|  |  |
| --- | --- |
| **Este documento possui dados pessoais** | |
| **Resumo** | **Acessos volumétricos originados do IP 191.235.64.85 direcionados ao vip-pmeuinssprxr.inss.gov.br** |
| **Indicadores de Ameaça** | Informar os indicadores de ameaça |
| **Período analisado** | **Informar data de início/fim** |
| **Credenciais envolvidas / Ativos de informações** | **Credenciais** |
| cred |
| **IPs de origem** |
| ips |
| **Ferramentas de análise** | ELK |
| **Possível Impacto** | Possível vazamento de informações. |
| **Contenção** | Foi realizado o bloqueio temporário dos endereços no WAF. |
| **Evidências/Contexto** | |
| **1** | **IP de Origem** |
| Evidência do endereço de origem | enderecoOrigem |
| **2** | **Log Aplicação- Consultas/SAT - ELK** |
| Verificação da volumetria | figurasSat |
| **3** | **Log WEB - ELK** |
| Volumetria de acessos | figurasContexto |
| **4** | **Log GERID - ELK** |
| Uso de credenciais | gerid |