Tempest

ACADEMY

Conference

2023

Da Identificação à Defesa: Desvendando o Ciclo de Vida das Detecções

Vanessa Bandeira

Tempest

ACADEMY

Conference

Vanessa Bandeira, formada em Ciência da Computação pela UFRPE. Atuo a 4,5 anos na área de segurança da informação com viés para a defesa cibernética. Durante esses anos venho atuando em gestão de vulnerabilidades e conformidades, bem como explorando e ampliando meus conhecimentos no time de consultoria do centro de operações de segurança(SOC).

linkedin.com/in/vblt/

Tempest

ACADEMY

Conference

Economia

BC comunica vazamento de dados de 238 chaves Pix

Foram divulgados dados cadastrais da Phi Pagamentos

Tempest
ACADEMY
Conference

Cibercrime se planeja para alta de consumo na Black Friday

Na era das compras online, a busca por descontos intensifica-se e traz consigo ameaças sérias, como ofertas falsas e ataques cibernéticos, exigindo cuidados tanto dos consumidores quanto das empresas

A empresa Atomic Wallet sofreu um desvio de criptoativos em junho de 2023, sofrendo um imenso prejuízo de US$100 milhões. O golpe foi vinculado ao grupo de cibercriminosos Lazarus, que vem aplicando inúmeros golpes desse tipo na Coréia do Norte.

CIBERSEGURANÇA

69% das organizações na AL sofreram um incidente de segurança durante o último ano

Ransomwares apresentam crescimento de quase 11% no Brasil, revela pesquisa

Relatório também aponta expressivo crescimento de 45% dos stealers

Por: Redação, 22/11/2023 às 17h11 - Atualizado em 22/11/2023 às 17h11

Home › Future of Money

Hackers da Coreia do Norte roubaram mais de R$ 900 milhões em criptomoedas em 2023

Em junho, grupo realizou um dos maiores roubos de criptoativos do ano, desviando mais de US$ 100 milhões da Atomic Wallet

Incidente de Segurança

Tempest
[ACADEMY]
Conference

É um evento ou ocorrência que compromete a **confidencialidade**, **integridade** ou **disponibilidade** de dados ou sistemas de informação em uma organização. Esses incidentes podem envolver uma ampla gama de atividades prejudiciais, como ataques cibernéticos, vazamentos de dados, malware, roubo de informações sensíveis, falhas de segurança, entre outros.

NIST

Incidente de Segurança

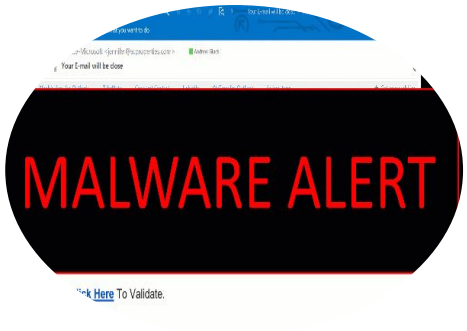
Tempest
[ACADEMY]
Conference

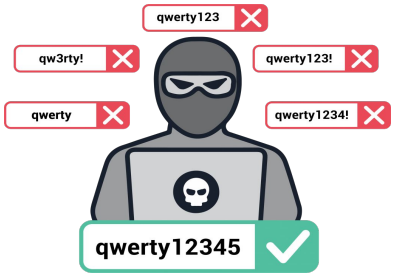
Todo ataque é um incidente de segurança,
mas nem todo incidente de segurança é um ataque.

Ameaças Cibernéticas

Tempest ACADEMY Conference

As ameaças estão ligadas a ações intencionais ou acidentais que buscam e exploram vulnerabilidades.





As ameaças a determinados ativos de informação se concretizam por meio das vulnerabilidades, fraquezas e lacunas na segurança.

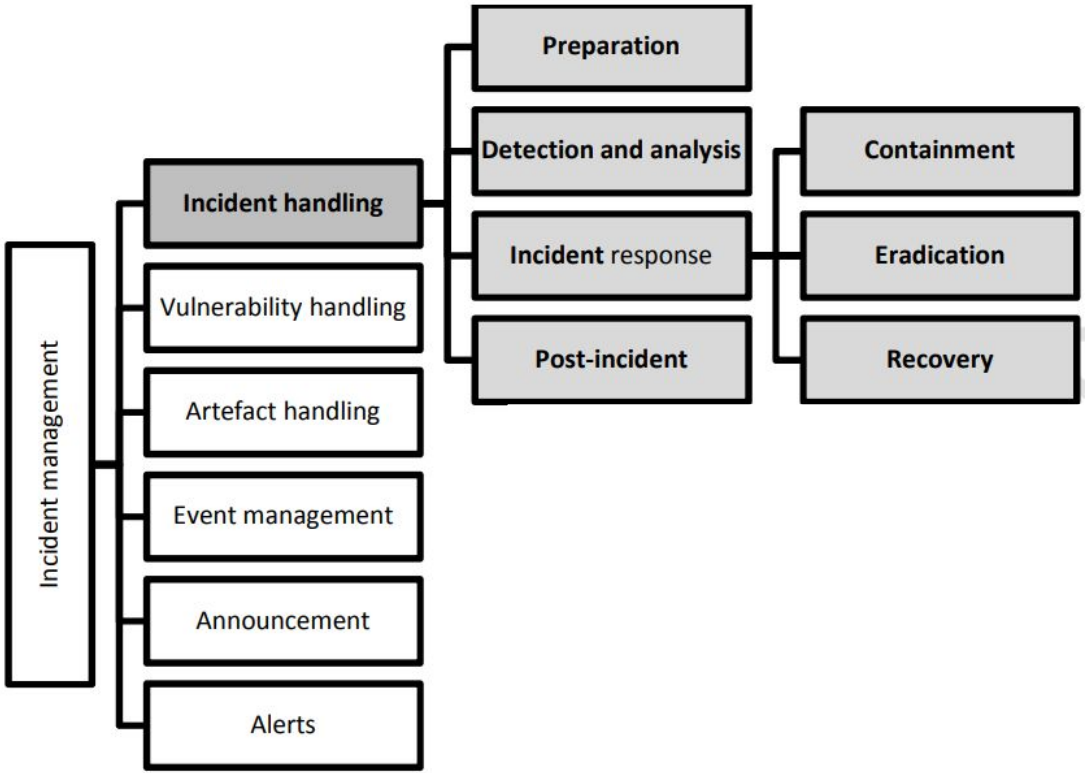
Correlação dentro da gestão de segurança

Ameaça: Rio
Risco: Erosão da barragem
Vulnerabilidade: Casa na beira do rio
Incidente: Casa desmorona na beira do rio

Ameaça: Sobrecarga na ponte
Risco: Colapso da estrutura da ponte
Vulnerabilidade: Capacidade máxima estrutural
Incidente: Queda da ponte com pessoas

Ciclo de Vida das Detecções de Ameaças

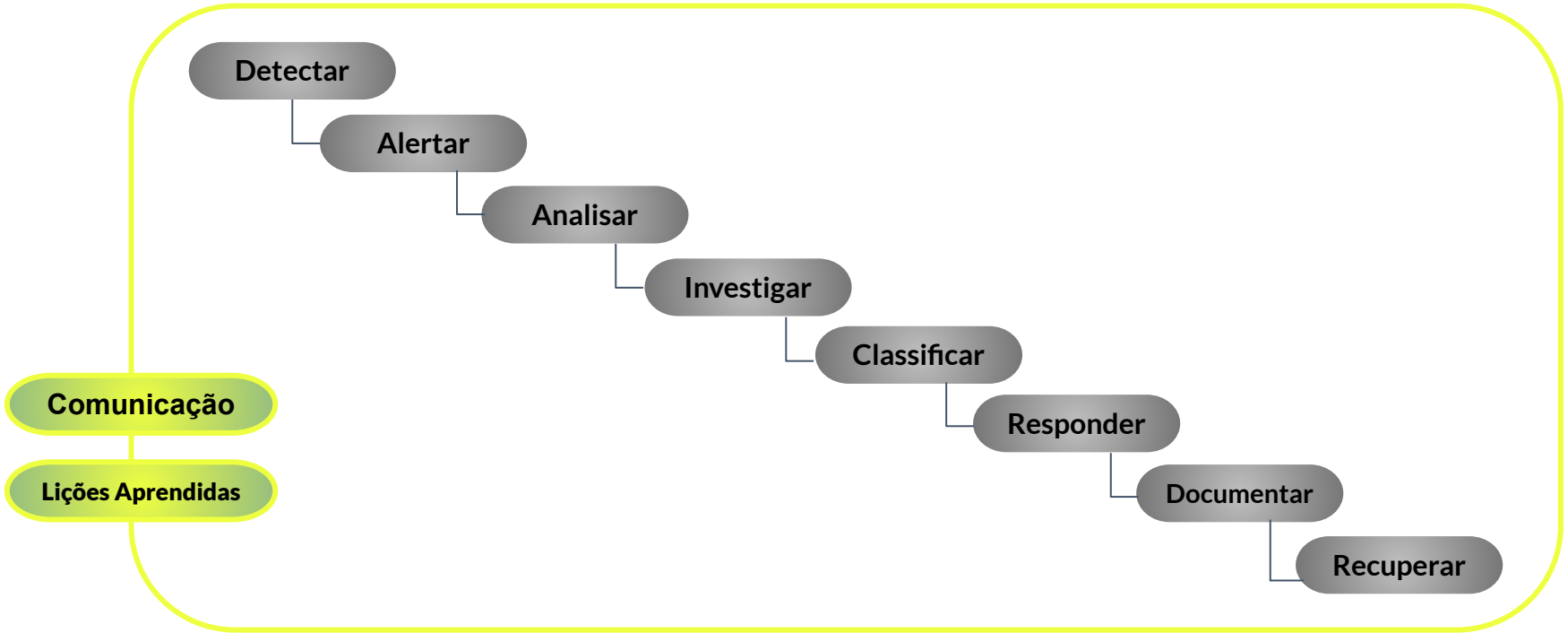
Tempest
ACADEMY
Conference



Adapted from: Alberts et al. 2004; British Standards Institution 2007; Cichonski & Scarfone

Ciclo de Vida das Detecções de Ameaças

Tempest ACADEMY Conference



Computer Security Incident Handling Guide - Special Publication 800-61, NIST

Ciclo de Vida das Detecções de Ameaças

Tempest
[ACADEMY]
Conference

Detectar

As ameaças são detectadas por meio de várias ferramentas de segurança



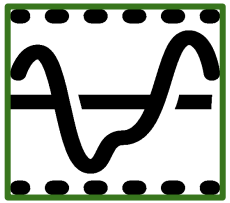


Ciclo de Vida das Detecções de Ameaças

Tempest
[ACADEMY]
Conference

Alertar

Um alerta é gerado e geralmente enviado a uma equipe de segurança ou a um centro de operações de segurança (SOC)

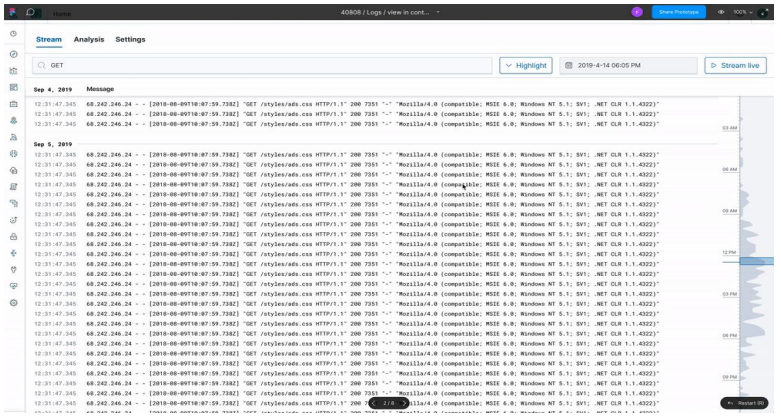


Ciclo de Vida das Detecções de Ameaças

Tempest
[ACADEMY]
Conference

Analisar

O alerta é analisado para determinar a gravidade da ameaça, o impacto potencial, a origem da ameaça e o método de ataque



Ciclo de Vida das Detecções de Ameaças

Tempest
[ACADEMY]
Conference

Investigar

Se o alerta for considerado legítimo, uma investigação mais aprofundada é realizada para entender como a ameaça conseguiu entrar e quais sistemas ou dados foram afetados. Isso pode envolver a coleta de evidências, análise forense e entrevistas com pessoas envolvidas

Ciclo de Vida das Detecções de Ameaças

Tempest
[ACADEMY]
Conference

Classificar

A ameaça é classificada com base em sua gravidade, origem e impacto. Isso ajuda na priorização das respostas

Ciclo de Vida das Detecções de Ameaças

Tempest
[ACADEMY]
Conference

Responder

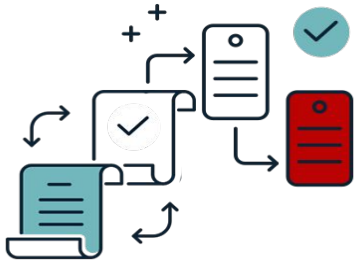
Com base na classificação da ameaça, são tomadas medidas para conter e mitigar o ataque. Isso pode envolver a remoção da ameaça, isolamento de sistemas afetados, atualizações de segurança e outras ações para evitar mais danos

Ciclo de Vida das Detecções de Ameaças

Tempest
[ACADEMY]
Conference

Documentar

São documentadas as ações e as descobertas das investigações para que sirvam de referência e aprimoramento contínuo da segurança

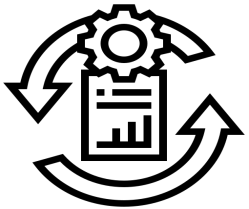


Ciclo de Vida das Detecções de Ameaças

Tempest
[ACADEMY]
Conference

Recuperar

Após conter a ameaça, a organização trabalha na recuperação completa dos sistemas afetados. Isso pode incluir restaurar sistemas e dados, aplicar correções e medidas de segurança adicionais



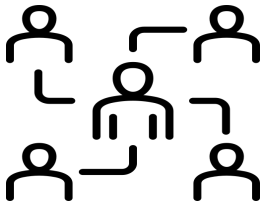
Ciclo de Vida das Detecções de Ameaças

Tempest
[ACADEMY]
Conference

Após o incidente, a organização realiza uma revisão para identificar lições aprendidas e oportunidades de melhoria na postura de segurança

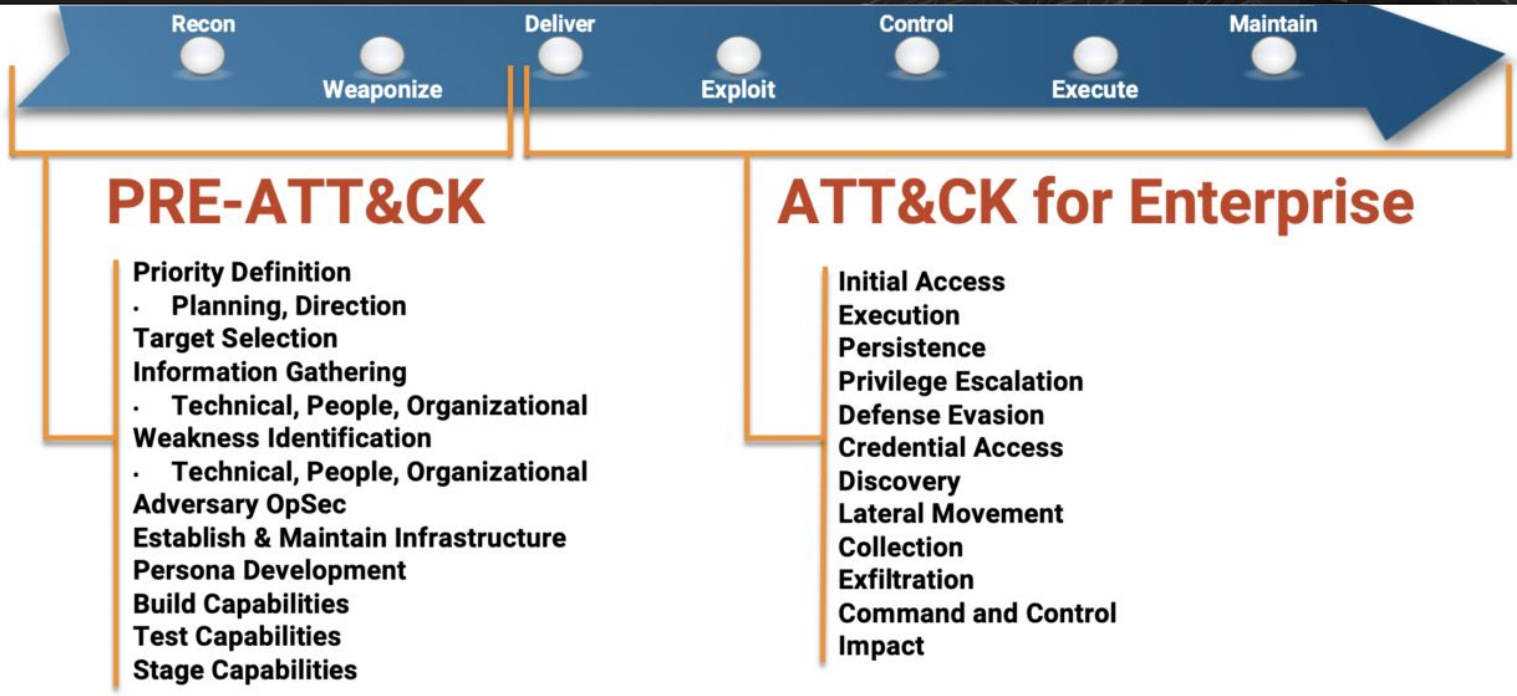
Comunicação

Lições Aprendidas



Meu aliado: Mitre Att&ck

Tempest
[ACADEMY]
Conference



MITRE Att&ck Framework: Security Trails, SOC Radar

Obsolescência de uma Detecção

Tempest ACADEMY Conference

Evolução das Ameaças

Mudanças na Tecnologia e Infraestrutura

Alterações de Política

Falsos Positivos

Atualizações de Software e Hardware

Assinaturas de Malware

Tecnologia Legada

Monitoramento Contínuo - Estrutura Faseada

Computer Security Incident Handling Guide - Special Publication 800-61, NIST

Obsolescência de uma Detecção: Aplicação de Caso

Cenário

Empresa: Umbrella Corporation

Detecção implementada no ambiente: Brute Force FTP em logs de Linux

Escopo do Log:

- Linux secure
  - tty ftp
    - *authentication failure*

Tática Mitre : Credential Access

Técnica Mitre : T1110 (Brute Force)

Ano de Implantação da Detecção: 2020

Tempest
ACADEMY
Conference

Obsolescência de uma Detecção: Aplicação de Caso

Investigação

1. A detecção possuía triggers recentes, dado o escopo mapeado para ela?
2. Considerando o histórico de alertas do ambiente, os logs recentes estavam conforme o esperado?
3. A coleta dos logs estava com algum problema de falha de recebimento no SIEM?
4. O contexto passado pela Umbrella Corporation deixava claro que aquela detecção estava funcional, conforme o ambiente atual?
5. Quais alternativas de detecção viáveis considerando o cenário abordado?

Tempest
ACADEMY
Conference

Obsolescência de uma Detecção: Aplicação de Caso

Análise

1. Avaliação da estrutura da coleta dos logs ;
2. Ajuste da lógica da detecção conforme o recebimento dos logs atualizados;
3. Entendimento da utilização do protocolo no ambiente;
4. Existência de políticas e ações de infraestrutura que ratificam a não utilização do protocolo;
5. Desativação da detecção utilizando o protocolo antigo;
6. Inserção de uma nova detecção mais atualizada.

Estratégias de Defesa e Prevenção

Tempest
[ACADEMY]
Conference

- ➔ Análise pós-incidente na busca por melhorias contínuas;
- ➔ Classificação Uniforme das Detecções;
- ➔ Utilização do modelo de segurança em camadas
- ➔ Estruturar um Plano de Resposta a Incidentes;
- ➔ Auditorias e Avaliações de Segurança;
- ➔ Gestão de Vulnerabilidades e Conformidades (Gestão de Riscos = prioridade para o negócio);
- ➔ Validação das ferramentas do ambiente **X** Modelo/Processo do negócio;
- ➔ Treinamento contínuo voltado a segurança da informação (pessoas = elo mais importante);
- ➔ Sistematização das detecções a fim de identificar comportamentos distintos;

Referências

- CICHONSKI, Paul; MILLAR, Tom; GRANCE, Tim; SCARFONE, Karen. Computer Security Incident Handling Guide: recommendations of the national institute of standards and technology. National Institute Of Standards And Technology, [S.L.], v. 2, n. 800-61, p. 1-79, ago. 2012. National Institute of Standards and Technology. http://dx.doi.org/10.6028/nist.sp.800-61r2.
- Create More Effective SOC With the Mitre ATT&CK Framework, SOCRadar® Community Edition, janeiro 2021, https://socradar.io/create-more-effective-soc-with-the-mitre-attck-framework/
- SANS 2022 SOC SURVEY. USA: Analyst Program, Maio 2022. Disponível em: https://soc-survey.com/2022/
- SOC MODEL GUIDE. USA: Gartner, 2021. Id G00 754096. Disponível em: https://www.gartner.com/en/documents/4851731
- ALL ABOUT SOC (SECURITY OPERATION CENTERS). USA: Green Circle, jun. 2023. Reviewed By: Mohammad Alkhudari. Disponível em: https://grcico.com/

Tempest ACADEMY Conference

Referências

- RAHMAN, Nurul Hidayah Ab; CHOO, Kim-Kwang Raymond. A survey of information security incident handling in the cloud. Computers & Security, [S.L.], v. 49, p. 45-69, mar. 2015. Elsevier BV. http://dx.doi.org/10.1016/j.cose.2014.11.006

- Giuseppe Settanni, Florian Skopik, Yegor Shovgenya, Roman Fiedler, Mark Carolan, Damien Conroy, Konstantin Boettinger, Mark Gall, Gerd Brost, Christophe Ponchel, Mirko Haustein, Helmut Kaufmann, Klaus Theuerkauf, Pia Olli, A collaborative cyber incident management system for European interconnected critical infrastructures, Journal of Information Security and Applications, Volume 34, Part 2, 2017, Pages 166-182, https://doi.org/10.1016/j.jisa.2016.05.005

Tempest
ACADEMY
Conference

Estarei disponível para um bate-papo e dúvidas no “Asking the Experts”

Obrigada

"Feminismo não é um conceito estranho ou ocidental. Feminismo é sobre igualdade de gênero, e isso é uma luta que todas as culturas e sociedades devem abraçar."

Chimamanda Ngozi Adichie

Tempest
ACADEMY
Conference