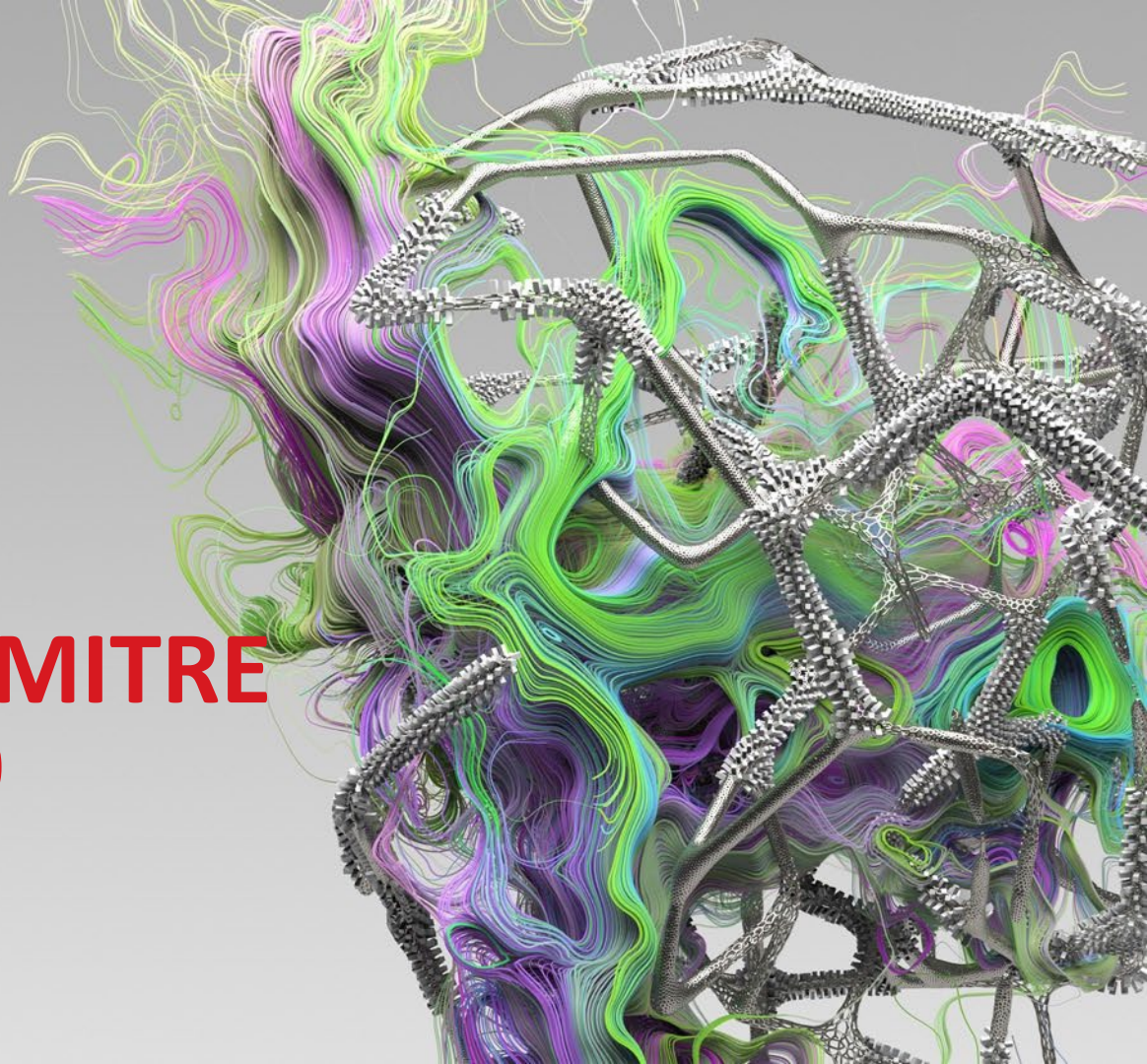


Resultados do MITRE ATT&CK APT29

Publicado em maio, 2020

APT29

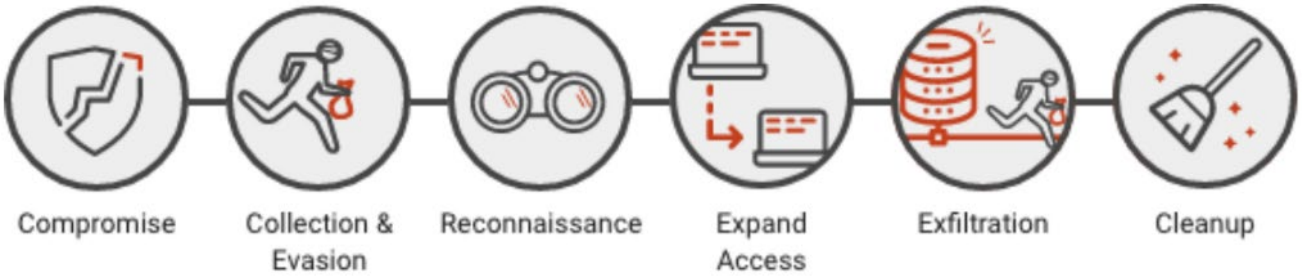
Nesse teste, a MITRE assumiu a persona do APT29, um grupo de ameaça atribuído ao governo russo e que opera pelo menos desde 2008.

Outros nomes: Cozy Bear, The Dukes, YTTRIUM

TREND MICRO™

APT29

Eles atacaram os ambientes dos participantes usando dois cenários. Esses cenários foram relatados publicamente para corresponder aos fluxos operacionais e de de negócios seguidos pelo grupo APT29.



Como esta avaliação diferencia

Centrado no adversário vs. Centrado no Malware

A avaliação MITRE testa como as soluções detectam um adversário executando um ataque direcionado. Ela não testa a capacidade de um produto de bloquear/prevenir malware.

APT29

Participantes incluíram:

TREND MICRO™
SentinelOne
McAfee™
CROWDSTRIKE
vmware Carbon Black
CORTEX™ BY PALO ALTO NETWORKS
kaspersky
Symantec™ A Division of Broadcom
BlackBerry CYLANCE
Microsoft

FireEye, Bitdefender, Cybereason, Cycraft, Elastic, F-Secure, HanSight, Malwarebytes, ReaQta, e Secureworks

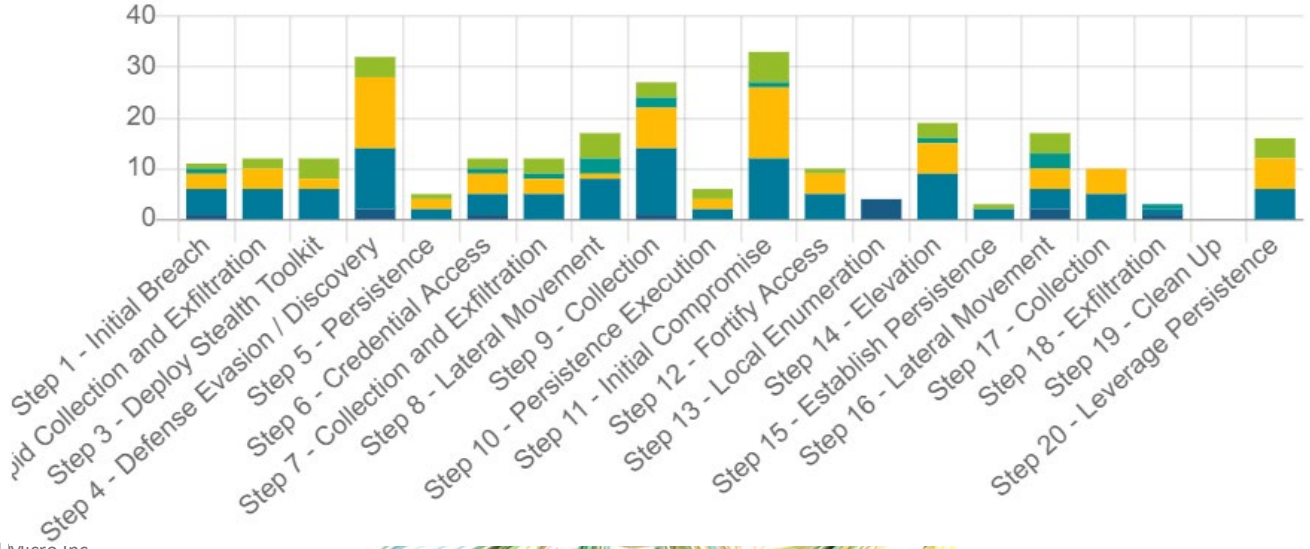
APT29

A avaliação analisou cada etapa do ataque para ver quais detecções (não a prevenção) foram registradas.

Detectado Automaticamente | **Detecção enriquecida usando a equipe do Trend Micro XDR** | **Não detectado**

TREND MICRO

Resultados

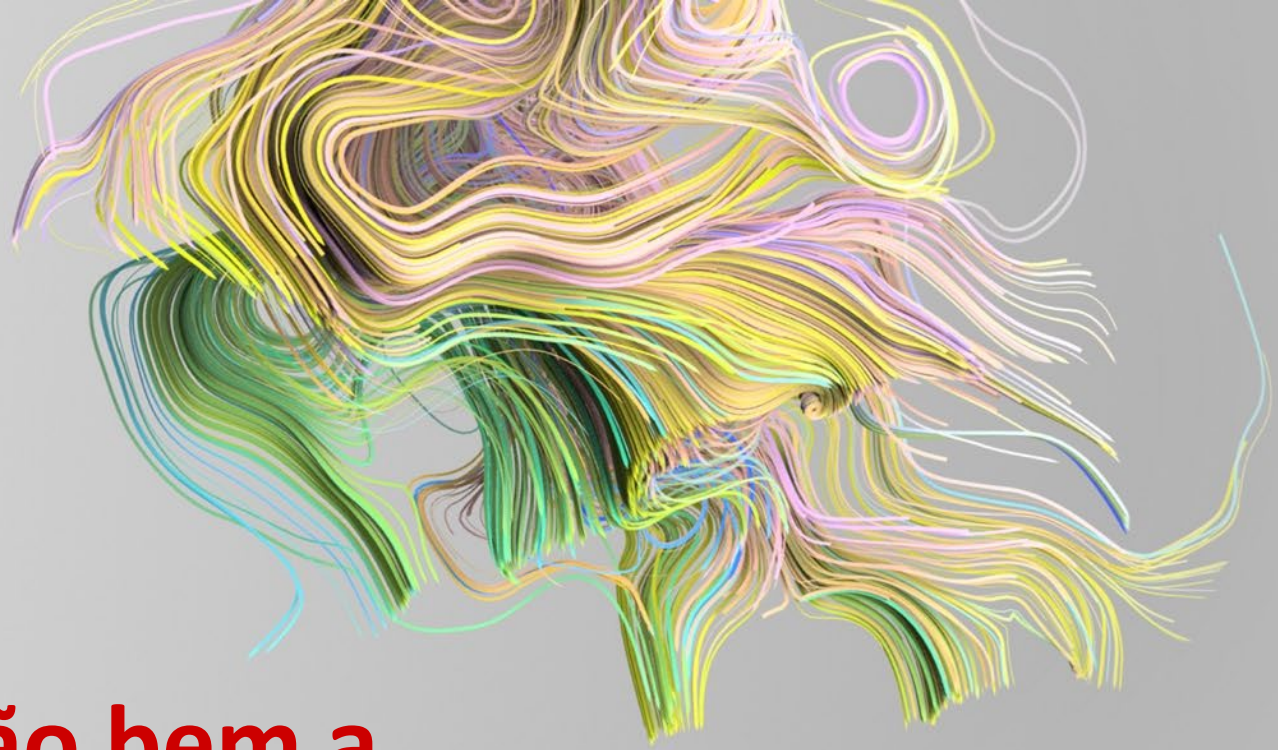


TREND MICRO

APT29

No entanto, o desafio é: nenhuma pontuação clara é dada.

> "Mostramos as detecções que observamos sem fornecer um "vencedor". Não há pontuações, classificações ou avaliações. Ao invés disso, mostramos como cada fornecedor aborda a defesa contra ameaças no contexto do ATT&CK."
>
> – MITRE



Então, quão bem a Trend Micro se saiu?

Nº 1 na detecção geral inicial

Líder

Taxa de detecção de 91% com configuração inicial
(em uma média de 78%)

#1
91%
TREND MICRO

#2
90%
SentinelOne

#3
89.5%
CORTEX BY PALO ALTO NETWORKS
Microsoft

Espera aí... Mas e quanto ao...

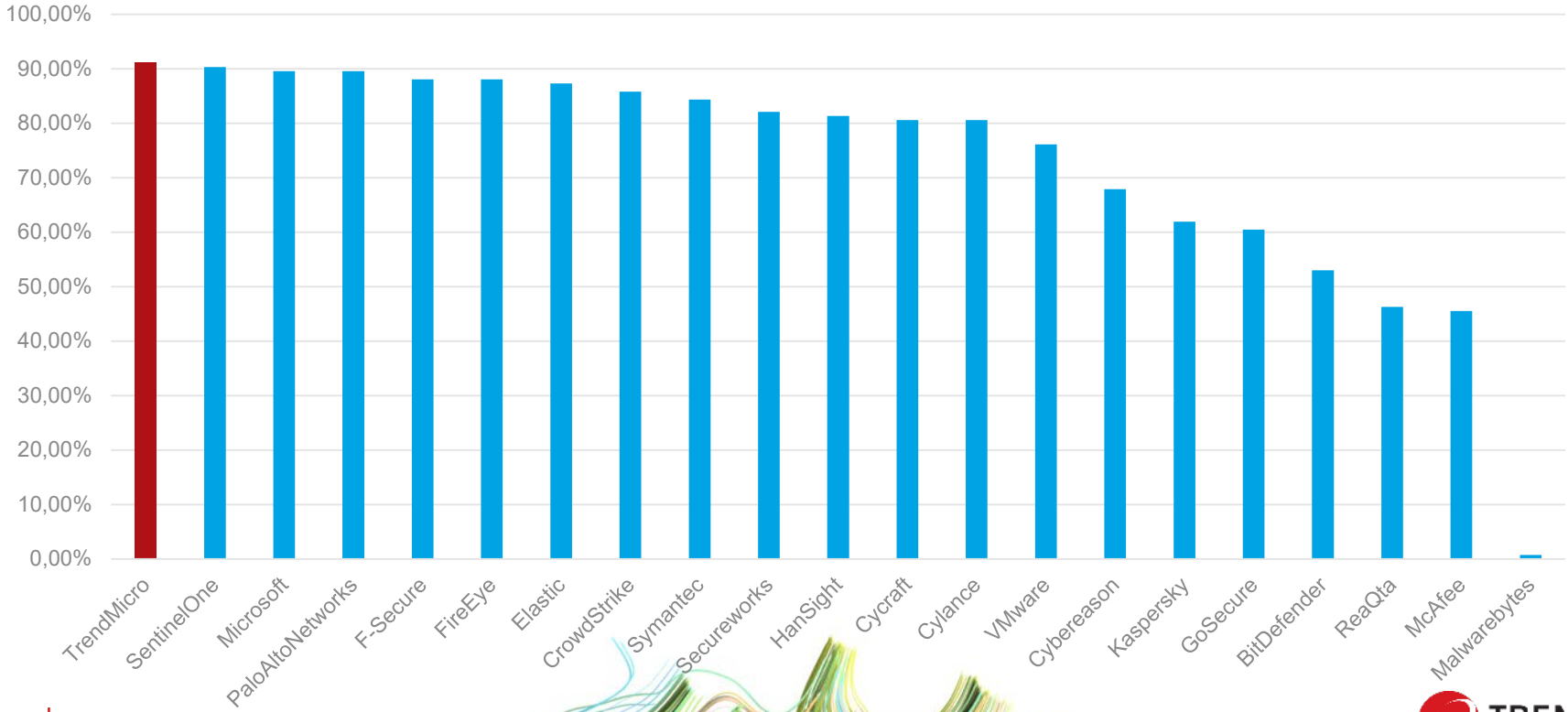
CROWDSTRIKE
#7
86%

vmware Carbon Black
#14
76%

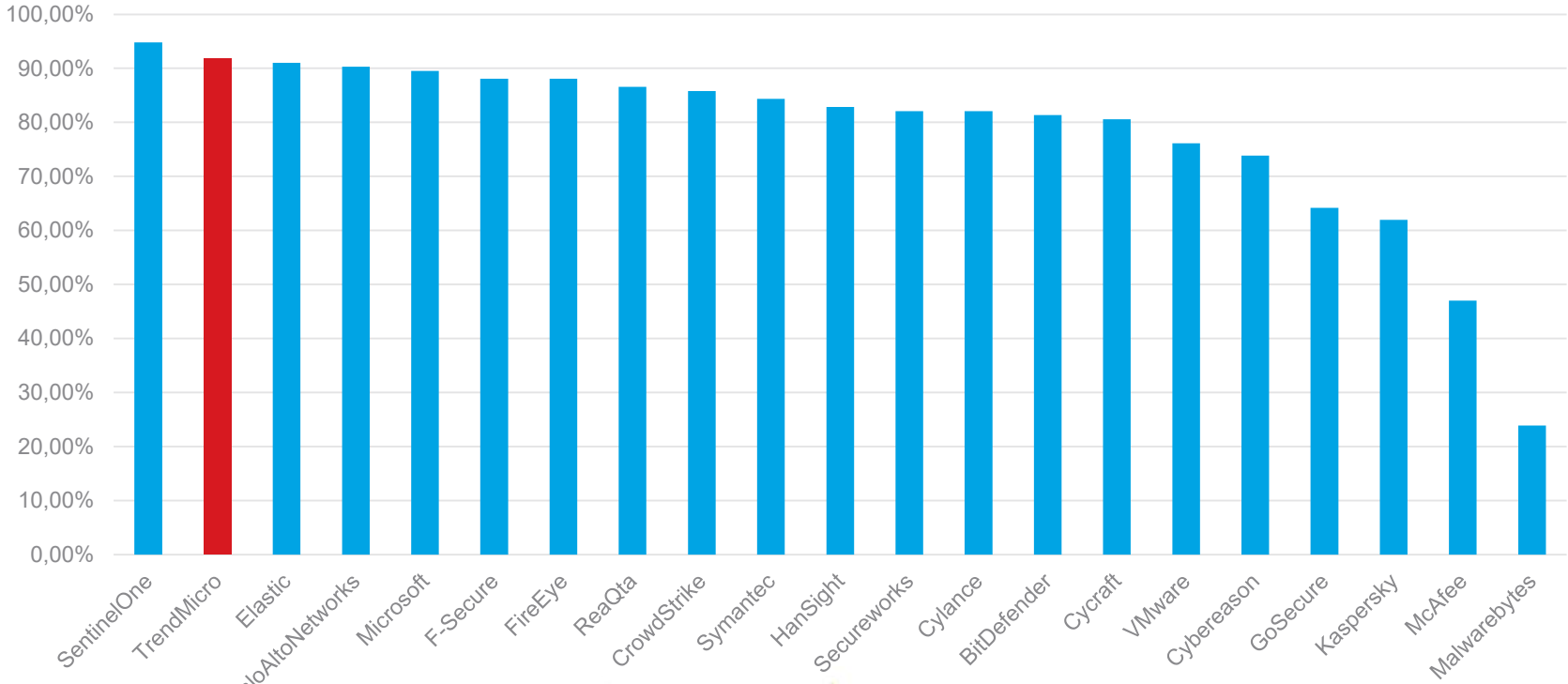
Symantec A Division of Broadcom
#8
84%

TREND MICRO

Detecções sem alterações de configuração

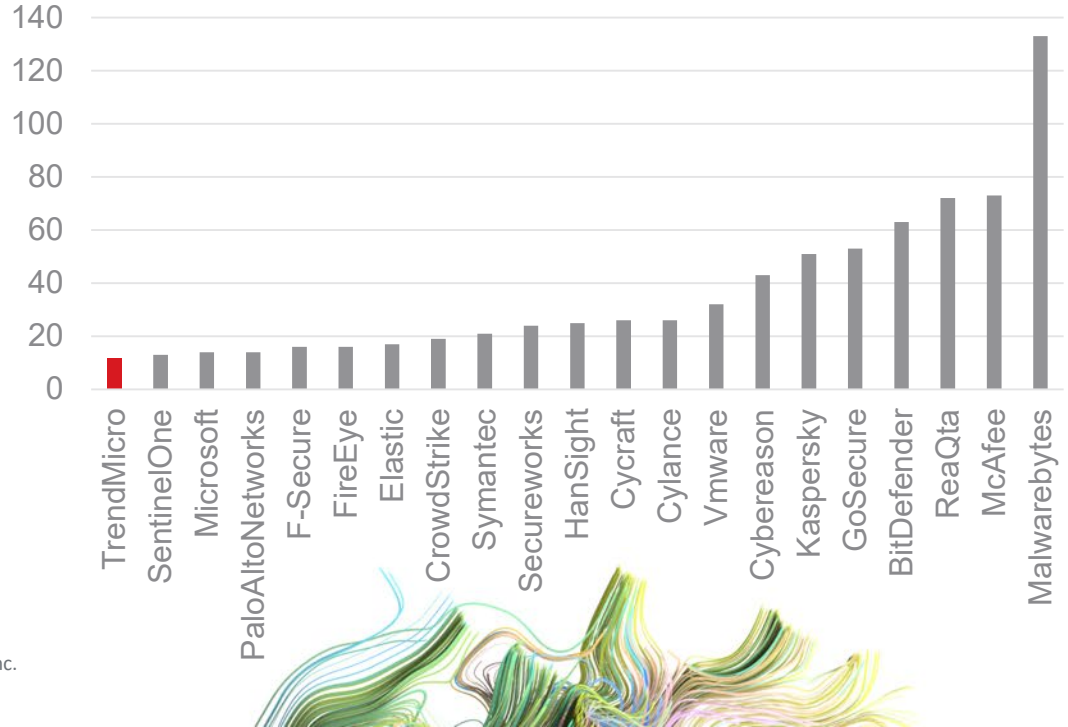


Detecções após mudanças de configuração



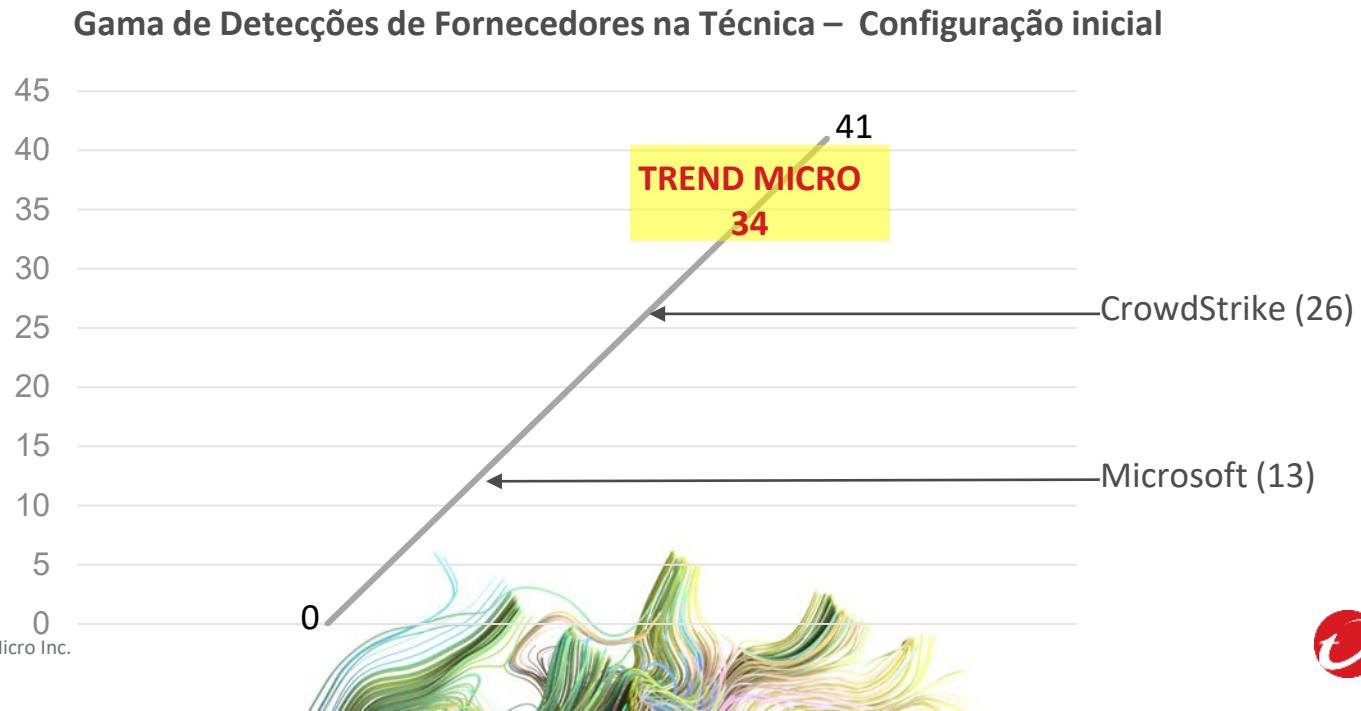
Principais destaques – Menos detecções perdidas

- Menor número de detecções perdidas entre todos os fornecedores – configuração inicial



Destaques Principais – Detecções de Técnica Fortes

- Detectou muito bem em técnicas de ataque individuais, que são detecções de maior confiança.



Destaques principais – Volume de Alertas Gerenciados

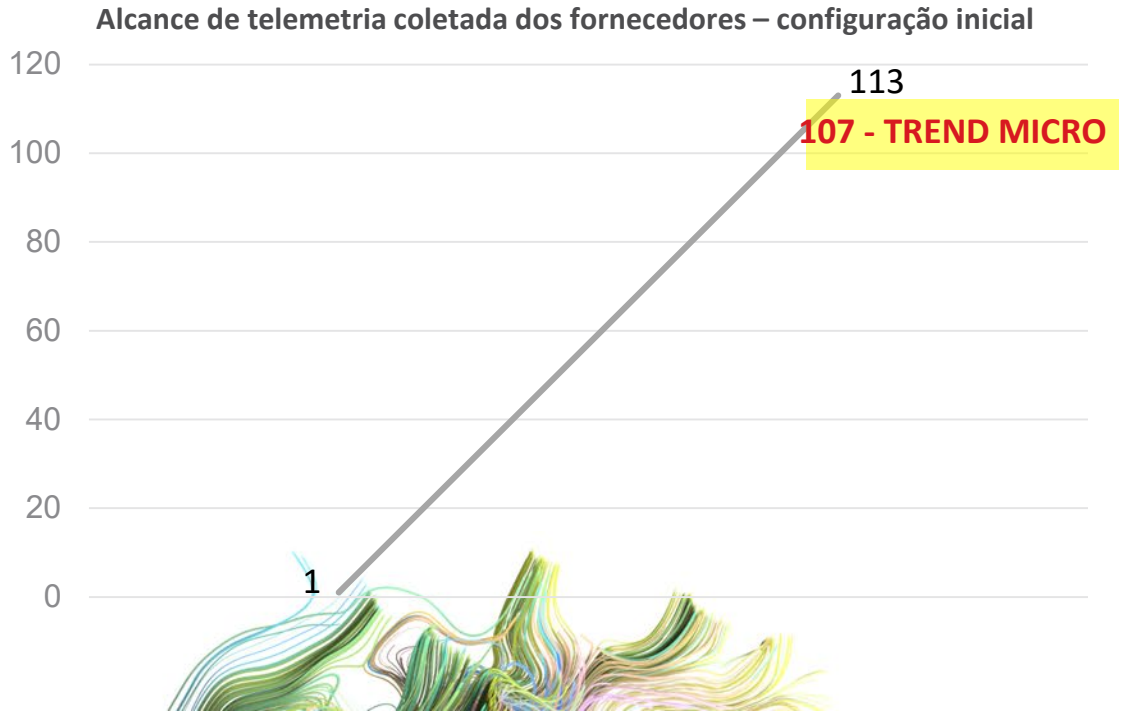
- Volume de alertas gerenciados para evitar fadiga de alertas.
- O nível mais baixo de alertas combinado com a alta taxa de detecção significa que reduzimos o ruído de todas as detecções em uma quantidade razoável de alertas.

Maior taxa de detecção, menor volume de alerta – Configuração Inicial

	Detection Rate	Alerts
TrendMicro	**91.04%**	**24**
SentinelOne	90.30%	51
Microsoft	89.55%	33
PaloAltoNetworks	89.55%	50
F-Secure	88.06%	38
FireEye	88.06%	54
Elastic	87.31%	46
CrowdStrike	85.82%	22
Symantec	84.33%	21
Secureworks	82.09%	34
…		
Cycraft	80.60%	90

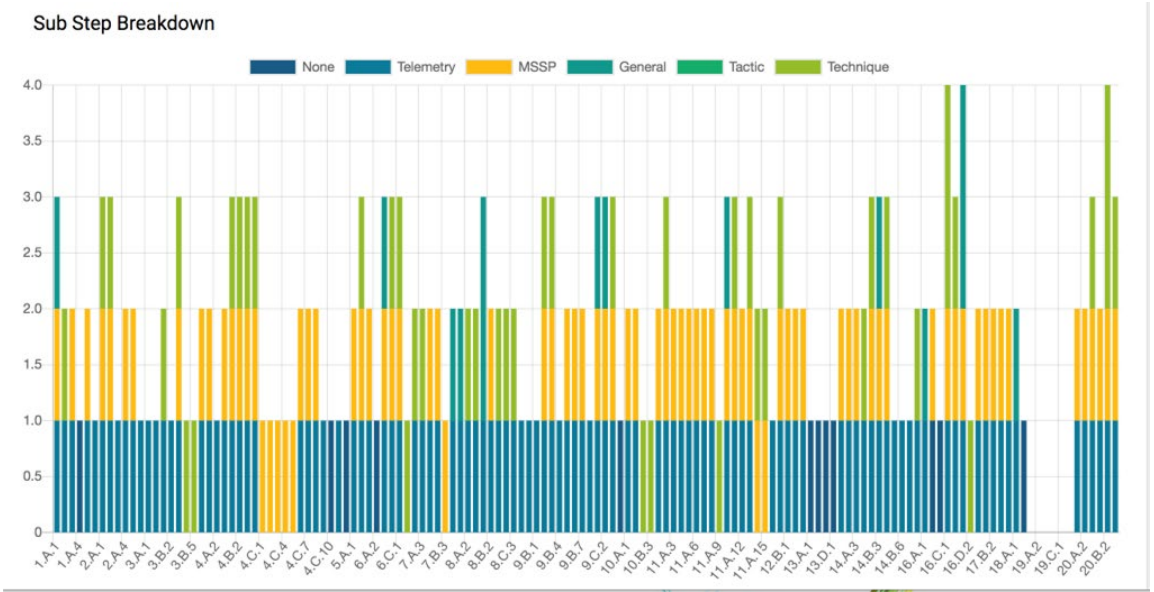
Destaques principais – Telemetria forte

- Telemetria = visibilidade. Fornecemos aos analistas de segurança acesso ao tipo e profundidade de visibilidade de que precisam ao examinar as atividades detalhadas do invasor



Destaques principais - Detecções Enriquecidas com MDR

- Nossos resultados de cobertura de detecção teriam permanecido fortes sem o serviço MDR, embora o serviço fosse capaz de adicionar contexto mais valioso para a detecção.



Apenas 6 detecções foram exclusivas para MSSP (MDR)

Destaques principais – Detecção Automatizada

- A avaliação verifica o comportamento *pós-comprometimento*: os fornecedores devem configurar os produtos em modo de detecção ou “somente alerta”.
- Como resultado, não leva em consideração nenhuma medida de detecção rápida e automatizada.
- A filosofia da Trend Micro é detectar e bloquear automaticamente o máximo possível, para que os clientes tenham menos para limpar e resolver

10+ passos bloqueados

Em pelo menos 10 etapas de ataque direcionado, a detecção e a resposta automatizadas teriam intervindo, interrompendo o ataque com uma ação de bloqueio (processo de eliminação, quarentena, isolamento etc.)

Destaques principais – XDR em 2020

- A plataforma Trend Micro XDR não fez parte desta avaliação

- Correlação e contexto são áreas de foco prioritárias para XDR:
  - Detecções correlacionadas com base em regras que procuram comportamentos diferentes nas camadas de segurança
  - Menos alertas acionáveis com maior contexto
  - Visibilidade e investigação integrada nas camadas de segurança: endpoint, e-mail, servidores & workloads em nuvem e rede

Referências

- Resultados da avaliação MITRE (APT29):
  - https://attackevals.mitre.org/evaluations.html?round=APT29

- Postagens do Blog:
  - https://blog.trendmicro.com.br/entendendo-avaliacoes-mitre-com-um-attcked-por-cozy-bear/
  - https://blog.trendmicro.com.br/top-dez-mitre/

TREND MICRO™

THE ART OF CYBERSECURITY

Unknown threats detected and stopped over time by Trend Micro. **Created with real data by artist Brendan Dawes.**