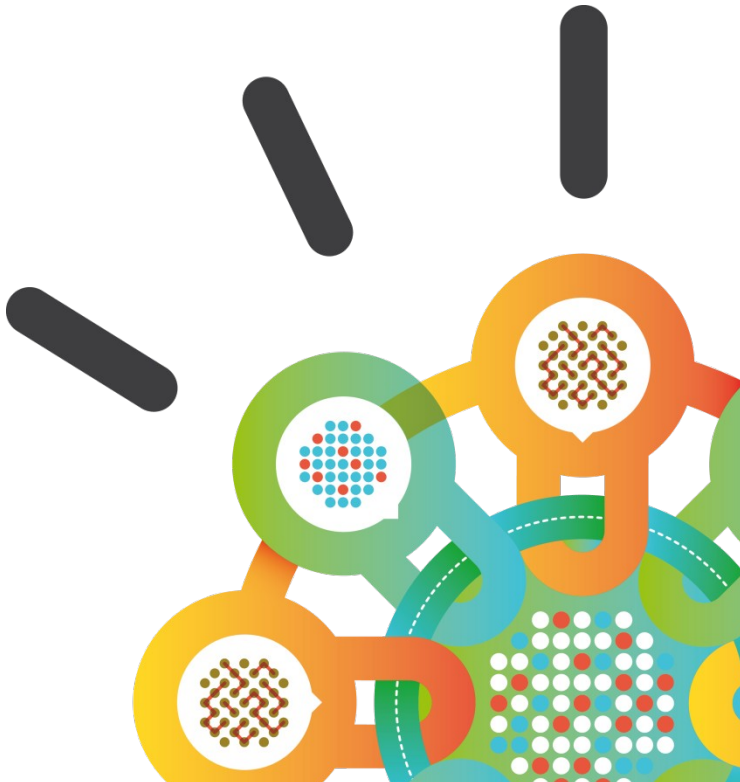
Security Intelligence.
Think Integrated.

Como tratar as ameaças mais recentes identificadas no Relatório de Tendências e Riscos IBM X-Force

Novembro de 2013



Ataques direcionados permanecem na lembrança

Bloomberg

A Arábia Saudita disse que o ataque virtual da Aramco veio de estados estrangeiros

– Bloomberg, Dez 2012

InformationWeek

Lockheed Martin sofre ataque virtual massivo

– InformationWeek, Maio 2011

theguardian

Facebook foi hackeado em "ataque sofisticado"

– The Guardian, Fev 2013

The New York Times

RSA encara usuários irritados após violação

– The New York Times, Junho 2011

THE WALL STREET JOURNAL.

Fed reconhece violação na segurança virtual

– The Wall Street Journal, Fev 2013

THE WALL STREET JOURNAL.

NASDAQ confirma violação em rede

– The Wall Street Journal, Fev 2011

THE HUFFINGTON POST

Apple Hackeada: Empresa admite que website de desenvolvimento foi violado

– Huffington Post, Julho 2013

CNN

Servidor de contribuintes da Carolina do Sul hackeado, 3,6 milhões de números do Seguro Social comprometidos

– CNN, Out 2012

WIRED

Hacking chinês de mídia dos EUA é "fenômeno predominante“

– Wired, Fev 2013

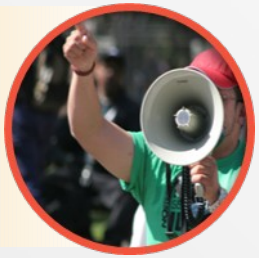
Por que isto continua? Os invasores aperfeiçoaram suas habilidades

MOTIVAÇÃO

Segurança Nacional, Espionagem Econômica

Atores de nível nacional, APTs
Stuxnet, Aurora, APT-1

Notoriedade, Ativismo, Difamação



Hacktivistas
Lulzsec, Anonymous

Ganho Monetário

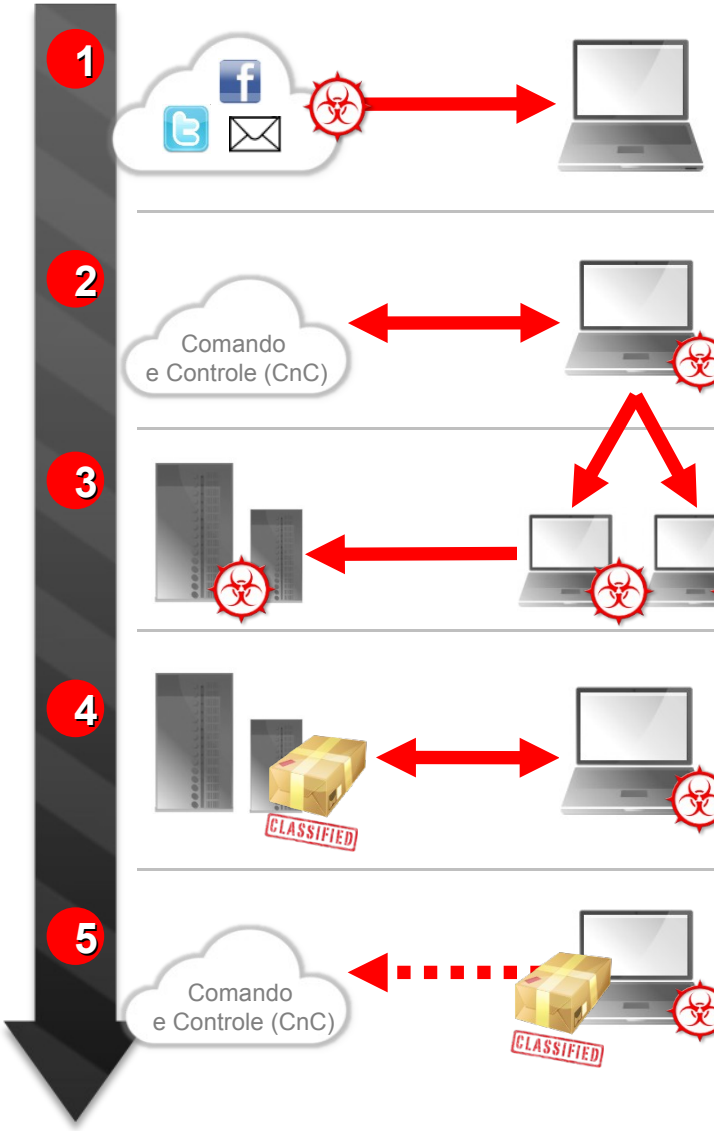
Crime organizado
Zeus, ZeroAccess, Pacote de Exploração de Blackhole

Aborrecimento, Curiosidade

Pessoas do grupo, Spammers, Script-kiddies
Nigerian 419 Scams, Code Red

SOFISTICAÇÃO

Os ataques mais direcionados seguem uma cadeia de 5 estágios



Infiltra — Reconhecimento, spear phishing e explorações remotas para obter acesso

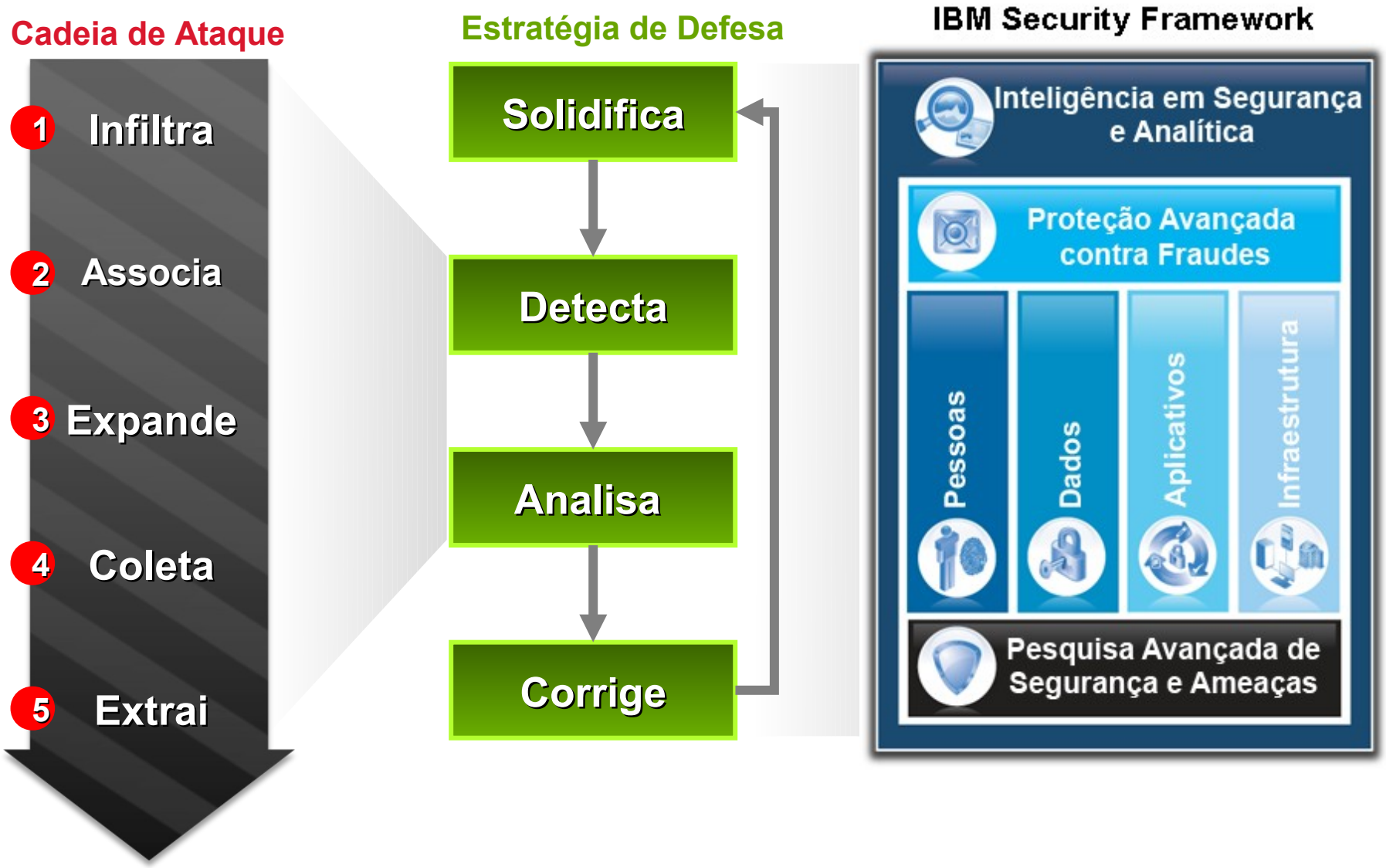
Associa — Malware e backdoors instalados para estabelecer uma base sólida

Expande — Movimento lateral para aumentar o acesso e manter uma presença

Coleta — Aquisição e agregação de dados confidenciais

Extrai — Extração de dados para redes externas

Os defensores devem seguir uma abordagem iterativa



Solidifica

O que o Relatório de Tendências X-Force nos diz:

A CORREÇÃO CONTINUA A SER PROBLEMÁTICA

"A distribuição de malware a usuários domésticos e corporativos ainda é altamente eficiente devido a vulnerabilidades em navegadores e plug-ins de navegação"

APLICATIVOS DE WEB SÃO UM CALCANHAR DE AQUILES

"Com base nos incidentes que cobrimos, o SQLi (SQL Injection) permanece como o paradigma mais comum de violação inclusive no primeiro semestre de 2013"

VULNERABILIDADES AINDA ESTÃO EM CRESCIMENTO

"No primeiro semestre de 2013, o X-Force reportou a soma de um pouco mais de 4100 novas vulnerabilidades de segurança reportadas publicamente no banco de dados"

Solidifica

Exemplo de Melhores Práticas:

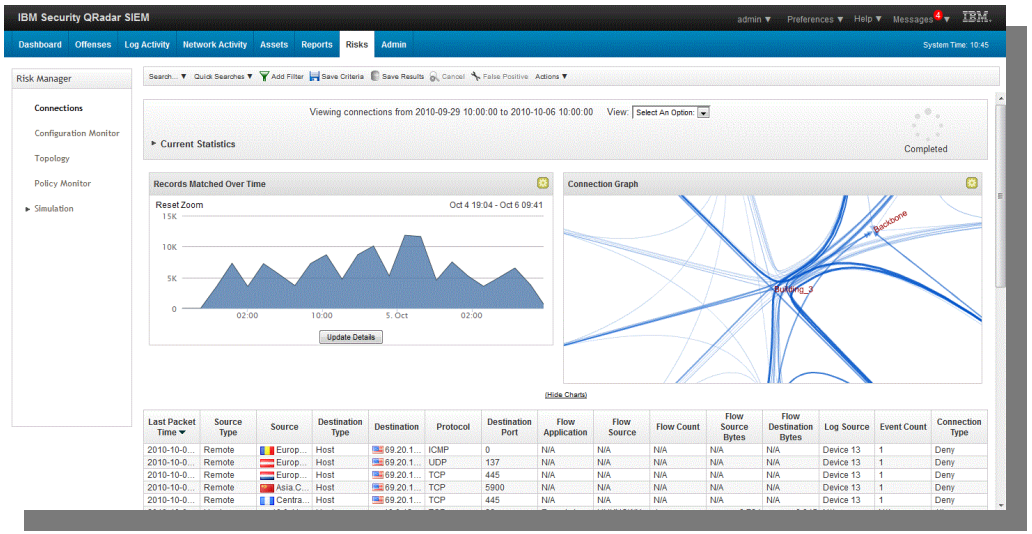
1. Configurar adequadamente e corrigir terminais
2. Monitorar e analisar configurações de rede
3. Desenvolver com segurança e auditar aplicativos da web
4. Controlar atividades privilegiadas e identidades compartilhadas
5. Varrer com inteligência e priorizar vulnerabilidades

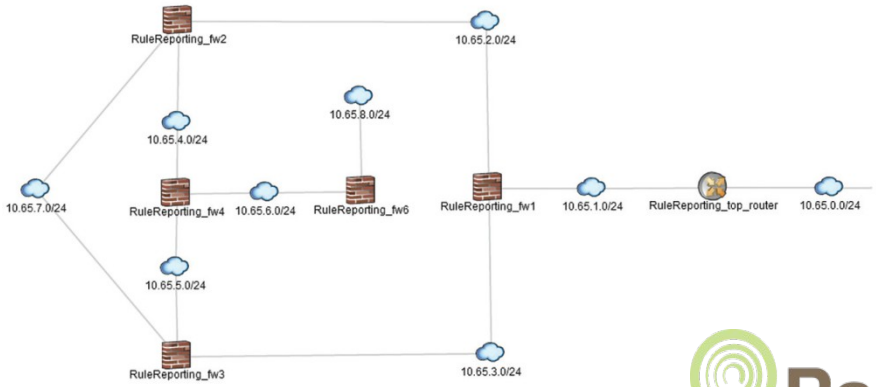
Solidifica 1. Configurar adequadamente e corrigir terminais

Como o IBM Endpoint Manager ajuda

- Gerencia centenas de milhares de terminais independentemente da localização, tipo de conexão ou status
- Automaticamente fiscaliza o cumprimento de linhas de base de segurança em todos os terminais dentro da organização, incluindo versões de software de navegador instaladas e configurações
- Aplica quarentena automática nos terminais fora de conformidade até que a conformidade seja atingida

Solidifica 2. Monitorar e analisar configurações de rede





Como o IBM QRadar ajuda

- Descreve visualizações de topologia, ajuda a visualizar padrões atuais e alternativos de tráfego de rede
- Coleta dados de configuração de dispositivos de rede para avaliar vulnerabilidades e facilitar a análise e relatórios
- Descobre erros na configuração de firewall e melhora o desempenho ao eliminar regras ineficientes
- Analisa a conformidade de políticas para exposições de tráfego da rede, topologia e vulnerabilidades

QRadar® Risk Manager

Solidifica 3. Desenvolver com segurança e auditar aplicativos web

Teste Automático de Segurança de Aplicativos

1. Varrer aplicativos
2. Analisar resultados
3. Corrigir problemas

*80% dos custos de desenvolvimento são gastos na identificação e correção de defeitos!**

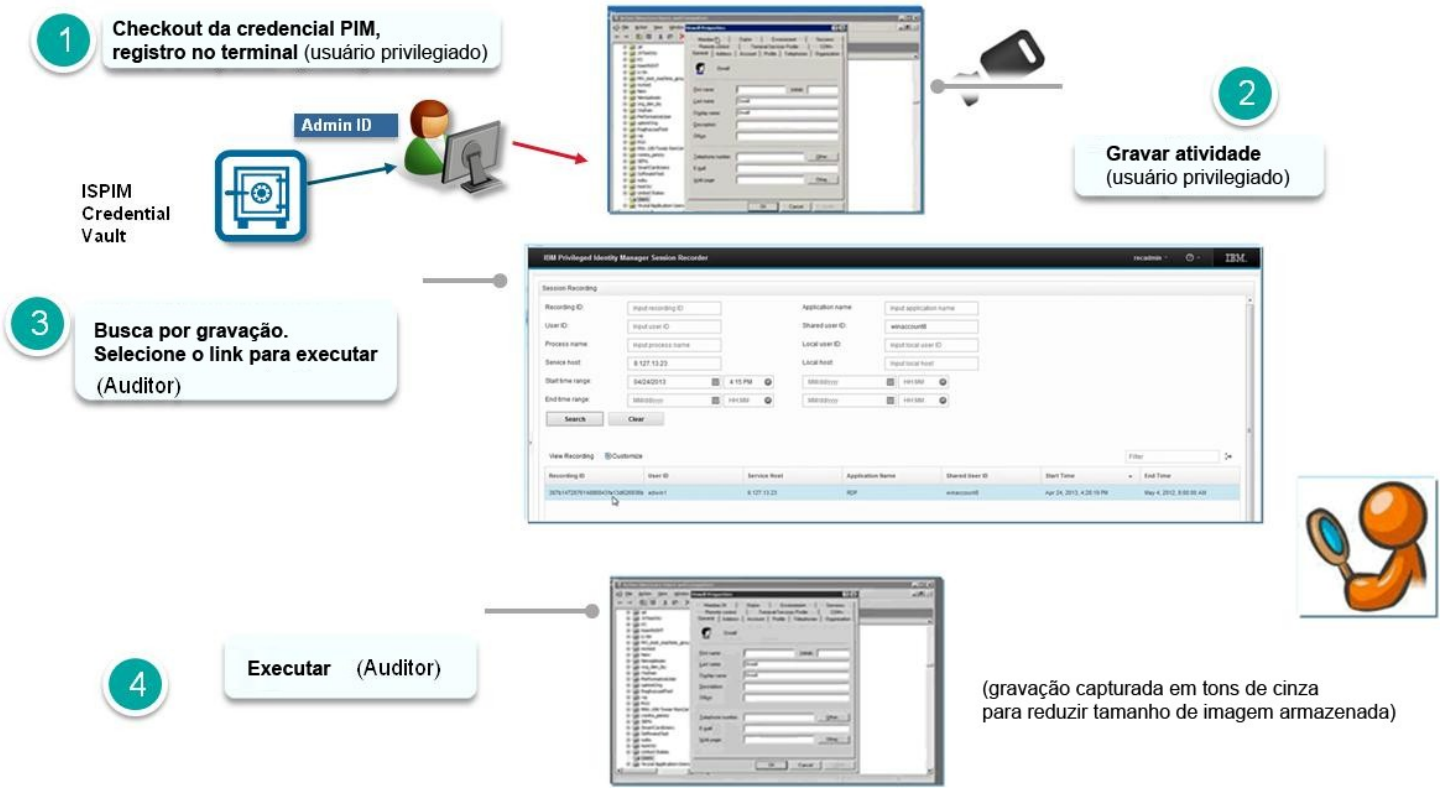
Como o IBM Security AppScan ajuda

- Inclue a segurança no processo de desenvolvimento do aplicativo
- Trata dos defeitos de segurança de maneira eficiente e eficaz antes da implementação
- Aproveita as várias tecnologias de varredura para a descoberta e correção de problemas por todas as equipes de segurança e desenvolvimento

Trate as vulnerabilidades de forma proativa no início do processo de desenvolvimento para reduzir custos

*Fonte: National Institute of Standards and Technology

Solidifica 4. Controlar atividades privilegiadas e identidades compartilhadas



Como o IBM Security Privileged Identity Manager ajuda

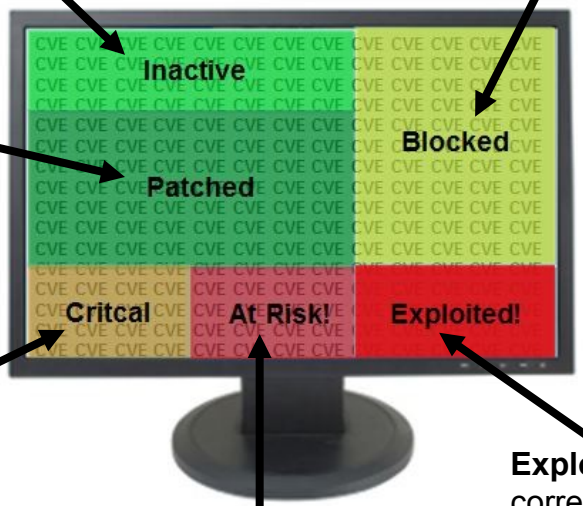
- Elimina a necessidade de compartilhar senhas através do gerenciamento automatizado de identidades privilegiadas
- Garante o suporte a conformidade e auditoria com gravação de sessão e suporte a reprodução
- Controles robustos de autenticação e SSO para acesso a contas de alto risco

Solidifica 5. Varrer com inteligência e priorizar vulnerabilidades

Inativo: Dados do QFlow Collector ajudam o QRadar Vulnerability Manager a perceber a atividade dos aplicativos

Bloqueado: O QRadar Risk Manager ajuda o QVM a entender quais vulnerabilidades estão bloqueadas por firewalls e IPSs

Corrigido: O IBM Endpoint Manager ajuda o QVM a entender quais vulnerabilidades serão corrigidas



Crítico: Base de conhecimento de vulnerabilidades, fluxo de reparos e políticas QRM informam ao QVM sobre vulnerabilidades críticas do negócio

Exploradas: A correlação SIEM e dados IPS ajudam o QVM a revelar quais vulnerabilidades foram exploradas

Em risco: O X-Force Threat e os dados SIEM de incidentes de segurança, unidos à visibilidade de tráfego de rede Qflow, ajudam o QVM a ver ativos se comunicando com potenciais ameaças.

Como o IBM QRadar ajuda

- Executa varreduras de vulnerabilidade de rede em tempo real
- Fornece visualização completa de vulnerabilidades incluindo feeds de dados de inteligência de ameaças e de scanner de terceiros
- Suporta processos de exceções e reparos com relatórios e painéis perfeitamente integrados
- Inclui o X-Force Threat Intelligence e rastreia dados do CVE (National Vulnerability Database)

QRadar Vulnerability Manager

Detecta

O que o Relatório de Tendências X-Force nos diz:

MÍDIA SOCIAL ESTÁ SENDO USADA PARA ABUSAR DA CONFIANÇA	*"Ataques sociais, que são mais humanos e pessoais, podem ser criados para se referirem a tópicos relevantes de interesse e eventos atuais"*
DIVERSOS "DIAS-ZERO" NOS PRIMEIROS 180 DIAS	*"Nos primeiros seis meses do ano, diversas vulnerabilidades de "dia-zero" afetando amplamente o software implementado, já haviam sido difundidas"*
A EXTRAÇÃO DE DADOS É O OBJETIVO	*"2012 foi um ano recorde para violação de dados reportados e 2013 está em via de ultrapassar 2012"*

Detecta

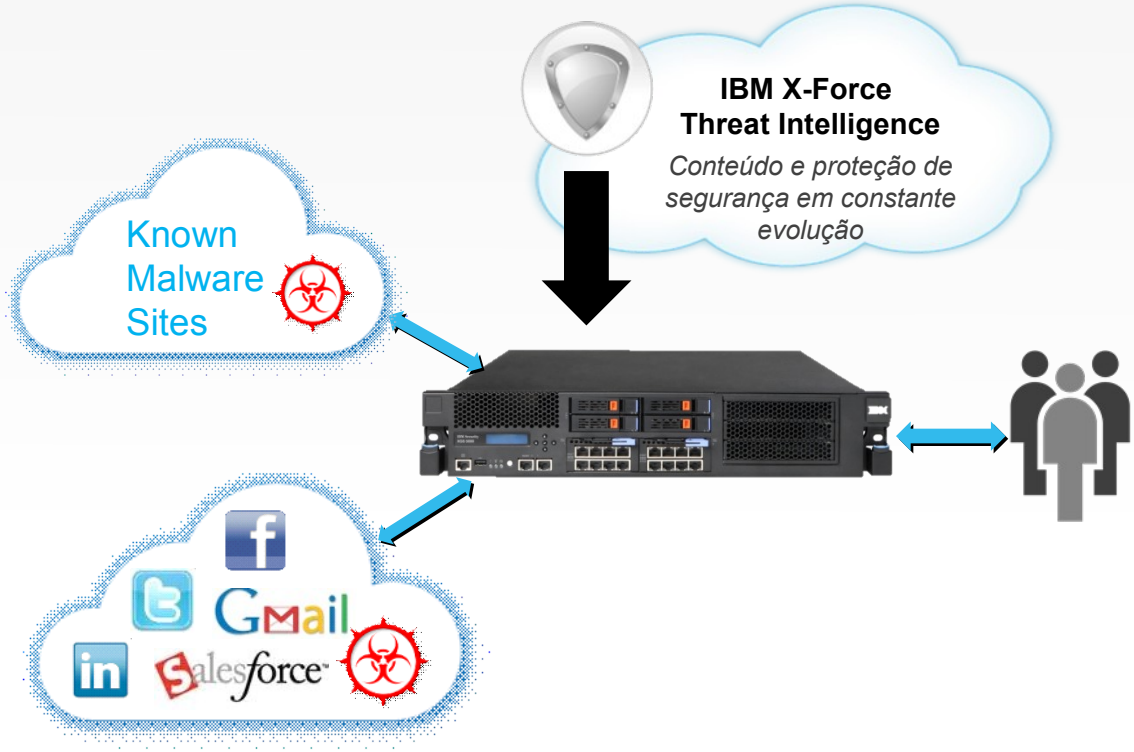
Exemplo de Melhores Práticas:

1. Gerenciar mídia social e risco de utilização da web
2. Proteger contra vulnerabilidades desconhecidas de "dia-zero"
3. Monitorar atividades de dados de acessos suspeitos
4. Identidade sensível a ameaças e políticas de acesso

Detecta 1. Gerenciar mídia social e risco de utilização da web

IBM Security Network Protection

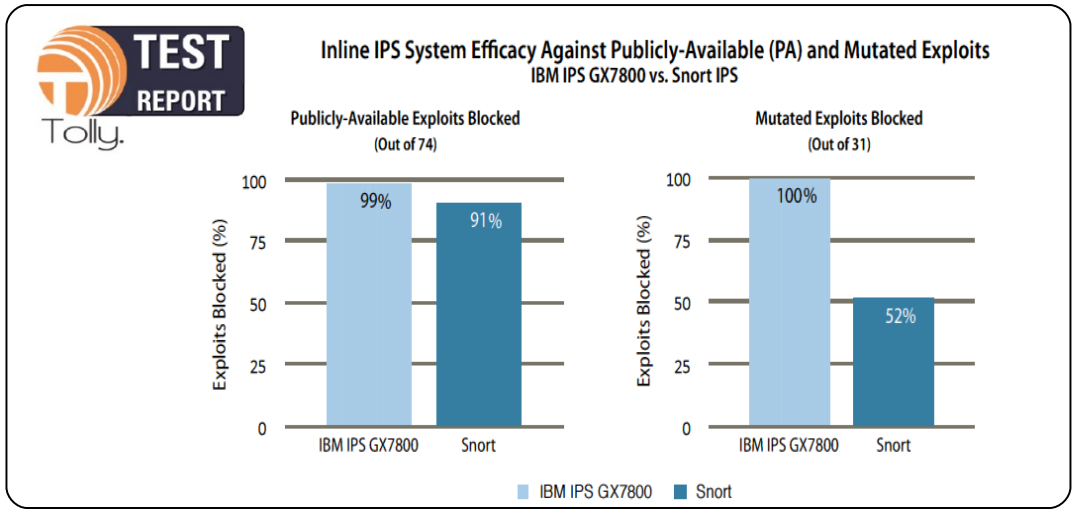
bloqueia o acesso de mensagens de phishing e links maliciosos incorporados



Como o IBM XGS ajuda

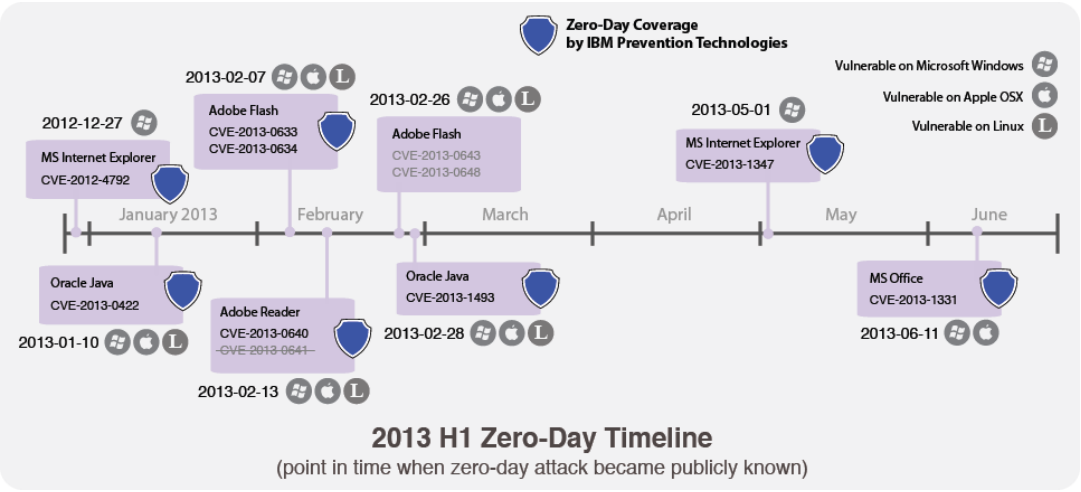
- Capacidade de controlar granularmente quais sites de mídia social são acessados a partir da rede
- Bloqueio dinâmico de usuários tentando acessar sites de malware conhecidos
- Abordagem de camada dupla para phishing ao limitar o acesso de mensagens de phishing, assim como bloquear acesso a links maliciosos
- Atualizado constantemente com a mais recente inteligência de ameaça na web do X-Force

Detecta 2. Proteger contra vulnerabilidades desconhecidas de "dia-zero"



Como o IBM IPS ajuda

- Utiliza abordagem baseada em protocolo para capturar muitos ataques "dia-zero" e ameaças mutantes versus IPS somente assinatura
- Oferece proteção contra vulnerabilidades conhecidas quando uma correção está indisponível ou implementado usando uma “correção virtual”
- Proteções java específicas como o módulo Java Heuristics trata de applets java maliciosos



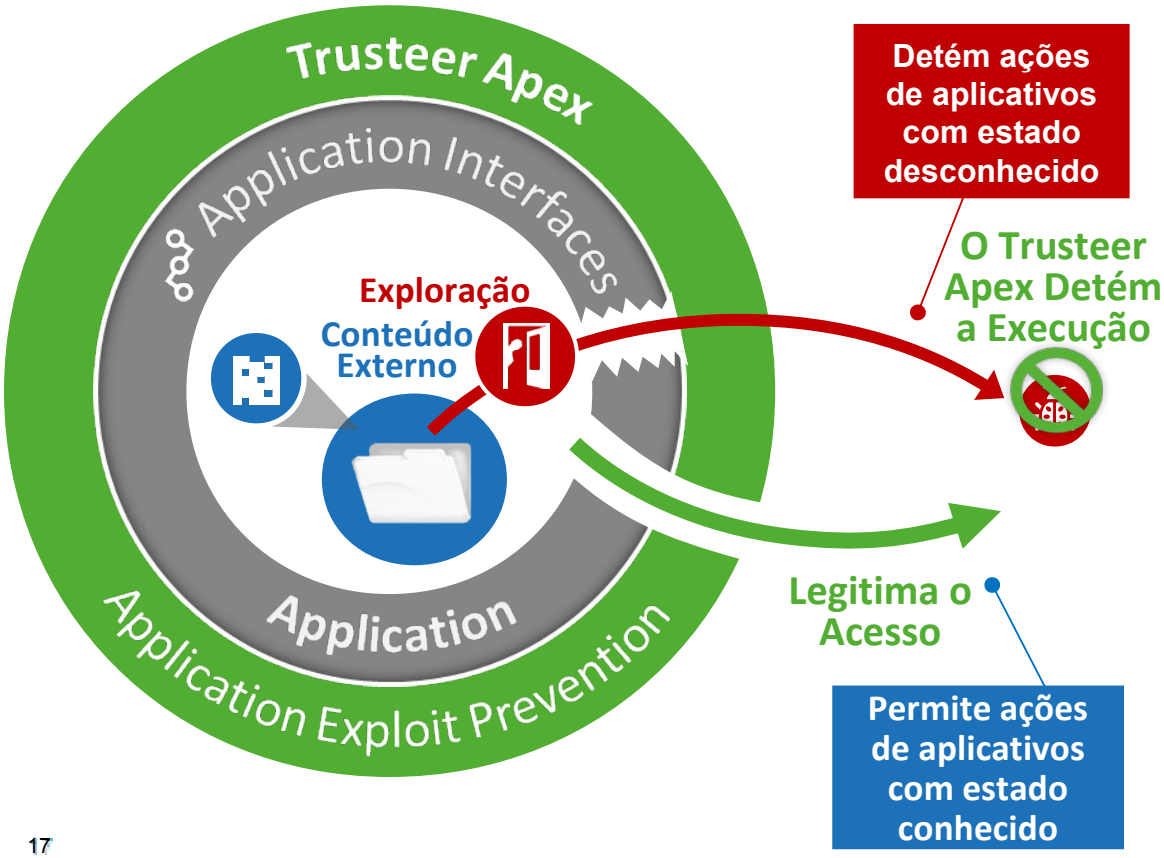
16 Fontes: Tolly Group, October 2012, IBM X-Force Research and Development Team

Detecta 2. Proteger contra vulnerabilidades desconhecidas de "dia-zero"

Controle estável de aplicativo

Determina se uma ação de um aplicativo é legítima ou maliciosa com base em:

- **o que** um aplicativo está fazendo (operação)
- **por que** está fazendo (estado)

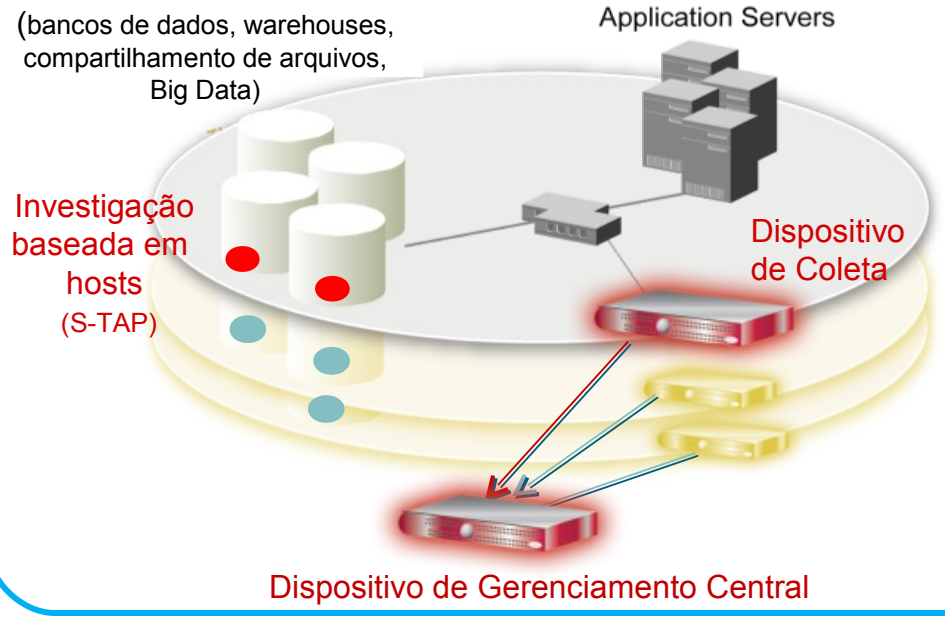


Como o Trusteer Apex ajuda

- Detecta e impede um malware de roubo de informações de terminais de funcionários
- Protege aplicativos que processam conteúdo não confiável incluindo: Navegadores de web, Adobe Acrobat, Flash, Java e MS-Office
- Unifica a proteção contra malware para terminais gerenciados e não gerenciados através de um único console baseado em web

Detecta 3. Monitorar atividades de dados de acessos suspeitos

Assegura a integridade de dados confidenciais



- ✓ Monitoramento contínuo em tempo real baseado em política de todas as atividades de tráfego de dados, incluindo ações por usuários privilegiados
- ✓ Varredura da infraestrutura de dados por correções ausentes, privilégios mal configurados e outras vulnerabilidades
- ✓ Automação da conformidade de proteção de dados

Como o IBM Guardium ajuda

- Impede alterações não autorizadas de dados, estruturas de bancos de dados, arquivos de configuração e registros
- Automatiza e centraliza os controles através de diversas regulações, tais como PCI-DSS, regulamentos de privacidade de dados, HIPAA/HITECH, etc.
- Protege dados em ambientes heterogêneos tais como bancos de dados, aplicativos, data warehouses e plataformas de Big Data como o Hadoop

Detecta 4. Identidade sensível a ameaças e políticas de acesso

Operações de Acesso	Conceder/ Negar
Um usuário autorizado solicita acesso ao portal e SSO	Conceder
A senha é roubada, a sessão é interceptada e o conteúdo HTTP é comprometido.	Negar
O conteúdo HTTP contém vulnerabilidades tais como SQL injection, cross-site scripting, falsificação de solicitação entre sites	Negar
O endereço IP possui uma baixa pontuação de reputação e local geográfico permitido	Negar
Reforçar a autenticação aprofundada ou acesso baseado em contexto para restaurar o acesso do usuário autorizado	Conceder

Como o IBM Access Manager Ajuda

- Validar identidade do cliente interagindo por meio de canais móveis e sociais
- Reforçar o contexto da identidade para acesso SaaS e Cloud
- Mitigar roubo de credenciais e tomada de contas com prevenção de fraudes
- Assegurar o acesso e proteger o conteúdo contra ataques direcionados

✓ Estender a proteção a ameaças para suportar o X-Force com base na reputação do IP e localização geográfica

Analisa

O que o Relatório de Tendências X-Force nos diz:

MANTER VISIBILIDADE GLOBAL

"Uma onda de violações de dados dirigida a filiais internacionais e franquias e sites de idioma local que nem sempre estão protegidos pelos mesmos padrões da matriz"

MESMO OS USUÁRIOS AVANÇADOS SÃO VULNERÁVEIS

"Ao comprometer um site central confiável e usando-o para servir malware, os invasores são capazes de alcançar mais vítimas tecnicamente experientes"

ENCONTRANDO SUTILEZAS NAS DISTRAÇÕES

"Ataques DDoS (Distributed Denial-of-Service) estão sendo utilizados como distração, permitindo que os invasores rompam outros sistemas na corporação"

Analisa

Exemplo de Melhores Práticas:

1. Obtenham uma abordagem holística e integrada da segurança de TI

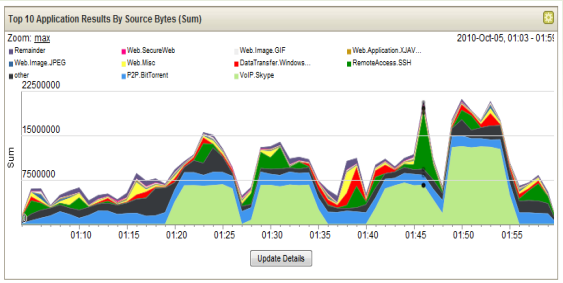
2. Analisem ameaças desconhecidas e atividade incomum

Analisa 1. Obter uma abordagem holística e integrada da segurança de TI

- Solução avançada de inteligência em segurança que analisa dados massivos de segurança e entrega informações para tomada de ação
- Correlação de registros, eventos, fluxos de rede, vulnerabilidades e inteligência de ameaças
- Inteligência com contexto de identidade e acesso
- Plataforma totalmente integrada que torna a busca, montagem de tabelas e investigação mais fáceis e rápidas
- Regras e relatórios prontos para uso imediato

Como o IBM QRadar ajuda

- Determina os padrões típicos de utilização para usuários, aplicativos de rede e acesso a dados
- Monitora e alerta sobre desvios significativos, fornecendo visibilidade do comportamento não autorizado
- Ajusta-se para tendências de sazonalidade e crescimento
- Está correlacionado com a inteligência de ameaças X-Force



Analisa 2. Analisar ameaças desconhecidas e atividade incomum

Offense 3063 — Summary | Attackers | Targets | Categories | Annotations | Networks | Events | Flows | Rules | Actions | Print

Magnitude				Relevance	0	Severity	8	Credibility	3
Description	Target Vulnerable to Detected Exploit preceded by Exploit Attempt Proceeded by Recon preceded by Exploit/Malware Events Across Multiple Targets preceded by Recon - External - Potential Network Scan		Event count	1428 events in 3 categories			
Attacker/Src	202.153.48.66		rt	2009-09-29 16:05:01			
Target(s)/Dest	Local (717)		ation	1m 32s			
Network(s)	Multiple (3)		igned to	Not assigned			
Notes	Vulnerability Correlation Use Case Illustrates a scenario involving correlation of vulnerability data with IDS alerts An attacker originating from China (202. ... g the Conficker worm exploit (CVE 2008-4250). The first sys...						

Qual foi o ataque?

Foi bem-sucedido?

Attacker Summary — Details

Magnitude		User	
Description	202.153.	Asset Name	Unknown
Vulnerabilities	0	MAC	Unknown
Location	China	Asset Weight	0

Quem foi o responsável?

Onde eu os encontro?

Top 5 Categories — Categories

Name	Magnitude	Local Target Count	
Buffer Overflow		8	
Misc Exploit		3	
Network Sweep		716	1417

Quantos alvos estão envolvidos?

Quão valiosos são os alvos para o negócio?

Top 5 Local Targets — Targets

IP/DNS Name	Mag..			User	MAC	Location	Weight
Windows AD Server		Un		Unknown	Unknown	main	0
10.101.3.3		Unknown	No	Unknown	Unknown	main	0
10.101.3.4		Unknown	No	Unknown	Unknown	main	0
DC106		Yes	No	Administr		main	10
10.101.3.11		Unknown	No	DCAdmin		main	0

Algum deles é vulnerável?

Top 10 Events — Events

Event Name	Magnitude	Log Source	Category	Destination	Dst Port	Time
Misc Exploit - Event CRE		Custom Rule Engine-8 :: qradar-vm	Misc Exploit	10.101.3.15	445	09-29 16:06:33
NETBIOS-DG SMB v4 srvsvc NetrpPathCo...		Snort @ 10.1.1.5	Buffer Overflow	10.101.3.10	445	09-29 16:06:28
NETBIOS-DG SMB v4 srvsvc NetrpPathCo...		Snort @ 10.1.1.5		01.3.15	445	09-29 16:06:33
Misc Exploit - Event CRE		Custom Rule Engine-8 :: qradar-vm		01.3.13	445	09-29 16:06:31
Network Sweep - QRadar Classify Flow		Flow Classification Engine-5 :: qradar-v		01.3.10	445	09-29 16:05:01
Network Sweep - QRadar Classify Flow		Flow Classification Engine-5 :: qradar-v		01.3.15	445	09-29 16:05:01
Network Sweep - QRadar Classify Flow		Flow Classification Engine-5 :: qradar-v		01.3.10	445	09-29 16:05:01
Network Sweep - QRadar Classify Flow		Flow Classification Engine-5 :: qradar-v		01.3.15	445	09-29 16:05:01

Onde está toda a evidência?

Corrige

O que o Relatório de Tendências X-Force nos diz:

A IMAGEM GLOBAL DA MARCA PODE SER IMPACTADA RAPIDAMENTE

"Ataques operacionais sofisticados denegriram marcas bem conhecidas. Isto pode danificar a reputação de uma marca e criar problemas legais se dados do cliente vazarem"

POSSUIR PLANO PARA TECNOLOGIAS EMERGENTES

"Invasores estão investindo em malwares móveis tecnicamente sofisticados que são mais resilientes e perigosos"

Corrige

Exemplo de Melhores Práticas:

1. Possuir plano e processos para executar quando a violação for descoberta

2. Utilizar investimentos em segurança para corrigir rapidamente e solidificar o ambiente

Corrige 1. Possuir plano e processos para executar quando a violação for descoberta

Serviços IBM de Resposta às Emergências

•Permite uma resposta mais rápida aos incidentes, com custos e riscos reduzidos

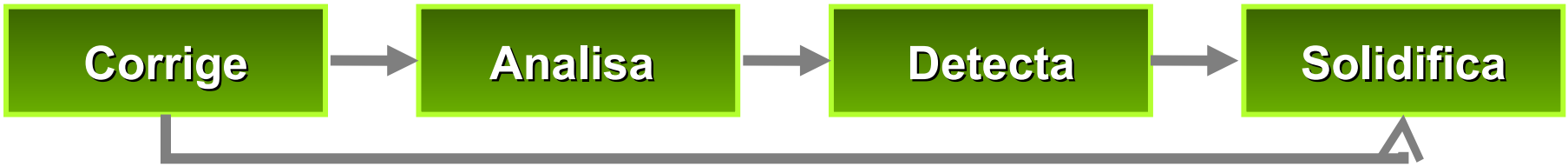
Acesso 24 horas a analistas de resposta a emergências altamente qualificados para ajudar a interromper ataques em andamento, reduzir o seu impacto, permitir uma rápida recuperação e executar uma detalhada análise forense de dados.

Se você está experimentando uma emergência de segurança, ligue:
1-888-241-9812 nos EUA
(001) 312-212-8034 Fora dos EUA

Como a IBM ajuda

- Ajuda a reduzir os riscos e a exposição às ameaças virtuais por meio de uma abordagem preventiva e proativa.
- Fornece acesso aos principais recursos que podem permitir uma rápida recuperação e ajuda a reduzir impacto decorrente de incidentes nos negócios
- Permite uma visão mais ampla e uma compreensão mais detalhada dos incidentes, utilizando dados de inteligência e analítica.

Corrige 2. Utilizar investimentos em segurança para corrigir rapidamente e solidificar o ambiente



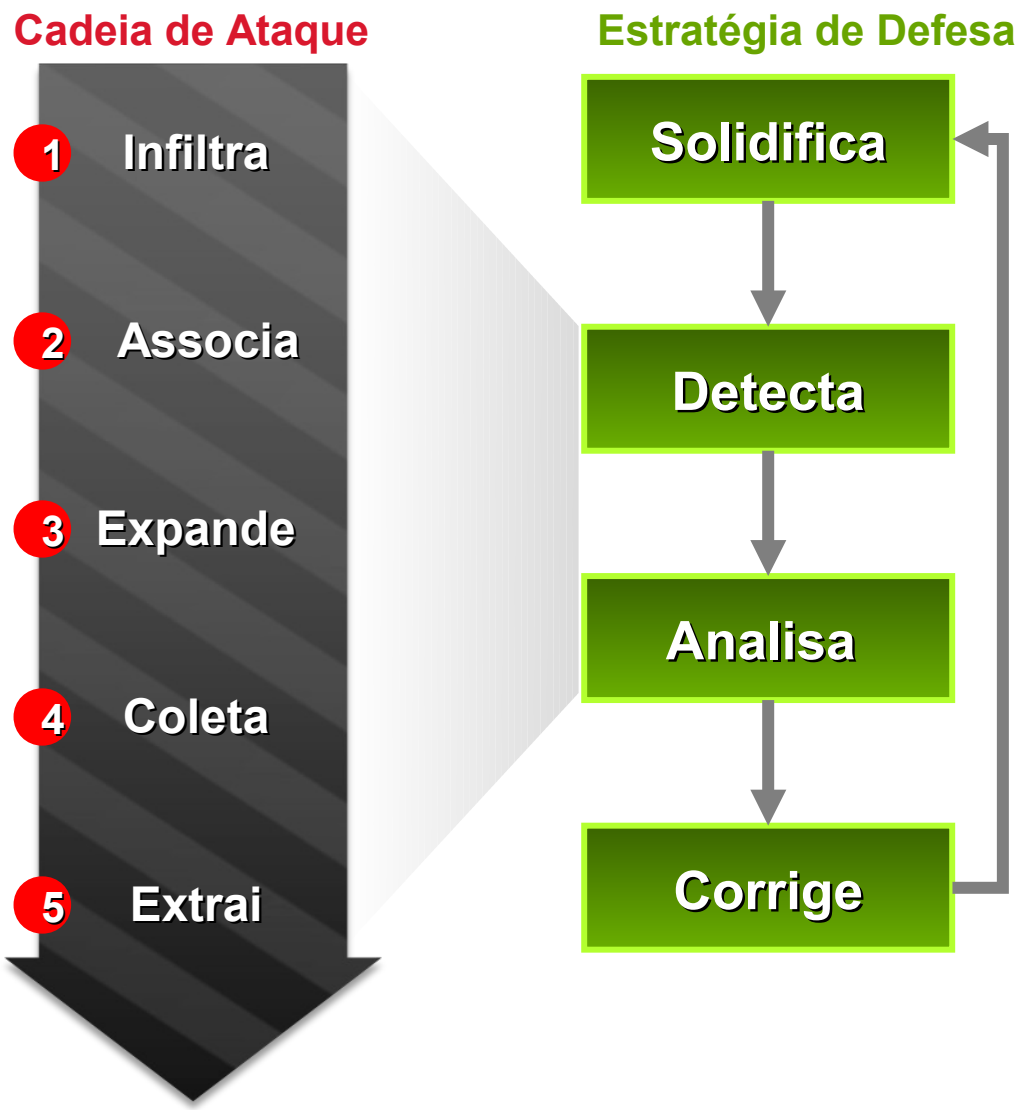
- Resposta a Emergências Serviço de (ERS)
- Bloqueio de Correção Virtual
- Quarentena
- Remoção de malware
- Reparo rápido – alteração de configuração, aplicar correção
- Limpar dados corporativos de dispositivo móvel
- Desabilitar o acesso

- Simulação de caminho de ataque
- Inteligência global de ameaças
- Inserir nova regra de análise
- Incorporar dados adicionais de ameaças
- Auditar atividade de aplicativos e usuários para suportar investigações de perícia forense

- Prevenção contra invasão
- Detecção de anomalia de rede
- Bloquear comandos de segurança não conformes
- Bloquear usuários na abertura de documentos infectados
- Monitorar eventos de mainframe para anomalias
- Treinar usuários sobre ataques a mídias sociais

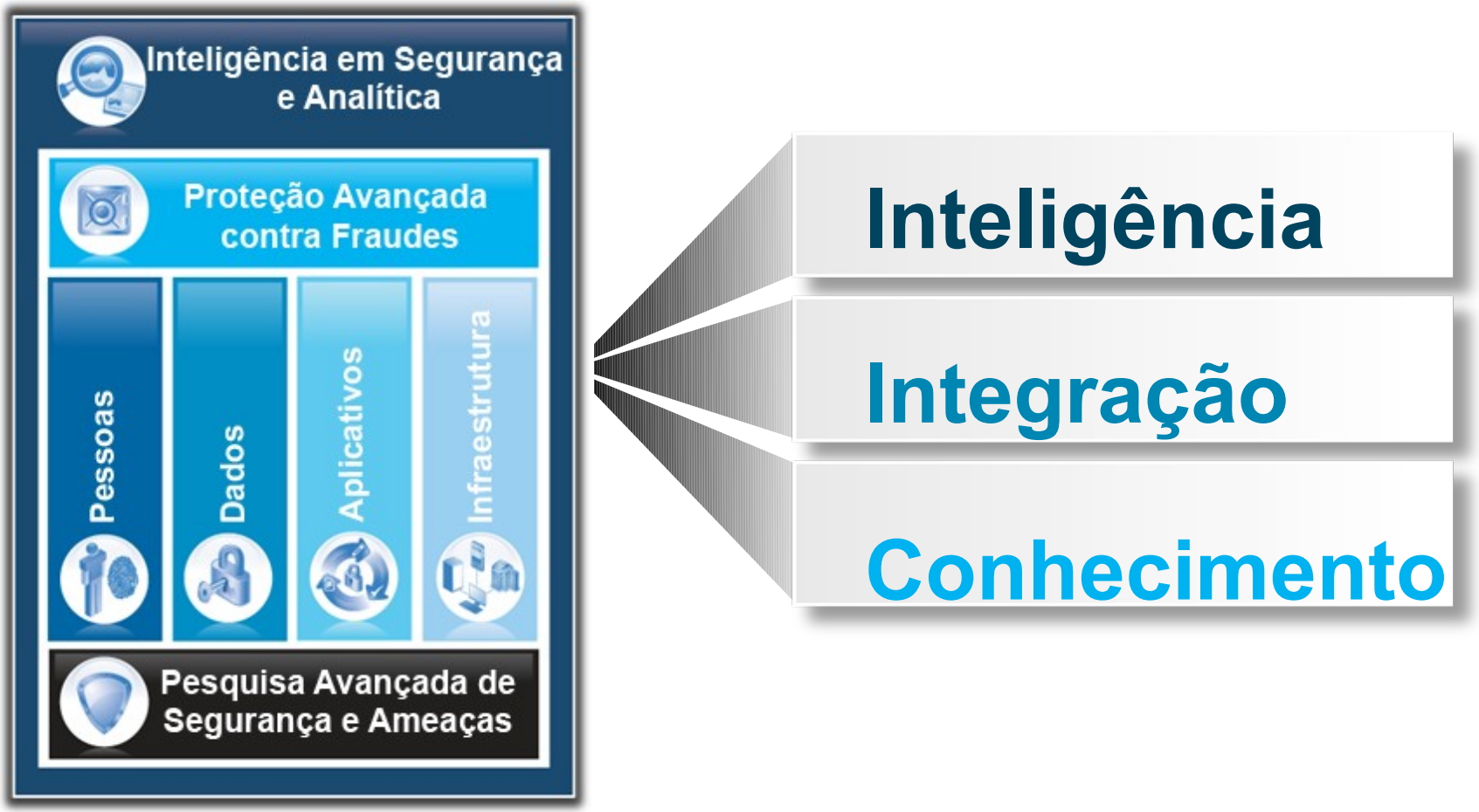
- Conformidade de correção
- Varredura de aplicativo da web
- Atualizar aplicativos de terceiros
- Auditar contas privilegiadas
- Rastrear o uso de identidades compartilhadas
- Reforçar políticas de senha

Resumo – Quebrando a cadeia de ataque



- Adotar diligência nas correções, monitorar configurações de rede, auditar aplicativos da web e controlar identidades privilegiadas.
- Ter uma estratégia de mídias sociais e de web, proteção contra vulnerabilidades desconhecidas e de "dia-zero", monitorar bancos de dados e acesso baseado em risco.
- Implementar um sistema abrangente de integração para visão holística e análise de ambiente.
- Estabelecer um plano de ação para o caso de violações e ajustar pontos de controle para melhorar a segurança.

Segurança IBM: Entregando inteligência, integração e experiência através de uma estrutura abrangente



Declaração de Práticas Adequadas de Segurança: O sistema de segurança de TI envolve a proteção de sistemas e informações através de prevenção, detecção e resposta ao acesso incorreto de dentro e fora de sua empresa. O acesso incorreto pode resultar na alteração, destruição ou desapropriação de informações, ou pode resultar em danos ou uso impróprio de seus sistemas, inclusive para atacar terceiros. Nenhum produto ou sistema de TI deve ser considerado completamente seguro e nenhum produto único ou medida de segurança pode ser totalmente eficaz na prevenção de acesso incorreto. Os sistemas e produtos IBM foram projetados para fazer parte de uma abrangente abordagem de segurança, que necessariamente envolverá procedimentos operacionais adicionais e pode exigir que outros sistemas, produtos ou serviços se tornem mais efetivos. A IBM NÃO GARANTE QUE OS SISTEMAS E PRODUTOS SEJAM IMUNES À CONDUTA ILEGAL OU MALICIOSA DE QUALQUER PARTE.

Obrigado

www.ibm.com/security