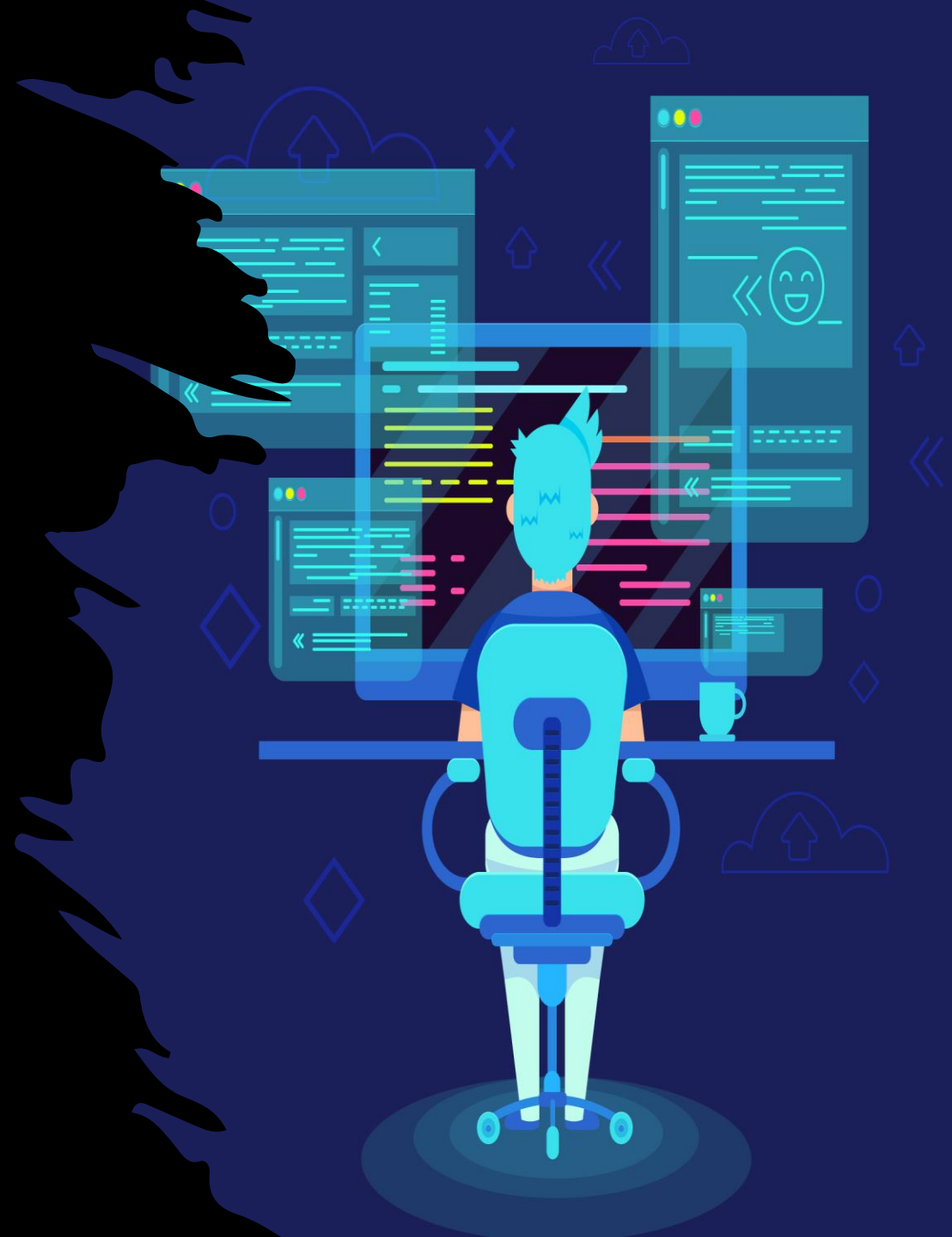
CYBER THREAT INTELLIGENCE 101

ANDERSON SILVA LIMA
WWW.LINKEDIN.COM/IN/LS-ANDERSON

O QUE É CTI?

É a coleta, processamento e análise de dados de várias origens, buscando entender o comportamento de atores de ameaças, seus alvos, motivações e padrão de ataques, possibilitando a mitigação ou tomada de ações proativas contra essas ameaças.



POR QUE É IMPORTANTE?

A partir da reunião de informações de inteligência sobre ameaças é possível:

- Revelar motivação de adversários e TTP’s (tactics, techniques, and procedures);
- Fornecer informações comportamentais de atores de ameaças;
- Fornecer informações relevantes para a tomada de decisão técnica;
- Fornecer informações relevantes para a tomada de decisão executiva.

CTI: LIFECYCLE

O ciclo de inteligência de ameaças é um framework de 6 passos, capaz de fornecer aos times de segurança a otimização de recursos para resposta às ameaças modernas:

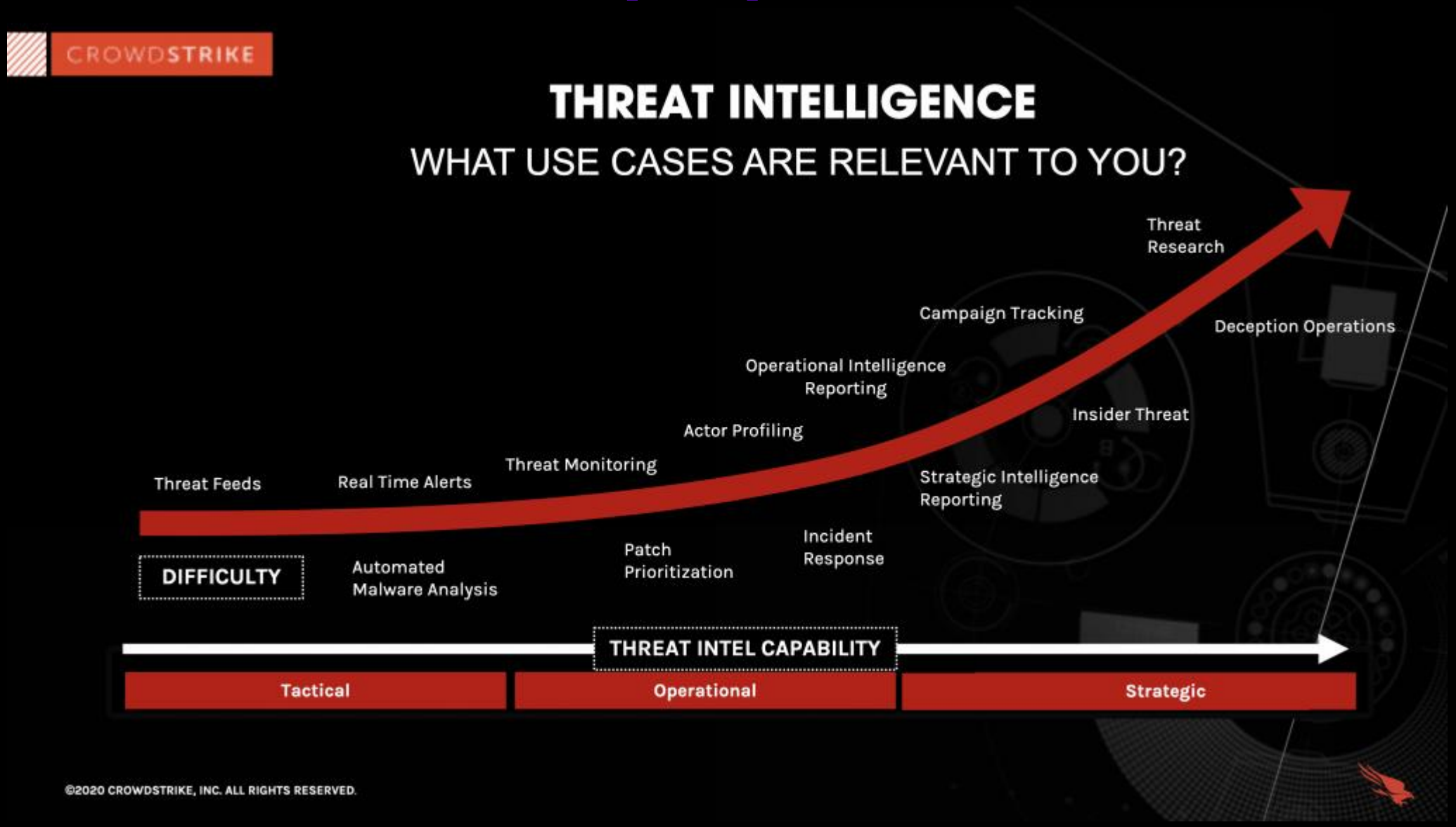
- Requirements;
- Collection;
- Processing;
- Analysis;
- Dissemination;
- Feedback.

CTI: CASOS DE USO (UC)

Function	Use Cases
Sec/IT Analyst	- Integrate TI feeds with other security products - Block bad IPs, URLS, domains, files etc
SOC	- Use TI to enrich alerts - Link alerts together into incidents - Tune newly deployed security controls
CSIRT	- Look for information on the who/what/why/when/how of an incident - Analyze root cause to determine scope of the incident
Intel Analyst	- Look wider and deeper for intrusion evidence - Review reports on threat actors to better detect them
Executive Management	- Assess overall threat level for the organization - Develop security roadmap

Fonte: https://www.crowdstrike.com/cybersecurity-101/threat-intelligence/

CTI: CASOS DE USO (UC)



CTI: RELATÓRIOS

A partir da criação de casos de uso para CTI é possível monitorar e relatar uma série de atividades maliciosas, sendo elas:

- Exposição de dados;
- Integridade da marca;
- Feed de IoC;
- Identificação de Phishing;
- Identificação de fraudes;
- Perfis suspeitos em redes sociais;
- Aplicativos móveis suspeitos;
- Monitoramento de VIP;
- Movimentações de grupos restritos;
- Informações sobre atores de ameaça;
- Outros.

CTI: BENEFÍCIOS

Function	Benefits
Sec/IT Analyst	Optimize prevention and detection capabilities and strengthen defenses
SOC	Prioritize incidents based on risk and impact to the organization
CSIRT	Accelerate incident investigations, management, and prioritization
Intel Analyst	Uncover and track threat actors targeting the organization
Executive Management	Understand the risks the organization faces and what the options are to address their impact

Fonte: https://www.crowdstrike.com/cybersecurity-101/threat-intelligence/

TIPOS DE THREAT INTELLIGENCE

No geral o Cyber Threat Intelligence pode ser dividido em 3 grupos distintos, baseado no tipo de informação relevante para cada grupo de stakeholders:

- Tactical intelligence;
- Operational intelligence;
- Strategic intelligence.

CTI: TIPOS

CROWDSTRIKE

INTELLIGENCE AREAS

TACTICAL

Focused on performing malware analysis & enrichment, as well as ingesting atomic, static, and behavioral threat indicators into defensive cybersecurity systems.

STAKEHOLDERS:
- SOC Analyst
- SIEM
- Firewall
- Endpoints
- IDS/IPS

"Mechanic"

OPERATIONAL

Focused on understanding adversarial capabilities, infrastructure, & TTPs, and then leveraging that understanding to conduct more targeted and prioritized cybersecurity operations.

STAKEHOLDERS:
- Threat Hunter
- SOC Analyst
- Vulnerability Mgmt.
- Incident Response
- Insider Threat

"Race Car Driver"

STRATEGIC

Focused on understanding high level trends and adversarial motives, and then leveraging that understanding to engage in strategic security and business decision-making.

STAKEHOLDERS:
- CISO
- CIO
- CTO
- Executive Board
- Strategic Intel

"The Owner"

CTI: IRoX Team

Em 19/10/2023 o grupo de Hacktivistas IRoX Team (Pró Palestina) declara guerra cibernética contra Israel e demais nações que a apoiam.

Em seu perfil do Telegram são publicadas as datas em que ocorrerão uma série de ataques contra essas nações, entre elas o Brasil.

Fonte: t.me/Irox_Team

TACTICAL INTELLIGENCE

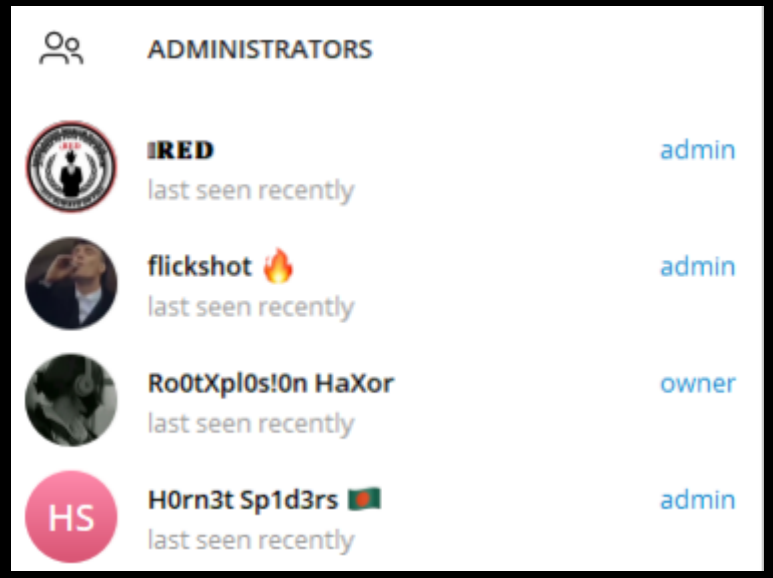
- Ações para futuro imediato: IoC.

Ghosts of Palestine / Hacktivist Of Garuda
185.199.108.153
185.199.109.153
185.199.110.153
185.199.111.153
Anonymous Sudan
101.167.152.76
101.167.152.90
109.235.139.13
213.61.253.152
213.61.253.250
213.61.254.11
213.61.254.36
217.110.80.14

OPERATIONAL INTELLIGENCE

Who: IRoX Team

- @Ro0txpl0s1on;
- @RED_official_69;
- @flickshot_officials;
- @h0rn3t_sp1d3r.



OPERATIONAL INTELLIGENCE

Why: Conflito Israel - Palestina

Os atores expressam que sua inspiração vem do suporte aos palestinos muçulmanos e da resistência a Israel, declarando seu propósito de se engajar em uma batalha digital contra Israel e seus aliados. O alvo, conforme destacado na comunicação do grupo, é "*aniquilar por completo o ambiente virtual daqueles que respaldam os judeus israelenses*".

Fonte: Heimdall Security Research *by* ISH Tecnologia

OPERATIONAL INTELLIGENCE

- How: TTP

Tática	Técnica	
Exfiltration (TA0010)		
Impact (TA0040)	Defacement (T1491)	
	Network DoS (T1498)	Direct Network Flood (T1498.001)
		Reflection Amplification (T1498.002)
	Endpoint DoS (T1499)	OS Exhaustion Flood (T1499.001)
		Service Exhaustion Flood (T1499.002)
		Application or System Exploitation (T1499.004)

STRATEGIC INTELLIGENCE

- Risco de negócio;
- Condições geopolíticas;
- Posicionamento da organização/alto escalão em mídias sociais;
- Priorização de riscos futuros em superfície de ataques específicas;
- Compreender as tendências;
- Gerar vantagem competitiva;
- Apresentar valor.

CYBER THREAT INTELLIGENCE 101

ANDERSON SILVA LIMA
WWW.LINKEDIN.COM/IN/LS-ANDERSON