Gestão de Incidentes em tempo real: Estratégias para respostas ágeis e eficientes

Agenda

TLP:CLEAR

- Abertura e Introdução.
- O que é Gestão de Incidentes em Tempo Real?
- Estratégias e Boas Práticas.
- Tecnologias e Automação no Processo de Resposta.
- Aplicação de IA e Machine Learning para detecção e resposta automática.

Abertura e Introdução

TLP:CLEAR

Nos ambientes organizacionais modernos, caracterizados por operações cada vez mais dependentes de tecnologia e conectividade, a **gestão de incidentes em tempo real** tornou-se um pilar essencial para garantir a continuidade dos negócios e a proteção contra impactos negativos.

➢ **Acelerando Respostas e Minimizando Impactos**

Incidentes podem surgir de diversas formas: falhas técnicas, ataques cibernéticos, interrupções de serviços, ou erros humanos. A capacidade de identificar, responder e mitigar esses problemas **em tempo real** é crucial para:

- ❑ **Minimizar impactos financeiros**: Reduzir perdas de receita associadas a períodos de inatividade.
- ❑ **Preservar a experiência do cliente**: Resolver falhas rapidamente evita danos à reputação e perda de confiança.
- ❑ **Garantir conformidade regulatória**: Muitos setores exigem resposta imediata para mitigar riscos e proteger dados sensíveis.
- ❑ **Reduzindo o Tempo de Inatividade:**
- ❑ Reduzir significativamente o tempo médio de recuperação (MTTR – Mean Time to Recovery).
- ❑ Detectar e conter incidentes antes que eles se transformem em problemas maiores.

O que é Gestão de Incidentes em Tempo Real?

TLP:CLEAR

Gestão Reativa

Definição:

A gestão reativa é uma abordagem em que ações e decisões são tomadas **somente após um problema ou incidente ter ocorrido**.
O foco principal é a resolução de problemas no momento em que surgem, sem planejamento ou antecipação prévia.

Características da Gestão Reativa:

Responde aos problemas conforme eles aparecem.
Geralmente não há planejamento para incidentes específicos.
Pode levar a decisões rápidas e improvisadas.
Tende a ser mais cara e demorada, devido à falta de preparo.
Foco na **contenção e reparação** do dano causado pelo problema.

Exemplo de Gestão Reativa:

Um sistema crítico apresenta falhas, e a equipe só age após as operações serem interrompidas e os usuários reclamarem. A solução é implementada no momento, mas sem prevenir que o problema ocorra novamente.

O que é Gestão de Incidentes em Tempo Real?

TLP:CLEAR

Gestão Proativa

Definição:

A gestão proativa é uma abordagem em que ações são planejadas e executadas **antes que os problemas ocorram**, com o objetivo de prevenir falhas e minimizar riscos. Envolve antecipação e preparação para possíveis cenários críticos.

Características da Gestão Proativa:

Baseia-se na prevenção de problemas, em vez de reagir a eles.
Utiliza monitoramento constante e análise de dados para identificar possíveis falhas.
Envolve planejamento, treinamento e implementação de medidas de segurança.
Mais eficiente a longo prazo, reduzindo custos e interrupções.
Foco em **prevenção e melhoria contínua**.

Exemplo de Gestão Proativa:

A equipe realiza manutenções preventivas regulares em sistemas críticos, identificando e corrigindo potenciais falhas antes que afetem as operações.

O que é Gestão de Incidentes em Tempo Real?

TLP:CLEAR

Diferenças

Aspecto	Gestão Reativa	Gestão Proativa
Foco	Resolver problemas após sua ocorrência.	Prevenir problemas antes que ocorram.
Ação	Resposta imediata e corretiva.	Planejamento e ações preventivas.
Custo	Normalmente maior devido a danos inesperados.	Normalmente menor, com custos controlados.
Tempo de Resposta	Mais lento, pois exige diagnóstico no momento do problema.	Mais rápido, pois há planos previamente definidos.
Planejamento	Pouco ou nenhum planejamento.	Baseado em análise de riscos e antecipação.
Impacto no Negócio	Pode causar interrupções significativas.	Minimiza interrupções e garante continuidade.

O que é Gestão de Incidentes em Tempo Real?

TLP:CLEAR

Exemplos de incidentes críticos que exigem respostas em tempo real:

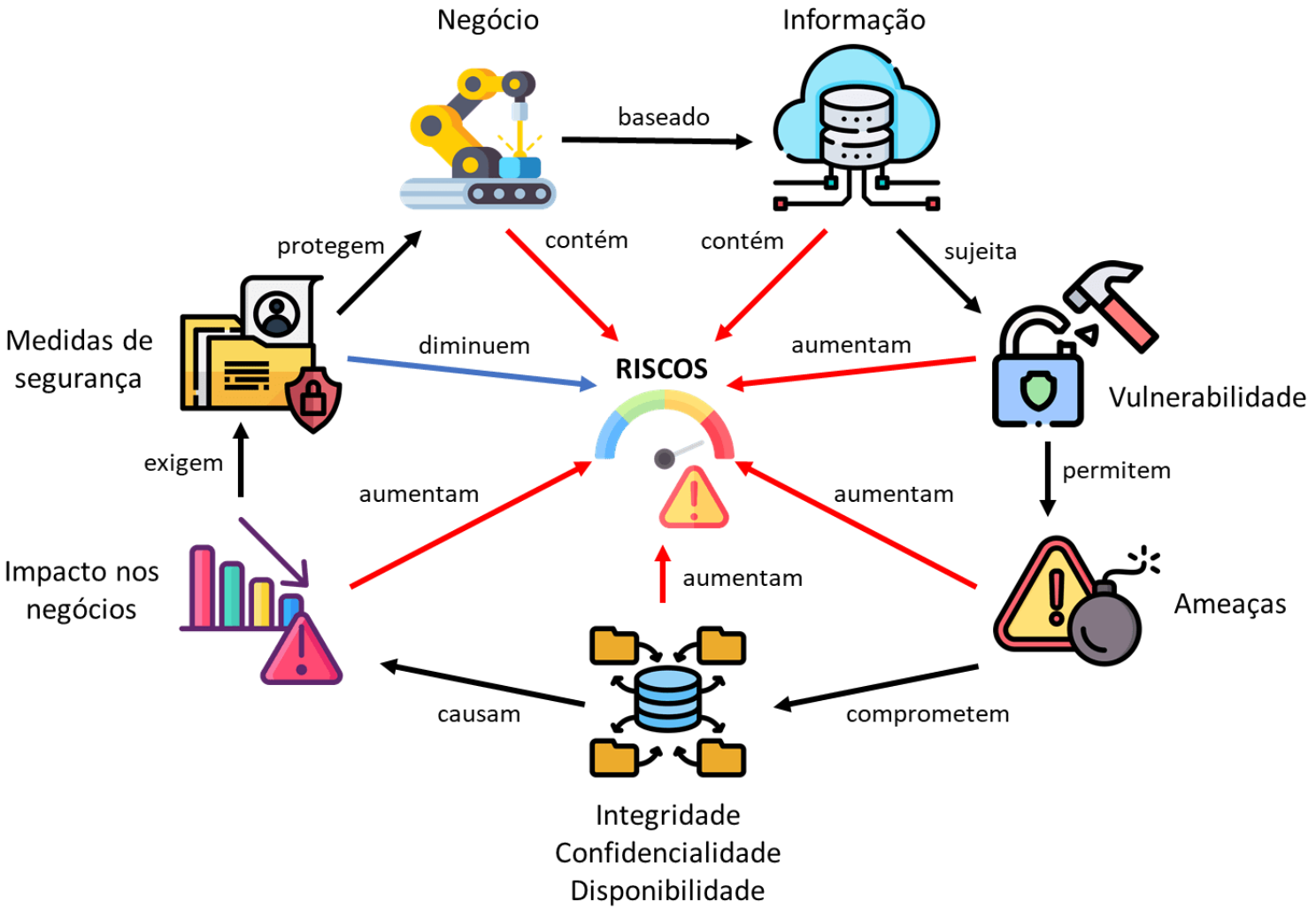
- Ransomware
- Phishing em massa
- DDoS (Ataque de Negação de Serviço Distribuído)
- Exfiltração de dados

O que é Gestão de Incidentes em Tempo Real?

TLP:CLEAR

Desafios

- Detecção Rápida e Precisa de Incidentes
- Comunicação e Coordenação Eficientes
- Priorização Adequada dos Incidentes
- Capacitação Contínua da Equipe
- Uso Eficiente de Ferramentas Tecnológicas
- Documentação e Melhoria Contínua
- Adaptação a Novas Ameaças e Tecnologias



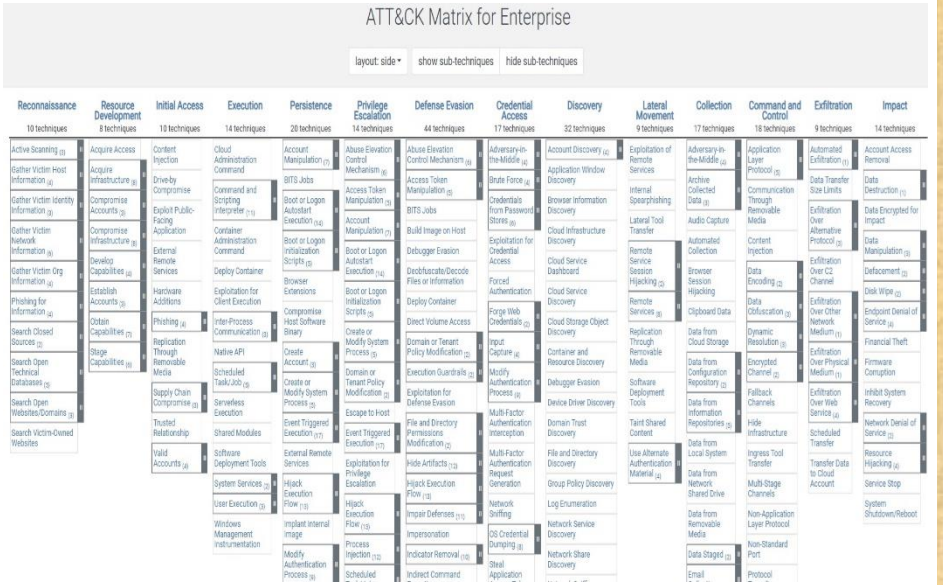
Estratégias e Boas Práticas

TLP:CLEAR

Para priorizar adequadamente os incidentes e identificar aqueles que são críticos, é necessário seguir um processo estruturado que envolve classificação, categorização e avaliação de impacto e urgência.

Classificação e Categorização de Incidentes

A classificação consiste em identificar o tipo específico de incidente e os componentes afetados.



Estratégias e Boas Práticas **TLP:CLEAR**

Avaliação de Impacto e Urgência

A priorização baseia-se principalmente em dois fatores:

- **Impacto**: Refere-se ao efeito do incidente nos negócios, medido pela extensão e gravidade das consequências.
  - ❑ Quantos usuários são afetados?
  - ❑ Quais serviços críticos estão comprometidos?
  - ❑ Há implicações legais ou de conformidade?
- **Urgência**: Indica a necessidade de resolução rápida, considerando o tempo disponível antes que o impacto se torne inaceitável.
  - ❑ O incidente está impedindo operações essenciais/críticas?
  - ❑ O que será afetado?
  - ❑ A indisponibilidade prolongada aumentará o impacto?

Combinando impacto e urgência, é possível determinar a prioridade do incidente. Uma ferramenta comum para isso é a **Matriz de Prioridade**, que cruza os níveis de impacto e urgência para definir a prioridade final.

Estratégias e Boas Práticas

TLP:CLEAR

ESTRATÉGIAS GERAIS

- revisar periodicamente a política de segurança da informação, de segurança cibernética ou equivalente;
- revisar periodicamente o plano estratégico de segurança dos ativos críticos da organização, além de manter atualizado o inventário desses ativos críticos;
- estabelecer um plano de gestão de backup que contemple o armazenamento seguro dos dados copiados e que sejam observadas questões para o backup tais como como estar isolado, offline, redundante, além de se realizar testes periódicos de recuperação de dados;
- possuir ambiente com virtualização de servidores, onde se considere a utilização de snapshots (preservando o estado e os dados de uma máquina virtual em um determinado momento), atualizados regularmente, de forma a viabilizar o rápido retorno de sistemas críticos quando necessário;
- estabelecer um plano de gestão de atualização de sistemas computacionais;
- implementar e revisar periodicamente a política de senhas da organização, obrigando que elas sejam fortes, que não possam ser repetidas quando trocadas, além de terem período de expiração razoável;
- mapear e rever os privilégios de usuários, implementando a política de privilégio mínimo;
- implementar um plano de segurança de acesso remoto da organização que contemple a utilização de VPN e duplo/múltiplo fator de autenticação, além da revisão periódica sobre a necessidade de acesso remoto para cada caso;
- implementar um plano de autenticação de sistemas que contemple a utilização de múltiplo fator de autenticação sempre que possível, além de gestão de acesso a usuários internos e externos, ativos ou afastados;
- manter registro de eventos de sistemas (logs) centralizado e em ambiente controlado;
- implementar plano de bloquear credenciais de funcionários ou colaboradores que estejam afastados (férias, licenças etc.);
- manter o sistema de gerenciamento contra malwares (antivírus) sempre atualizado, avaliando possíveis recomendações de melhoria que o produto ou fabricante possa oferecer;e
- estabelecer plano de conscientização do público interno sobre medidas de segurança quando da utilização do e-mail e rede corporativa, reforçando a necessidade de comunicação à equipe de prevenção, tratamento e resposta a incidentes cibernéticos (ETIR) local em caso de suspeita de incidentes.

Estratégias e Boas Práticas

TLP:CLEAR

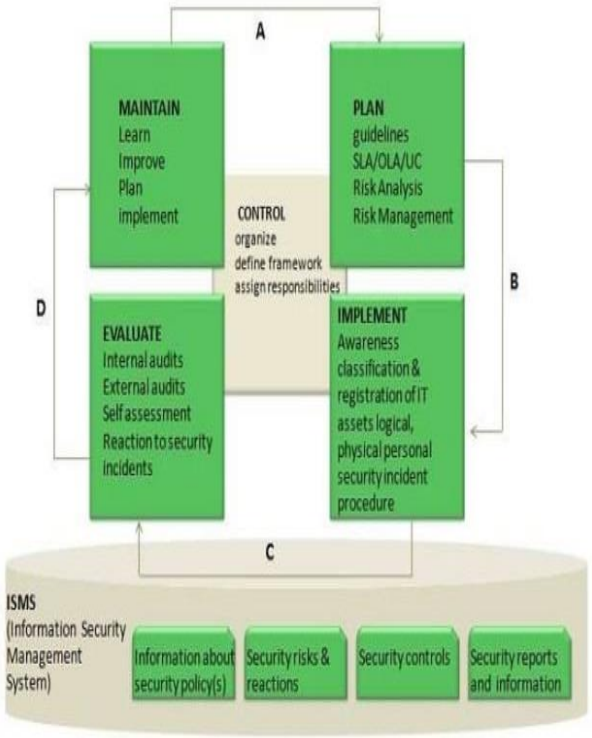
ESTRATÉGIAS PARA UTILIZAÇÃO DE VPN

- Exigir a utilização de Autenticação Multifator (MFA) para todas as credenciais de VPN;
- Definir o escopo de acesso de rede para cada perfil de usuário da VPN;
- Implementar, quando possível e viável, a segregação de rede virtual em cada conexão de VPN;
- Bloquear acesso via VPN às interfaces administrativas de serviços críticos;
- Forçar desautenticação por inatividade;
- Garantir a atualização de sistemas de VPN e assinaturas contra ameaças digitais nos endpoints;
- Implementar o princípio de privilégio mínimo que garanta que usuários tenham o nível mínimo de acesso necessário para cumprir suas tarefas; e
- Auditar acessos via VPN, especialmente eventos de login cujos endereços IP de origem sejam estranhos à rotina normal da organização ou registrados em horários fora do usual.

Estratégias e Boas Práticas

TLP:CLEAR

Metodologias Ágeis – ITIL / COBIT



Principais aspectos do ITIL que podem ser explorados para fortalecer a segurança da informação nas organizações:

1. Gerenciamento de Segurança da Informação (Information Security Management - ISM)
O ISM é uma prática central no ITIL dedicada a alinhar a segurança de TI com a segurança empresarial, garantindo que a segurança da informação seja gerida de forma eficaz em todas as atividades de serviço e gerenciamento de serviços;

2. Integração com o Ciclo de Vida do Serviço (A segurança da informação é incorporada em todas as fases do ciclo de vida do serviço);

Estratégia de Serviço (Service Strategy): Define políticas e estratégias de segurança alinhadas aos objetivos de negócio.
Desenho de Serviço (Service Design): Segurança como parte integral do design dos serviços, assegurando que os controles de segurança sejam incorporados.
Transição de Serviço (Service Transition): Garante que aspectos de segurança sejam considerados durante a transição de novos serviços ou mudanças.
Operação de Serviço (Service Operation): Foca no monitorando incidentes de segurança e respondendo a ameaças.
Melhoria Contínua de Serviço (Continual Service Improvement): Avalia e aprimora continuamente as práticas de segurança.

3. Gestão de Incidentes e Problemas

O ITIL enfatiza a importância de processos robustos de **Gestão de Incidentes** e **Gestão de Problemas** para lidar com eventos de segurança:
Gestão de Incidentes: Foca na restauração rápida dos serviços após um incidente de segurança, minimizando o impacto nos negócios.
Gestão de Problemas: Investiga as causas raiz dos incidentes de segurança para prevenir recorrências, implementando soluções permanentes.

4. Gestão de Acessos (Access Management)

Este processo assegura que apenas indivíduos autorizados tenham acesso a sistemas e informações, alinhando-se aos princípios de **least privilege** e **need-to-know**.

5. Gestão de Continuidade de Serviços de TI (IT Service Continuity Management)

Foca na preparação e resposta a eventos que podem interromper os serviços de TI, incluindo desastres naturais ou ataques cibernéticos. Desenvolve planos de continuidade e recuperação que asseguram a resiliência dos serviços e a proteção das informações críticas.

6. Melhoria Contínua de Serviço (Continual Service Improvement - CSI)

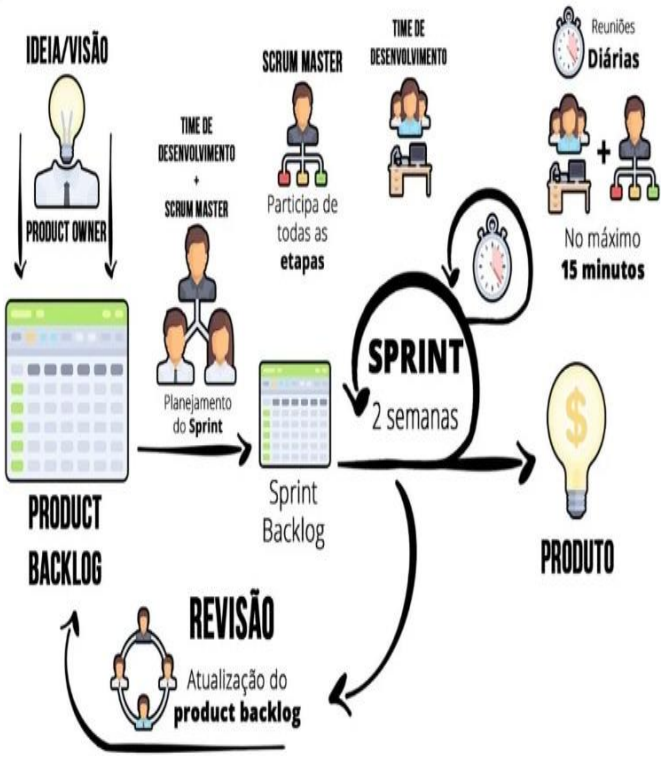
O CSI promove a avaliação regular dos processos de segurança, identificando áreas de melhoria e implementando mudanças para fortalecer a postura de segurança da organização. Utiliza métricas e indicadores de desempenho para monitorar a eficácia das práticas de segurança e garantir a conformidade com as políticas estabelecidas.

Ao integrar essas metodologias e funcionalidades do ITIL, as organizações podem estabelecer uma abordagem estruturada e proativa para a segurança da informação, alinhando as práticas de TI com os objetivos de negócio e garantindo a proteção contínua dos ativos de informação.

Estratégias e Boas Práticas

TLP:CLEAR

Metodologias Ágeis - SCRUM



O **Scrum** é um framework ágil amplamente utilizado no desenvolvimento de software, caracterizado por ciclos iterativos e incrementais chamados de *sprints*., como pode ser explorado para fortalecer a segurança da informação:

1. Integração de Requisitos de Segurança no *Product Backlog*:
No Scrum, o *Product Backlog* é uma lista priorizada de funcionalidades, melhorias e correções que devem ser implementadas no produto para garantir segurança em aspectos como autenticação, autorização e criptografia e identificar possíveis cenários de ataque incorporando-os como itens do *Backlog*, permitindo que a equipe desenvolva defesas apropriadas.

2. Revisão de Segurança nas Reuniões de Planejamento de Sprint:
Avaliar os aspectos de segurança de cada item selecionado. E assegurar que as considerações de segurança sejam incorporadas desde o início do desenvolvimento de cada funcionalidade.

3. Implementação de *Sprints* Focados em Segurança:

- **Realizar Análises de Vulnerabilidades:** Identificar vulnerabilidades no código existente;
- **Conduzir Testes de Penetração:** Simular ataques para avaliar a robustez das defesas implementadas.
- **Atualizar Dependências e Bibliotecas:** Garantir que todas as dependências estejam atualizadas e livres de vulnerabilidades conhecidas.

4. Reuniões Diárias (*Daily Stand-ups*) com Foco em Segurança:
As reuniões diárias são oportunidades para a equipe discutir o progresso, identificar impedimentos, relatar preocupações, ameaças ou vulnerabilidades descobertas.

5. Revisão de Sprint com Ênfase em Segurança:
Mostrar como os requisitos de segurança foram atendidos nas novas funcionalidades.

6. Retrospectiva de Sprint com Foco em Melhoria Contínua da Segurança:

- Discutir o que funcionou bem e o que pode ser aprimorado em termos de segurança.
- Definir ações para melhorar a postura de segurança nos próximos Sprints.

7. Papéis e Responsabilidades Claras em Relação à Segurança

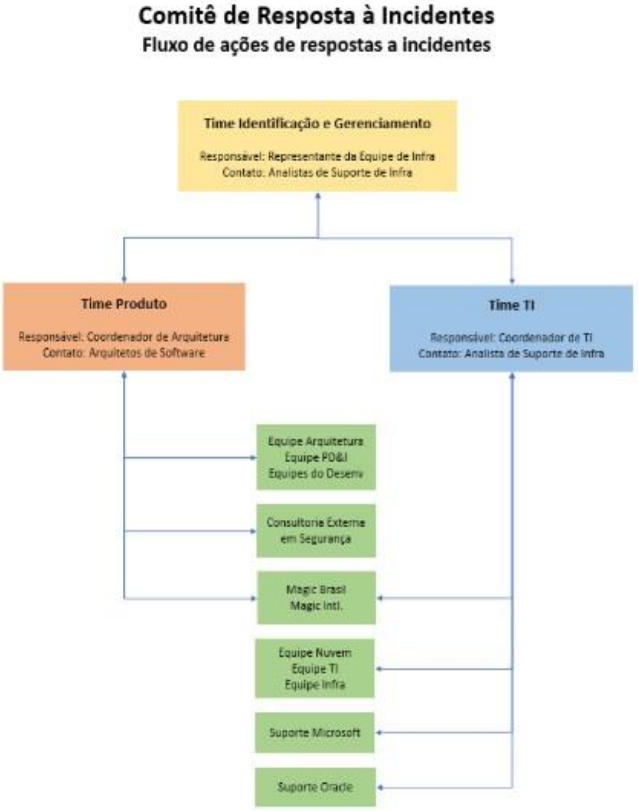
- **Product Owner**: Garantir que os requisitos de segurança estejam claramente definidos e priorizados no *Backlog*.
- **Scrum Master**: Assegurar que as práticas de segurança sejam seguidas pela equipe e remover impedimentos relacionados à segurança.
- **Equipe de Desenvolvimento**: Implementar as funcionalidades atendendo aos requisitos de segurança e realizar revisões de código focadas em identificar vulnerabilidades.

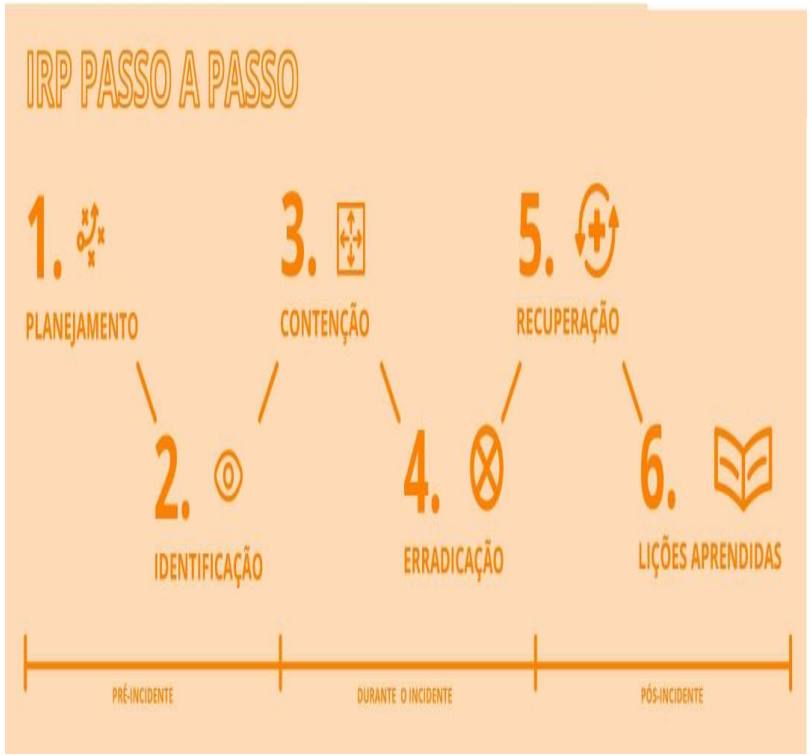
Ao integrar essas práticas no framework Scrum, as equipes podem desenvolver produtos que não apenas atendem às necessidades funcionais dos usuários, mas também mantêm um alto padrão de segurança, protegendo os dados e sistemas contra ameaças potenciais.

Tecnologias e Automação no Processo de Resposta

TLP:CLEAR

Definição de Papéis e Responsabilidades: A importância de um plano claro para a equipe.
Ferramentas de Suporte: Ferramentas integradas e automatizadas.





Tecnologias e Automação no Processo de Resposta

TLP:CLEAR

Existem várias ferramentas livres que oferecem funcionalidades para coleta, indexação e análise de dados gerados por máquinas:

OpenObserve
Uma plataforma escrita em Rust e Vue, projetada para ser uma alternativa ao Elasticsearch, Splunk e Datadog. Oferece recursos para logs, métricas, traces, dashboards e alertas, com foco em facilidade de uso e eficiência no armazenamento de dados. O OpenObserve pode ser configurado para armazenar dados localmente ou em serviços compatíveis com S3, como MinIO e Azure Blob.

Exemplo: Coleta de Logs e Métricas, Análise e Correlacionamento de Eventos, Alertas em Tempo Real,Dashboards Personalizados e Auditoria e Conformidade

Zabbix
Uma solução de monitoramento de rede e aplicações que coleta e analisa dados de desempenho de servidores, dispositivos de rede e outros componentes de infraestrutura. Embora seu foco principal seja o monitoramento, o Zabbix também oferece funcionalidades para coleta e análise de logs.
Exemplo 1: Definindo um Trigger de Alerta se mais de 10 falhas de login forem detectadas em 300 segundos (5 minutos), um alerta será acionado:

{Server:log[/var/log/auth.log, "Failed password"].count(300)} > 10

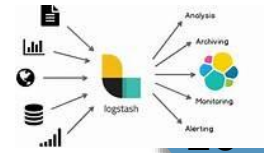
Exemplo 2: Definindo um Trigger de Alerta quando o código de resposta HTTP de um determinado domínio for diferente de 200, um alerta será acionado:

{Host:web.page.get[https://seudominio.com].last()} <> 200

Graylog
Uma plataforma de gerenciamento de logs que facilita a coleta, indexação e análise de grandes volumes de dados de maneira eficiente. O Graylog oferece uma interface web intuitiva para buscas e visualizações em tempo real, além de alertas personalizados.

SigNoz
Uma alternativa de código aberto ao que fornece monitoramento de desempenho de aplicações e observabilidade. O SigNoz permite que os desenvolvedores rastreiem métricas, logs e traces em uma única interface, facilitando a identificação e resolução de problemas.

Logstash
Uma ferramenta de pipeline de dados de código aberto que coleta, processa e armazena logs de diversas fontes. Geralmente é usada em conjunto com o Elasticsearch e o Kibana (conhecidos coletivamente como ELK Stack) para fornecer uma solução completa de análise e visualização de logs.

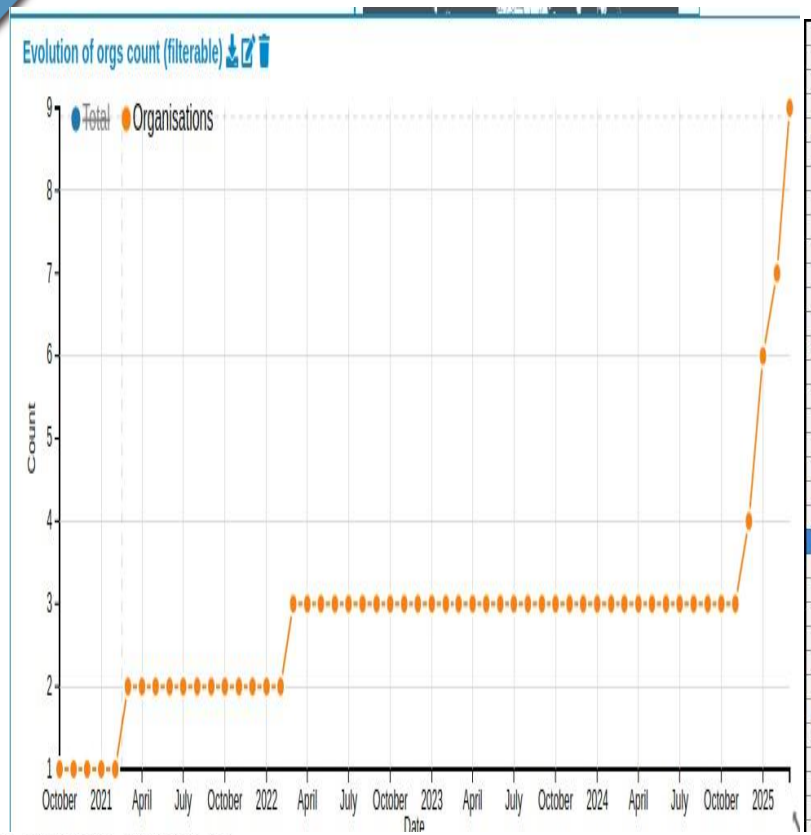


Essas ferramentas oferecem alternativas robustas e flexíveis para organizações que buscam soluções de análise e monitoramento de dados em tempo real, sem os custos associados a plataformas proprietárias. A escolha da ferramenta mais adequada dependerá das necessidades específicas do seu ambiente e dos recursos desejados.

Tecnologias e Automação no Processo de Resposta

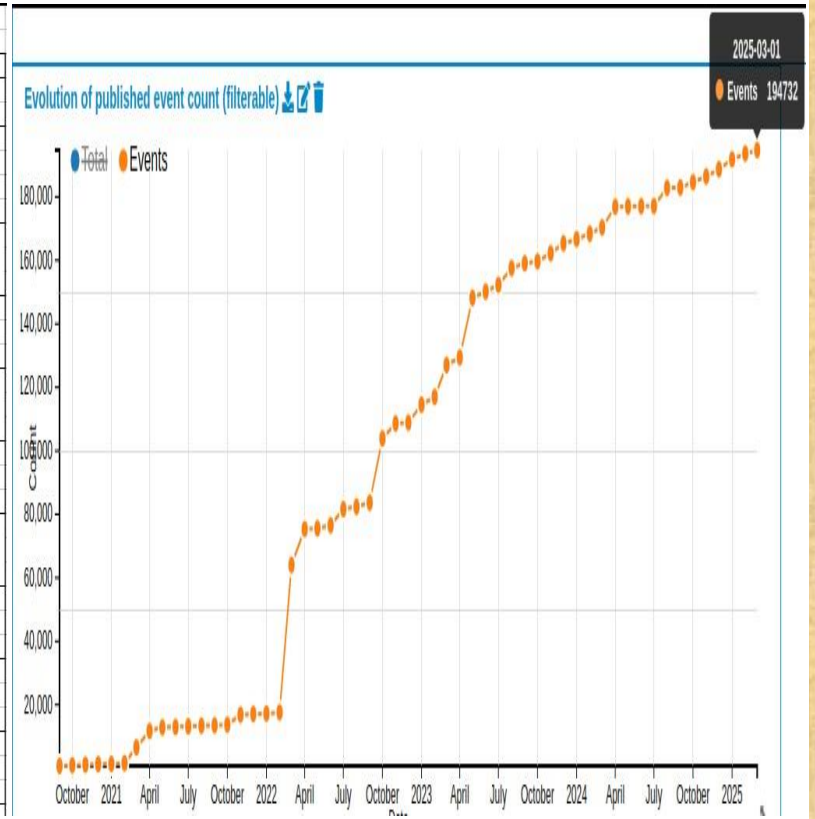
TLP:CLEAR

MISP



Malware Information Sharing Platform – MISP CITR Gov/ReGIC

Organização	Tipo de Compartilhamento	Ações Futuras ou Tratativas
ANATEL	Unidirecional	Transformar o compartilhamento em bidirecional
CDCIBER	Bidirecional	Transformar o compartilhamento em bidirecional, as tratativas para isso já estão sendo desencadeadas.
cert.br	Unidirecional	
certUY	Bidirecional	Embora o canal esteja pronto não está havendo compartilhamento haja vista problemas técnico do lado do CertUy.
CSIRTAmericas Network	Unidirecional	
POLÍCIA FEDERAL	Bidirecional	Tratativas realizadas e compartilhamento em fase de finalização de configuração, aguardando configuração de firewall do lado da PF.
DECEA	Bidirecional	
PETROBRAS	Unidirecional	A avaliar possibilidade de mudança no tipo de compartilhamento.
PRODEB	Bidirecional	Aguardando manutenção na instância MISP BA.
RONDÔNIA	Bidirecional	Em fase de implementação, tratativas em andamento, aguardando troca de auth keys.



Aplicação de IA e Machine Learning para detecção e resposta automática

TLP:CLEAR

Uma empresa financeira está enfrentando ataques **credential stuffing**, tipo de **ataque cibernético automatizado** em que invasores usam **combinações de login e senha vazadas** de um serviço para tentar acessar outras contas em diferentes sites e aplicativos.
Para mitigar o problema, a organização decide implementar uma solução baseada em **Inteligência Artificial (IA) e Machine Learning (ML)** para detectar e responder automaticamente a essas tentativas de ataque.

1. Coleta de Dados e Monitoramento em Tempo Real

A plataforma de monitoramento coleta logs de autenticação em tempo real de servidores, APIs e firewalls.
Logs de tentativas de login são enviados para uma IA de Análise Comportamental.

2. Aplicação de Machine Learning para Detecção

Faz-se a Análise de Anomalias para detectar padrões incomuns.
A IA avalia múltiplas falhas de login de um único IP ou diferentes localizações geográficas em curtos períodos de tempo.
O sistema compara a atividade suspeita com perfis normais de usuários, verificando velocidade de digitação, uso de proxies, comportamento de cliques e tempo entre tentativas.
Se um acesso for classificado como potencial ataque, ele é marcado para resolução automática.

3. Resposta Automática ao Incidente

Bloqueio em Tempo Real: Se a pontuação de risco do usuário atingir um limite crítico, o sistema bloqueia automaticamente o IP no firewall e no WAF.
Para acessos suspeitos, o sistema impõe um Captcha ou autenticação multifator (MFA) antes de permitir novas tentativas.
Geração de Alertas:

4. Benefícios da Automação com IA
✓ Detecção Proativa: A IA identifica ataques antes que causem danos significativos.
✓ Resposta em Milissegundos: Evita a necessidade de intervenção manual para bloqueio de ameaças.
✓ Redução de Falsos Positivos: O aprendizado contínuo melhora a precisão da detecção ao longo do tempo.
✓ Menor Impacto para Usuários Legítimos: Apenas acessos suspeitos enfrentam desafios adicionais, reduzindo atritos.

Com a IA e Machine Learning integrados ao processo de resposta a incidentes, a empresa conseguiu reduzir ataques de credential stuffing em 90%, sem impactar a experiência dos clientes legítimos. Esse modelo de automação pode ser estendido para outros tipos de ameaças, como ataques de DDoS, phishing e intrusões em redes corporativas.

Aplicação de IA e Machine Learning para detecção e resposta automática

TLP:CLEAR

ESTUDO DE CASO

Caso: PayPal e a Prevenção de Fraudes em Tempo Real

Cenário:
O PayPal processa milhões de transações por dia e precisava de um sistema para detectar fraudes instantaneamente.

Solução com Automação e IA:

Implementou um modelo de deep learning que analisa cada transação em milissegundos.
Quando uma transação suspeita é identificada, o sistema aciona automaticamente um bloqueio ou uma análise adicional sem intervenção humana.
O sistema aprende continuamente e se adapta a novas técnicas de fraude usadas por hackers.

Resultados:

✓ Bloqueio de mais de $1 bilhão em fraudes por ano.
✓ Resolução de incidentes 10x mais rápida que antes da automação.

Conclusão:

A IA e automação tornam a gestão de incidentes mais ágil e eficiente, ajudando empresas a reduzir o impacto de ataques e responder a ameaças em tempo real.

Estatísticas de CiberSecurity

TLP:CLEAR

Aproximadamente 70% das violações em 2021 foram motivadas financeiramente, enquanto menos de 5% foram motivadas por espionagem. (Verizon)

As multas do GDPR totalizaram US$ 1,2 bilhão em 2021. (CNBC)

US$ 17.700 são perdidos a cada minuto devido a um ataque de phishing. (CSO On-line)

Os custos mundiais do cibercrime atingirão US$ 10,5 trilhões anualmente até 2025. (Cybersecurity Vultures)

No ano passado, os ataques de ransomware aumentaram 93%. (Cyber Talk)

Globalmente, a ameaça de ataques cibernéticos aumentou 16% desde o início da guerra entre Rússia e Ucrânia em fevereiro de 2022. (Built In)

O ransomware como serviço continua ganhando popularidade entre os agentes de ameaças, com violações de ransomware dobrando de frequência em 2021. (Verizon)

86% dos casos de ransomware envolvem uma ameaça de vazamento de dados exfiltrados. (Coveware)

Mais da metade de todas as instituições financeiras foram atingidas por ransomware no ano passado – um aumento de 62% em relação ao ano anterior. (Sophos)

43% de todas as violações são ameaças internas, intencionais ou não. (Check Point) E 30% das violações de dados envolvem atores internos. (Verizon)

94% do malware é entregue por e-mail. (Verizon)

Em média, hackers atacam 26 mil vezes por dia, ou um ataque a cada três segundos. (Forbes)

Estatísticas de CiberSecurity

TLP:CLEAR

O trabalho remoto está crescendo. A Gallup estima que mais de 70 milhões de trabalhadores nos Estados Unidos podem fazer seu trabalho com sucesso remotamente. (Gallup)

No Brasil, cerca de 20,5 milhões de trabalhadores estão em ocupações com potencial para o trabalho remoto. (IPEA)

57% das organizações relatam que mais da metade de sua força de trabalho trabalha em casa pelo menos dois dias por semana. (Check Point)

Quando o trabalho remoto é um fator que causa uma violação de dados, o custo médio é US$ 1,07 milhão maior. (IBM)

O trabalho remoto está gerando um aumento de 50% no tráfego mundial da internet, levando a novas oportunidades de ataques cibernéticos. (Banco Mundial)

47% dos funcionários citaram a distração como um motivo para cair em um golpe de phishing enquanto trabalhavam em casa. (Tessian)

Trabalhadores remotos causaram uma violação de segurança em 20% das organizações durante a pandemia. (Malwarebytes)

Um estudo revelou que mais de 77% das organizações não possuem um plano de resposta a incidentes, o que ressalta a necessidade de investimentos tanto em prevenção quanto em resposta a incidentes. varonis.com

Além disso, a Gartner enfatiza que, até 2026, organizações que investirem pelo menos 20% de seus recursos de segurança em programas de resiliência e design flexível reduzirão o tempo total de recuperação pela metade quando um grande ataque ocorrer. gartner.com.br

Essas informações sugerem que, embora a prevenção seja fundamental, a capacidade de resposta eficaz a incidentes é igualmente crucial para minimizar os impactos operacionais e financeiros das ameaças cibernéticas.

Maurício Leite Ferreira
Analista de Incidentes – CTIR Gov

mauricio.leite@presidencia.gov.br

Site: https://www.gov.br/ctir

Comunicação de Incidentes: ctir@ctir.gov.br

Linkedin: https://www.linkedin.com/company/ctirgov/

Twitter: https://twitter.com/CtirGov


Formulário de Avaliação do Webinário