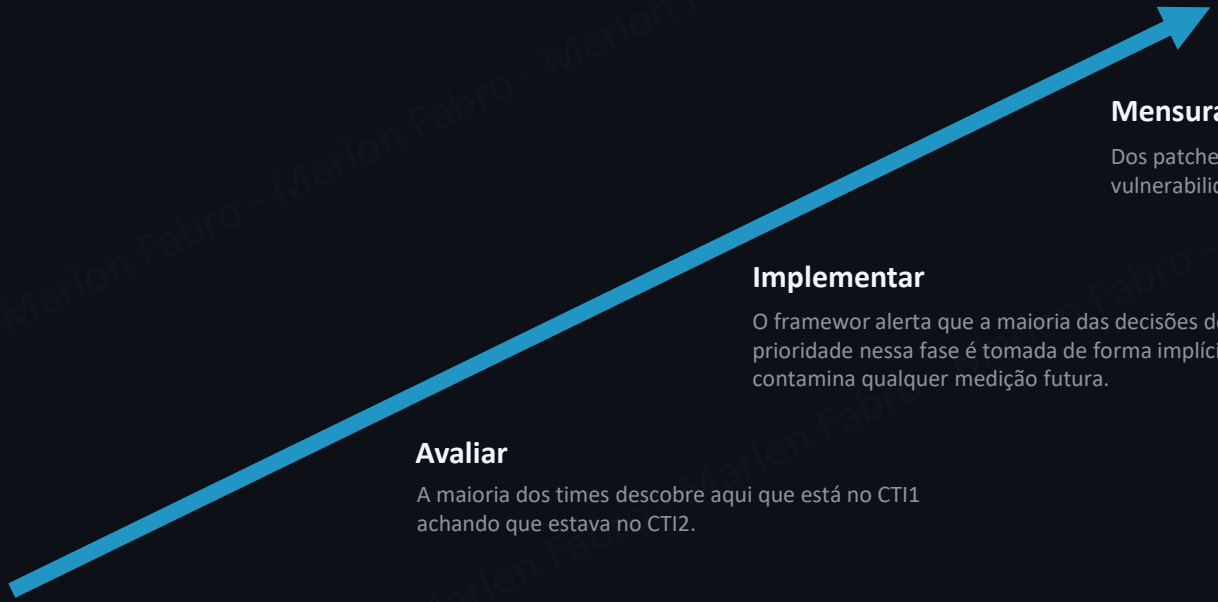
De Apagando Incêndio a Prevendo o Fogo

TLP:CLEAR

Reflexões...

CTI 0 PRE-FOUNDATIONAL	■ O CISO pergunta "quem nos ataca?" e a resposta honesta é "não sabemos" ■ IOCs chegam do vendor e vão direto pro SIEM sem triagem, gerando alert fatigue sem nenhuma inteligência real
CTI 1 FOUNDATIONAL	■ O analista de CTI é acionado durante um incidente pelo WhatsApp porque não existe processo formal de integração com IR ■ Existe uma lista das top famílias de malware do setor, mas ninguém sabe se a organização já teve contato com alguma delas
CTI 2 ADVANCED	■ Patches são priorizados com contexto de exploração ativa: Vuln Management para de tratar tudo como crítico e foca no que o ator relevante está usando agora ■ IOCs de alta fidelidade entram automaticamente no SIEM via SOAR com TTL definido, sem intervenção manual
CTI 3 LEADING	■ Antes de comprar um novo appliance, CTI avalia se o fornecedor tem histórico de targeting ou supply chain compromise relevante pro setor ■ O time não entrega só "esse ator usa Cobalt Strike, entrega recomendação de named pipes a bloquear e ajuste de policy específico pro ambiente

Reflexões...



Preparar

Sem esse alinhamento, o programa nasce respondendo perguntas que ninguém fez.

Avaliar

A maioria dos times descobre aqui que está no CTI1 achando que estava no CTI2.

Implementar

O framewor alerta que a maioria das decisões de prioridade nessa fase é tomada de forma implícita, e isso contamina qualquer medição futura.

Mensurar

Dos patches priorizados, quantas vulnerabilidades eram relevantes ao setor?

Preparar, Avaliar, Implementar e Mensurar

TLP:CLEAR

Partes interessadas

CTI não é apenas IOCs, é inteligência acionável direcionada a audiências específicas que move decisões.

CTI não é para CTI, é para alguém que toma decisão que nos fornece um requisito.

Stakeholder engagement é pré-condição para maturidade. Sem saber para quem você trabalha, tudo é ruído.

Papéis são confusos na indústria. Alinhe expectativas explicitamente dos dois lados da mesa.

O OODA loop do defensor precisa ser mais veloz que o do adversário. CTI é o multiplicador de força.

Maturidade não é sobre ferramentas, é sobre práticas repetíveis alinhadas a outcomes de negócio (CTI-CMM).

Intelligence is never completed. Improvement is continuous. Meça, itere, evolua.

TLP:CLEAR

Referências

- RECORDED FUTURE. The Intelligence Handbook. 4ª ed. Recorded Future, 2024. Disponível em: recordedfuture.com
- SADOWSKI, J.; VANDERLEE, K.; STONE, S.; COMPTON, J.; SLOWIK, J.; WILLIAMS, J. Mandiant CTI Analyst Core Competencies Framework. Mandiant / Google Cloud, maio 2022.
- DEBOLT, M. et al. Cyber Threat Intelligence Capability Maturity Model (CTI-CMM). v1.3. Intel 471, 2026. Disponível em: cti-cmm.org
- INSA – INTELLIGENCE AND NATIONAL SECURITY ALLIANCE. Cyber Intelligence: Preparing Today's Talent for Tomorrow's Threats. Cyber Intelligence Task Force. Arlington: INSA, setembro 2015. Disponível em: insaonline.org
- SANS INSTITUTE. FOR578: Cyber Threat Intelligence. Disponível em: sans.org/for578
- DOYLE, J. CTI Analyst Core Competencies — slides de referência ao Mandiant CTI Framework. Mandiant, 2022.

Obrigado

linkedin.com/in/marlonfabro

"Sem inteligência, você não defende. Você descobre."