Infraestrutura Tecnológica de Operações da Dataprev

Centro de Operações de Segurança
ou *Security Operations Center* (SOC)

Atividades

- Identificação de eventos em tempo real
- Monitoramento contínuo de segurança
- Priorização baseada em riscos
- Atividades de resposta
- Mitigação dos ataques

SOC

É a estrutura que reúne processos, pessoas e tecnologias envolvidas na **detecção, contenção** e **resposta** a ameaças cibernéticas.

15 analistas de processamento trabalham **24h por dia, 7 dias por semana,** no tratamento e resolução de incidentes.

Profissionais organizados em três times

AZUL
Defende proativamente, monitorando e respondendo às ameaças cibernéticas

VERMELHO
Responsável pela análise de vulnerabilidades da infraestrutura e teste dos mecanismos de defesa

ROXO
Revisa as estratégias de defesa, realiza a integração entre os times Azul e Vermelho e atua na conformidade da segurança operacional

SOC em números

2 mil
eventos de segurança tratados desde 2020 (ano de criação do SOC)

Desse universo, mais de

1,4 mil
eventos foram encaminhados à Comissão de Tratamento e Resposta a Incidentes Cibernéticos e Violações à Privacidade (CTIR)

+1,19 trilhão
de registros processados e mais de **15 mil** alertas gerados pelo Security Information and Event Management (SIEM)* desde 2020

** SOC utiliza a ferramenta de SIEM (Security Information and Event Management), capaz de correlacionar eventos gerados por diversas fontes e identificar rapidamente tentativas de explorações de vulnerabilidades.*

2,8 mil
detecções de credenciais comprometidas em pouco mais de 3 anos

Ferramentas para prover a segurança • 2023

13,5 milhões
de bloqueios realizados pelo *Web Application Firewall* (WAF)

312 milhões
de bloqueios realizados pelo *Intrusion Prevention System* (IPS)

Informações:
www.dataprev.gov.br

Fonte: **Dataprev**
Posição em junho de 2023