**Diário do manipulador de incidentes**

**Instruções**

À medida que você avança neste curso, você pode usar este modelo para registrar suas descobertas após concluir uma atividade ou para fazer anotações sobre o que aprendeu sobre uma ferramenta ou conceito específico. Você também pode usar este diário como uma forma de registrar as principais conclusões sobre as diferentes ferramentas ou conceitos de segurança cibernética que você encontrar neste curso.

|  |  |
| --- | --- |
| **Data:**  09 de Dezembro de 2024 | **Entrada:**  1 |
| Descrição | Registro de um incidente de segurança envolvendo ransomware que interrompeu as operações de uma clínica de saúde. |
| Ferramenta(s) usada(s) | NA |
| Os 5 W's | Capture os 5 W's de um incidente.  ● Quem causou o incidente? Um grupo de Hackers Antiéticos, conhecido por atacar organizações dos setores de saúde e transporte.  ● O que aconteceu? Um ataque de Ransomware criptografou os arquivos de computador da clínica, impossibilitando o acesso a dados críticos  ● Quando o incidente ocorreu? Terça-feira, às 9h  ● Onde o incidente aconteceu? Em uma pequena clínica de saúde dos EUA  ● Por que o incidente aconteceu? A causa do incidente de segurança foi um e-mail de Phishing que continha um anexo malicioso. Depois de baixado, o ransomware foi implantado e criptografou os arquivos de computador da organização. |
| Notas adicionais | A clínica deve pagar o resgate para recuperar a chave de descriptografia? |

|  |  |
| --- | --- |
| **Data:**  13 de Dezembro de 2024 | **Entrada:**  2 |
| Descrição | Alerta de download de um arquivo suspeito |
| Ferramenta(s) usada(s) | VirusTotal |
| Os 5 W's | Capture os 5 W's de um incidente.  ● Quem causou o incidente? Malware conhecido como FlagPro  ● O que aconteceu? Um funcionário fez um download de arquivo enviado em anexo no seu e-mail, em seguida, digitou a senha para abrir o arquivo. Quando o funcionário abriu o arquivo, um payload malicioso foi executado em seu computador.  ● Quando o incidente ocorreu?  1:11 p.m.: Um funcionário recebe um e-mail com um arquivo anexado.  1:13 p. m.: O funcionário faz o download e abre o arquivo com sucesso.  13:15: Vários arquivos executáveis não autorizados são criados no computador do funcionário.  13:20: Um sistema de detecção de intrusão detecta os arquivos executáveis e envia um alerta ao SoC.  ● Onde o incidente aconteceu? Em uma empresa de serviços financeiros  ● Por que o incidente aconteceu? Um funcionário acessou um arquivo malicioso devido a uma falha no reconhecimento de e-mails de phishing e abriu o anexo fornecido, permitindo a execução do payload. |
| Notas adicionais | * malware foi identificado pelo VirusTotal como **FlagPro**, com várias detecções por fornecedores de segurança. * Realizar treinamento de conscientização sobre phishing para os funcionários. |

|  |  |
| --- | --- |
| **Data:**  14 de Dezembro de 2024 | **Entrada:**  3 |
| Descrição | Possível tentativa de Phishing. |
| Ferramenta(s) usada(s) | VirusTotal  Phishing Playbook  Email. |
| Os 5 W's | Capture os 5 W's de um incidente.  ● Quem causou o incidente? Def Communications <76tguyhh6tgftrt7tg.su> <114.114.114.114> ( Remetente do e-mail, possivelmente mal intencionado)  ● O que aconteceu?  Um e-mail malicioso foi enviado para a equipe de RH, contendo um arquivo suspeito anexo.  ● Quando o incidente ocorreu? Ocorreu em Julho 20, 2022 09:30:14 AM  ● Onde o incidente aconteceu? No computador/e-mail de um funcionário do RH da organização.  ● Por que o incidente aconteceu? O atacante tentou enganar o destinatário simulando um processo legítimo de candidatura a emprego, com a intenção de distribuir um malware. |
| Notas adicionais | * Após investigar o **hash** do arquivo anexo no VirusTotal, verificou-se que **bfsvc.exe** é malicioso. * Recomenda-se bloquear o remetente, monitorar possíveis conexões para os IPs envolvidos e verificar se houve execução do anexo no computador do funcionário. |

|  |  |
| --- | --- |
| **Data:**  17 de Dezembro de 2024 | **Entrada:**  4 |
| Descrição | acesso não autorizado às informações pessoais identificáveis (PII) e informações financeiras do cliente. |
| Ferramenta(s) usada(s) | Liste todas as ferramentas de segurança cibernética que foram usadas. |
| Os 5 W's | Capture os 5 W's de um incidente.  ● Quem causou o incidente? Um invasor que se aproveitou de uma falha web  ● O que aconteceu? um indivíduo conseguiu obter acesso não autorizado às informações pessoais identificáveis (PII) e informações financeiras do cliente.  ● Quando o incidente ocorreu? 28 de dezembro de 2022, às 19h20  ● Onde o incidente aconteceu? No aplicativo da web (e-commerce)  ● Por que o incidente aconteceu? A causa raiz do incidente foi identificada como uma vulnerabilidade no aplicativo da web de comércio eletrônico. Essa vulnerabilidade permitiu que o invasor realizasse um ataque de navegação forçada e acessasse dados de transações do cliente modificando o número do pedido incluído na sequência de URL de uma página de confirmação de compra. Essa vulnerabilidade permitiu que o invasor acessasse as páginas de confirmação de compra do cliente, expondo dados do cliente, que o invasor então coletou e exfiltrou. |
| Notas adicionais | Havia uma **única fonte de log** mostrando um volume excepcionalmente alto de pedidos de clientes listados sequencialmente.  Seria necessário conserta a falha no aplicativo web e implementar que apenas usuários autenticados tenham acesso autorizado ao conteúdo |

|  |  |
| --- | --- |
| **Data:**  18 de Dezembro de 2024 | **Entrada:**  5 |
| Descrição | Explorando assinaturas e registros com o Suricata |
| Ferramenta(s) usada(s) | Suricata |
| Os 5 W's | Capture os 5 W's de um incidente.  ● Quem causou o incidente? O incidente foi gerado por pacotes de tráfego de rede contidos no arquivo sample.pcap.  ● O que aconteceu? O Suricata foi executado com regras personalizadas para detectar e alertar sobre solicitações HTTP GET, resultando na geração de alertas nos arquivos fast.log e eve.json  ● Quando o incidente ocorreu? O teste foi realizado em 2024-12-18  ● Onde o incidente aconteceu? O incidente foi simulado em um ambiente de laboratório utilizando a máquina local do analista.  ● Por que o incidente aconteceu? O incidente ocorreu para monitorar e analisar o tráfego HTTP, especificamente para detectar requisições GET, a fim de validar as regras de detecção no Suricata. |
| Notas adicionais | O Suricata funcionou conforme o esperado, acionando alertas corretamente quando as regras foram atendidas. |

|  |  |
| --- | --- |
| **Data:**  24 de Dezembro de 2024 | **Entrada:**  6 |
| Descrição | Realizando uma consulta com o Splunk |
| Ferramenta(s) usada(s) | Splunk |
| Os 5 W's | Capture os 5 W's de um incidente.  ● Quem causou o incidente? incidente foi originado por tentativas de login SSH na conta raiz do servidor de e-mail.  ● O que aconteceu? O Splunk foi utilizado para indexar e pesquisar eventos de log, resultando na identificação de mais de 100 logins SSH com falha para a conta raiz.  ● Quando o incidente ocorreu? A análise foi realizada em 2024-12-24.  ● Onde o incidente aconteceu? O incidente foi analisado a partir de logs no servidor de e-mail da Buttercup Games.  ● Por que o incidente aconteceu? objetivo da análise foi investigar tentativas de login não autorizadas, possivelmente relacionadas a ataques de força bruta ou tentativas de acesso não autorizado. |
| Notas adicionais | A analise foi gerada com base em um arquivo com dados fictícios fornecidos pelo curso, afim de aprender a utilizar a ferramenta |

|  |  |
| --- | --- |
| **Data:**  24 de Dezembro de 2024 | **Entrada:**  7 |
| Descrição | Investigação de domínio suspeito com o Chronicle |
| Ferramenta(s) usada(s) | Chronicle |
| Os 5 W's | Capture os 5 W's de um incidente.  ● Quem causou o incidente? O incidente está relacionado a um possível phishing que envolveu o domínio signin.office365x24.com.  ● O que aconteceu? Utilizei o Chronicle para investigar se o domínio era mal-intencionado, encontrando evidências de que estava associado a atividades de phishing  ● Quando o incidente ocorreu? A análise foi realizada em 2024-12-24.  ● Onde o incidente aconteceu? A investigação foi feita utilizando dados do Chronicle sobre o domínio signin.office365x24.com.  ● Por que o incidente aconteceu? A análise teve como objetivo identificar e confirmar a natureza maliciosa do domínio, que foi suspeito de estar envolvido em campanhas de phishing. |
| Notas adicionais | Durante a investigação, verifiquei a reputação do domínio através do VirusTotal, onde um fornecedor o sinalizou como malicioso. Explorei as guias de ATIVOS e LINHA DO TEMPO para identificar os ativos que acessaram o domínio, registrando que diversos dispositivos acessaram o domínio e que houve solicitações POST para a página /login.php, sugerindo uma possível violação de dados. |

### Precisa de outro modelo de entrada de diário?

Se você quiser adicionar mais entradas de diário, copie uma das tabelas acima e cole-a no modelo para usar em entradas futuras.

|  |
| --- |
| Reflexões/Notas: Este diário de incidentes serve como uma ferramenta valiosa para documentar e analisar eventos de segurança que impactam a organização. Ao registrar cada incidente, podemos identificar padrões e vulnerabilidades recorrentes, permitindo uma resposta mais eficaz e a implementação de medidas preventivas. As anotações sobre ataques de ransomware, tentativas de phishing e acessos não autorizados destacam a crescente sofisticação das ameaças enfrentadas. |