Integração SOC-CSIRT

Jornada de melhoria do processo de gestão de incidentes

Agosto 2023 TLP:CLEAR

Integração SOC-CSIRT

Apresentadores

Glauco Chaves
Coordenador da CORI
glauco.chaves@dataprev.gov.br

José Antônio Casemiro Neto
Líder da Equipe de SOC
jose.casemiro@dataprev.gov.br

Norton Evers
Analista de Sistemas
norton.evers@dataprev.gov.br

Agenda

- Contexto – Ambiente Dataprev
- CTIR – Organizar a Resposta
- SOC – Melhorar a Detecção
- Integração das Equipes
- Exemplo do Processo (estudo de caso)
- Desafios Futuros

Dataprev
Soluções

PREVIDÊNCIA

Processamento da folha de pagamento de benefícios mensal do INSS para

37,4 milhões de beneficiários

TRABALHO

Processamento do seguro desemprego em 2022 de 5,1 milhões de requerimentos resultando em

4,5 milhões de beneficiários

ASSISTÊNCIA

Processamento da verificação periódica do Cadastro Único com seleção de público em

10,6 milhões de famílias

Referência: 2022

Aplicações de Missão Crítica

TLP:CLEAR

Definições

- Equipes independentes envolvidas no processo:
  - CTIR: resposta a incidentes (CSIRT)
  - SOC: monitoramento de segurança

CTIR

Organizando a Resposta

Agosto 2023 TLP:CLEAR

SOC

Melhorando a detecção

Agosto 2023 TLP:CLEAR

Referências

- Computer Security Incident Response Team (CSIRT) Services Framework Version 2.1" FIRST
- "Defining Incident Management Processes for CSIRTs: A Work in Progress". CMU/SEI-2004-TR-015
- "How to setup up CSIRT and SOC – Good Practice Guide", ENISA
- Curso Advanced Topics in Incident Handling (ATIH) – CERT.br
- Curso GHSOC – GoHacking

Obrigado!

Perguntas?

Fale conosco!

ctir@dataprev.gov.br

dataprevtecnologia

dataprev

dataprev

dataprev-tecnologia

dataprevtecnologia

Agosto 2023 TLP:CLEAR