Abril de 2017

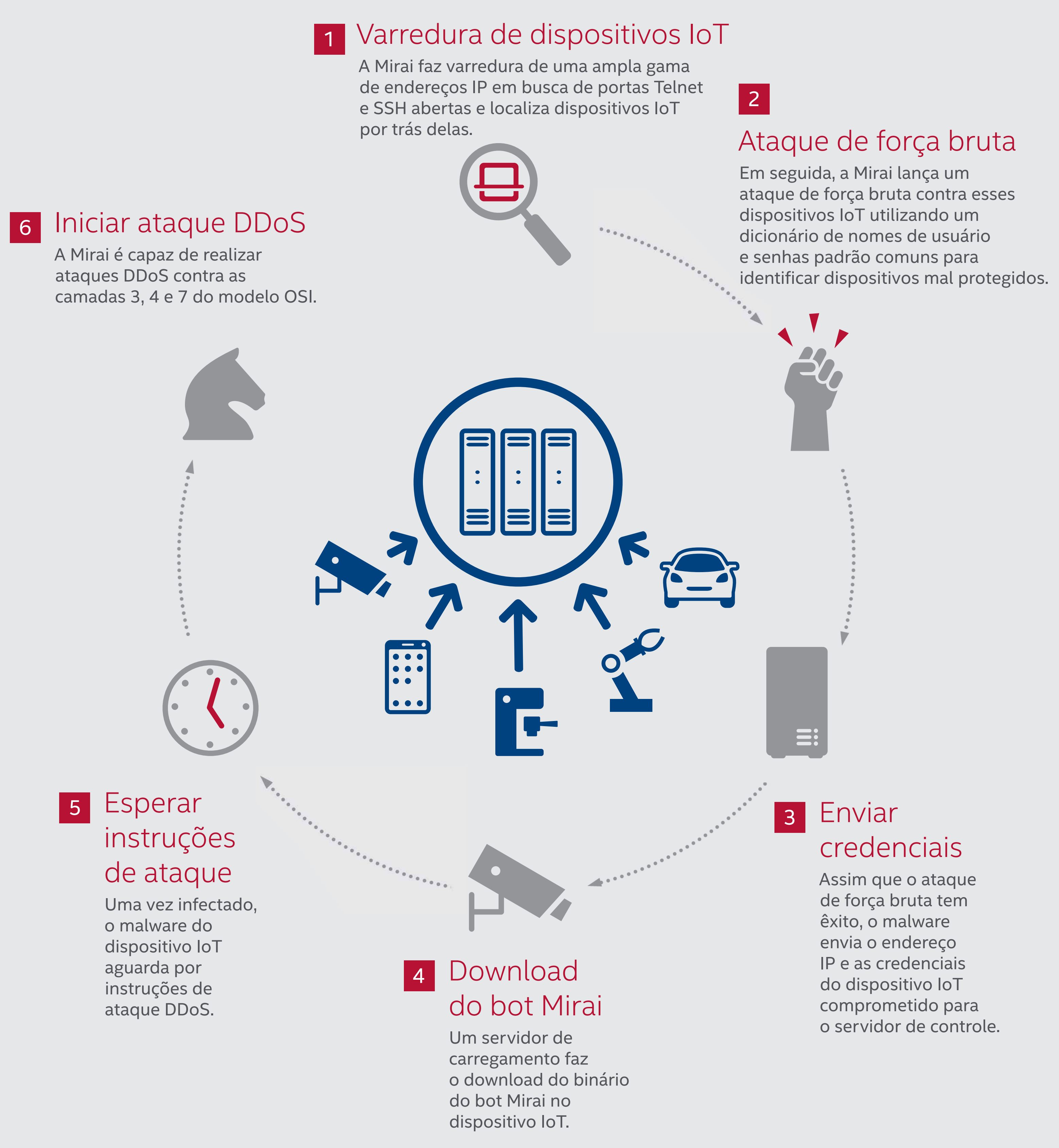
Relatório sobre ameaças

McAfee Labs

Mirai, a rede de bots da IoT

A rede de bots Mirai infectou e, em seguida, explorou dispositivos IoT mal protegidos para realizar o maior ataque de negação de serviço distribuída já registrado.

Processo de ataque



1 Varredura de dispositivos IoT

A Mirai faz varredura de uma ampla gama de endereços IP em busca de portas Telnet e SSH abertas e localiza dispositivos IoT por trás delas.

2 Ataque de força bruta

Em seguida, a Mirai lança um ataque de força bruta contra esses dispositivos IoT utilizando um dicionário de nomes de usuário e senhas padrão comuns para identificar dispositivos mal protegidos.

3 Enviar credenciais

Assim que o ataque de força bruta tem êxito, o malware envia o endereço IP e as credenciais do dispositivo IoT comprometido para o servidor de controle.

4 Download do bot Mirai

Um servidor de carregamento faz o download do binário do bot Mirai no dispositivo IoT.

5 Esperar instruções de ataque

Uma vez infectado, o malware do dispositivo IoT aguarda por instruções de ataque DDoS.

6 Iniciar ataque DDoS

A Mirai é capaz de realizar ataques DDoS contra as camadas 3, 4 e 7 do modelo OSI.

2,5 milhões

Aproximadamente 2,5 milhões de dispositivos IoT foram infectados pela Mirai.

5 por minuto

A cada minuto, aproximadamente cinco endereços IP são adicionados às redes de bots Mirai.

1,2 Tbps de tráfego

Em seu pico, um alvo da rede de bots Mirai foi inundado por 1,2 Tbps de tráfego, o maior volume de tráfego DDoS já registrado.

US$ 50 a US$ 7.500 por dia

Os ataques DDoS com base na Mirai agora são oferecidos como serviço a um preço de U$ 50 a US$ 7.500 por dia.

Cronologia da evolução da Mirai

Agosto | Setembro | Outubro | Novembro

1 *Por volta de agosto de 2016*

Lançamento inicial da Mirai

Começam a surgir binários ELF da Mirai.

2 *20 de setembro de 2016*

DDoS contra o site da “Krebs on Security”

A Mirai infecta DVRs e CCTVs pela porta Telnet.

3 *1º de outubro de 2016*

Divulgação do código-fonte da Mirai

Anna-Senpai divulga o código-fonte da Mirai.

4 *4 de outubro de 2016*

Mirai, rede de bots como serviço

Fórum underground oferece DDoS como serviço.

5 *28 de novembro de 2016*

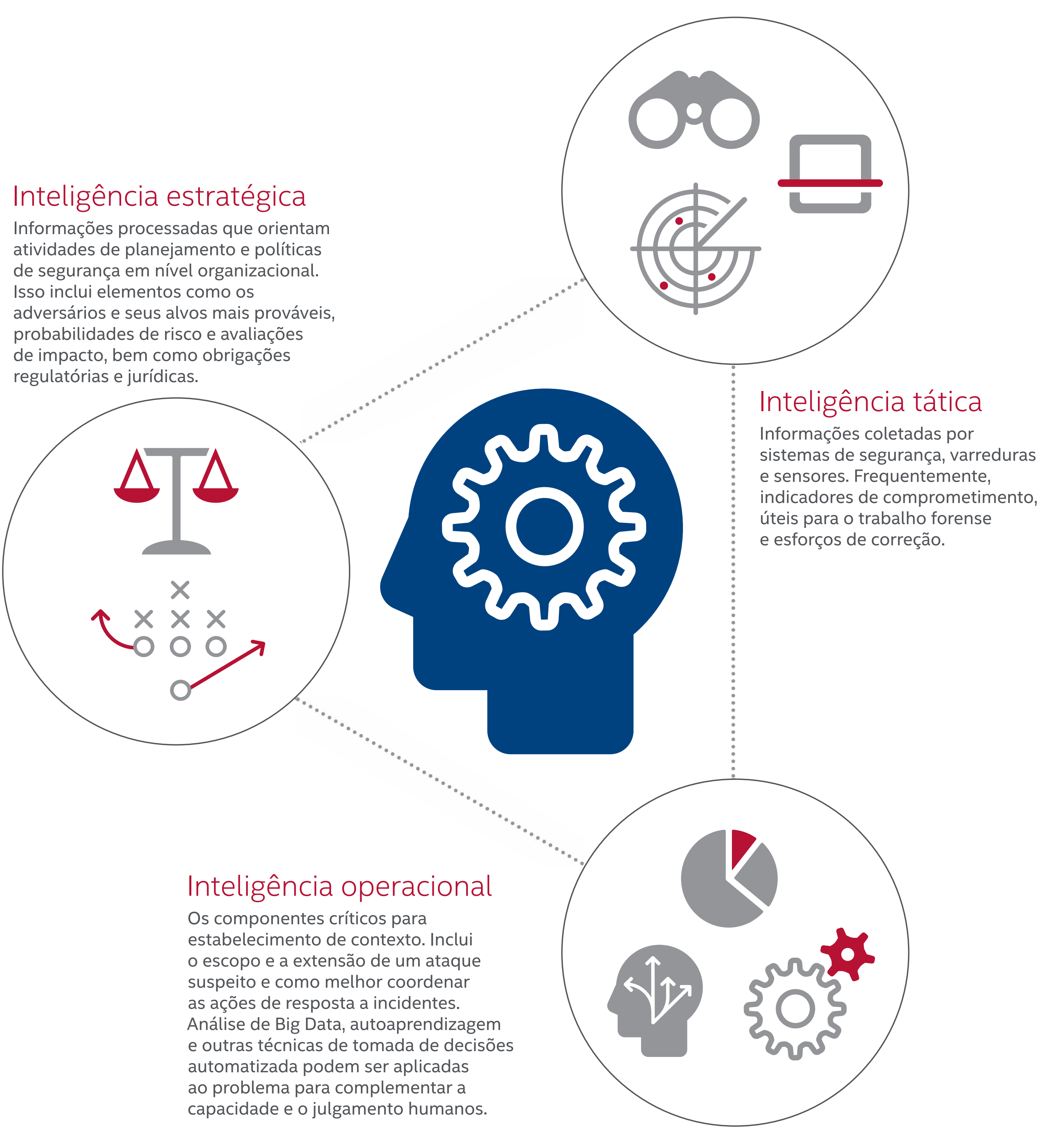
Paralisação da Deutsche Telekom

Encontrada nova variante da Mirai. Visa a porta 7547.

Compartilhamento de inteligência contra ameaças

O que você não sabe pode atingi-lo.

O que é inteligência contra ameaças?



Inteligência estratégica

Informações processadas que orientam atividades de planejamento e políticas de segurança em nível organizacional. Isso inclui elementos como os adversários e seus alvos mais prováveis, probabilidades de risco e avaliações de impacto, bem como obrigações regulatórias e jurídicas.

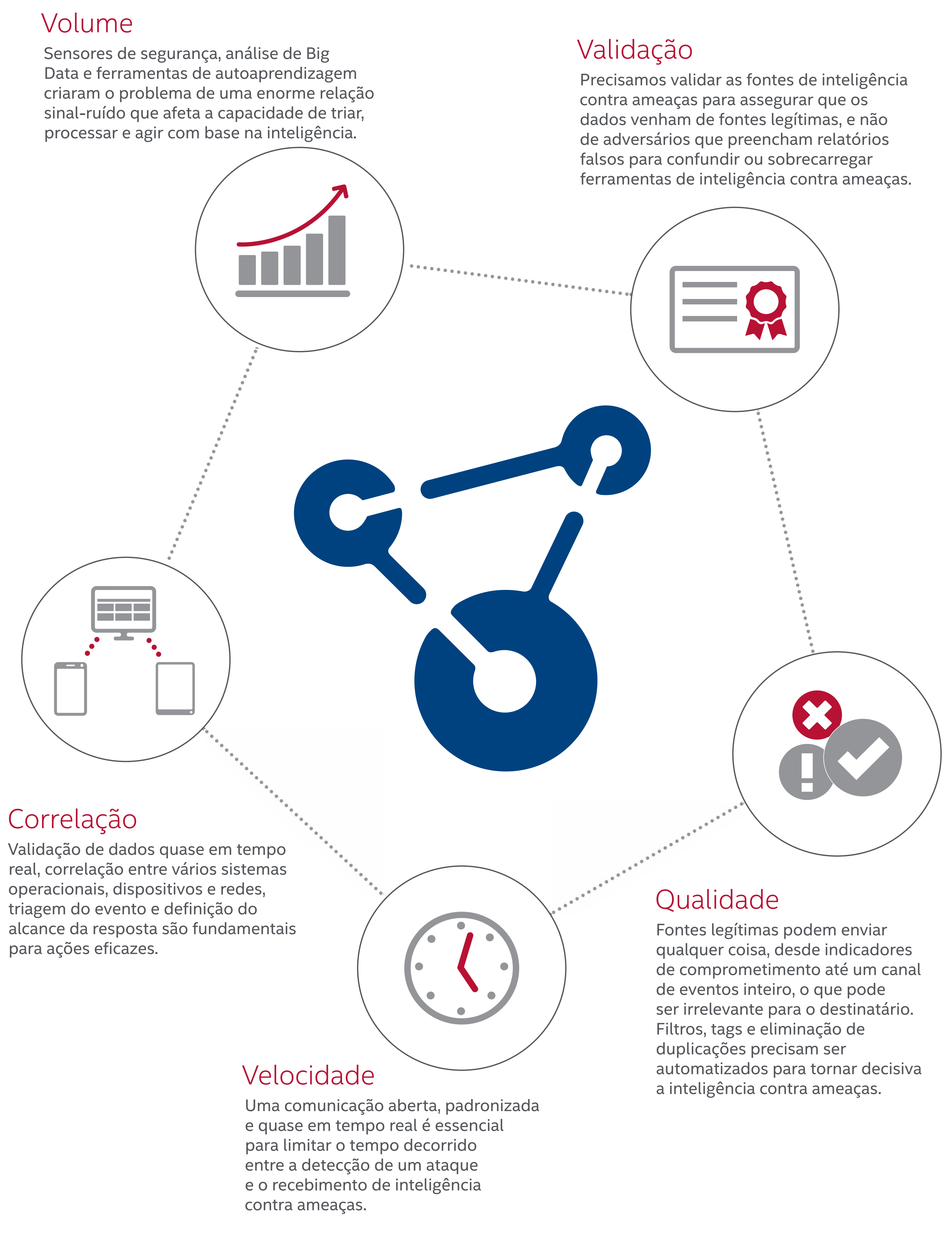
Inteligência tática

Informações coletadas por sistemas de segurança, varreduras e sensores. Frequentemente, indicadores de comprometimento, úteis para o trabalho forense e esforços de correção.

Inteligência operacional

Os componentes críticos para estabelecimento de contexto. Inclui o escopo e a extensão de um ataque suspeito e como melhor coordenar as ações de resposta a incidentes. Análise de Big Data, autoaprendizagem e outras técnicas de tomada de decisões automatizada podem ser aplicadas ao problema para complementar a capacidade e o julgamento humanos.

Desafios críticos no compartilhamento de inteligência contra ameaças



Volume

Sensores de segurança, análise de Big Data e ferramentas de autoaprendizagem criaram o problema de uma enorme relação sinal-ruído que afeta a capacidade de triar, processar e agir com base na inteligência.

Validação

Precisamos validar as fontes de inteligência contra ameaças para assegurar que os dados venham de fontes legítimas, e não de adversários que preencham relatórios falsos para confundir ou sobrecarregar ferramentas de inteligência contra ameaças.

Correlação

Validação de dados quase em tempo real, correlação entre vários sistemas operacionais, dispositivos e redes, triagem do evento e definição do alcance da resposta são fundamentais para ações eficazes.

Qualidade

Fontes legítimas podem enviar qualquer coisa, desde indicadores de comprometimento até um canal de eventos inteiro, o que pode ser irrelevante para o destinatário. Filtros, tags e eliminação de duplicações precisam ser automatizados para tornar decisiva a inteligência contra ameaças.

Velocidade

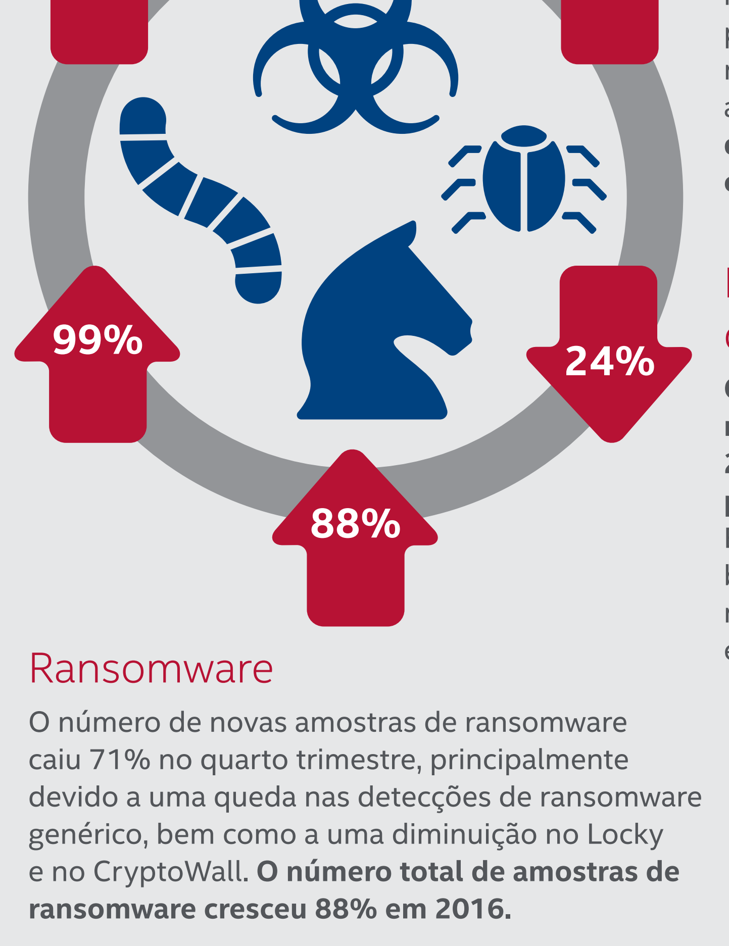
Uma comunicação aberta, padronizada e quase em tempo real é essencial para limitar o tempo decorrido entre a detecção de um ataque e o recebimento de inteligência contra ameaças.

Estatísticas sobre ameaças

Surgem 176 novas ameaças a cada minuto ou quase três por segundo.

Incidentes

Contamos 197 incidentes públicos conhecidos no quarto trimestre e 974 incidentes públicos conhecidos em 2016.



Malware

O número de novas amostras de malware no quarto trimestre — 23 milhões — caiu 17% em relação ao terceiro trimestre. **Porém, a contagem total cresceu 24% em 2016, para 638 milhões de amostras.**

Malware para Mac OS

Embora ainda pequeno em comparação com as ameaças para Windows, o número de novas amostras de malware para Mac OS cresceu 245% no quarto trimestre devido à agregação de adware. **O total de malware para Mac OS cresceu 744% em 2016.**

Malware móvel

O número de novas amostras de malware móvel caiu em 17% no quarto trimestre. **Mas o total de malware móvel cresceu 99% em 2016.**

Redes de bots de spam

Os e-mails de spam das dez maiores redes de bots caíram 24% no quarto trimestre, para 181 milhões de e-mails. Essas dez maiores redes de bots geraram 934 milhões de mensagens de e-mail de spam em 2016.

Ransomware

O número de novas amostras de ransomware caiu 71% no quarto trimestre, principalmente devido a uma queda nas detecções de ransomware genérico, bem como a uma diminuição no Locky e no CryptoWall. **O número total de amostras de ransomware cresceu 88% em 2016.**

McAfee Global Threat Intelligence

O McAfee GTI recebeu, em média, 49,6 bilhões de consultas por dia.

McAfee GTI

66 milhões

As proteções do McAfee GTI contra URLs maliciosos **aumentaram para 66 milhões por dia no quarto trimestre**, em relação a 57 milhões por dia no terceiro trimestre.

37 milhões

As proteções do McAfee GTI contra programas potencialmente indesejados (PUPs) **aumentaram para 37 milhões por dia no quarto trimestre**, em relação a 32 milhões por dia no terceiro trimestre.

71 milhões

As proteções do McAfee GTI contra arquivos maliciosos **diminuíram para 71 milhões por dia no quarto trimestre**, em relação a 150 milhões por dia no terceiro trimestre, devido a um maior bloqueio de downloads.

35 milhões

As proteções do McAfee GTI contra endereços IP arriscados **aumentaram para 35 milhões por dia no quarto trimestre**, em relação a 27 milhões por dia no terceiro trimestre.

Relatório do McAfee Labs sobre ameaças: abril de 2017

Visite www.mcafee.com/April2017ThreatsReport para ler o relatório completo.

intel Security

2614_0217_info-threat-report-mirai-iot