ABAC
ASSOCIAÇÃO BRASILEIRA DE ADMINISTRADORAS DE CONSÓRCIOS

Painel CyberSegurança

CONAC - 2024

ABAC
ASSOCIAÇÃO BRASILEIRA DE ADMINISTRADORAS DE CONSÓRCIOS

Cenário de um evento cibernético

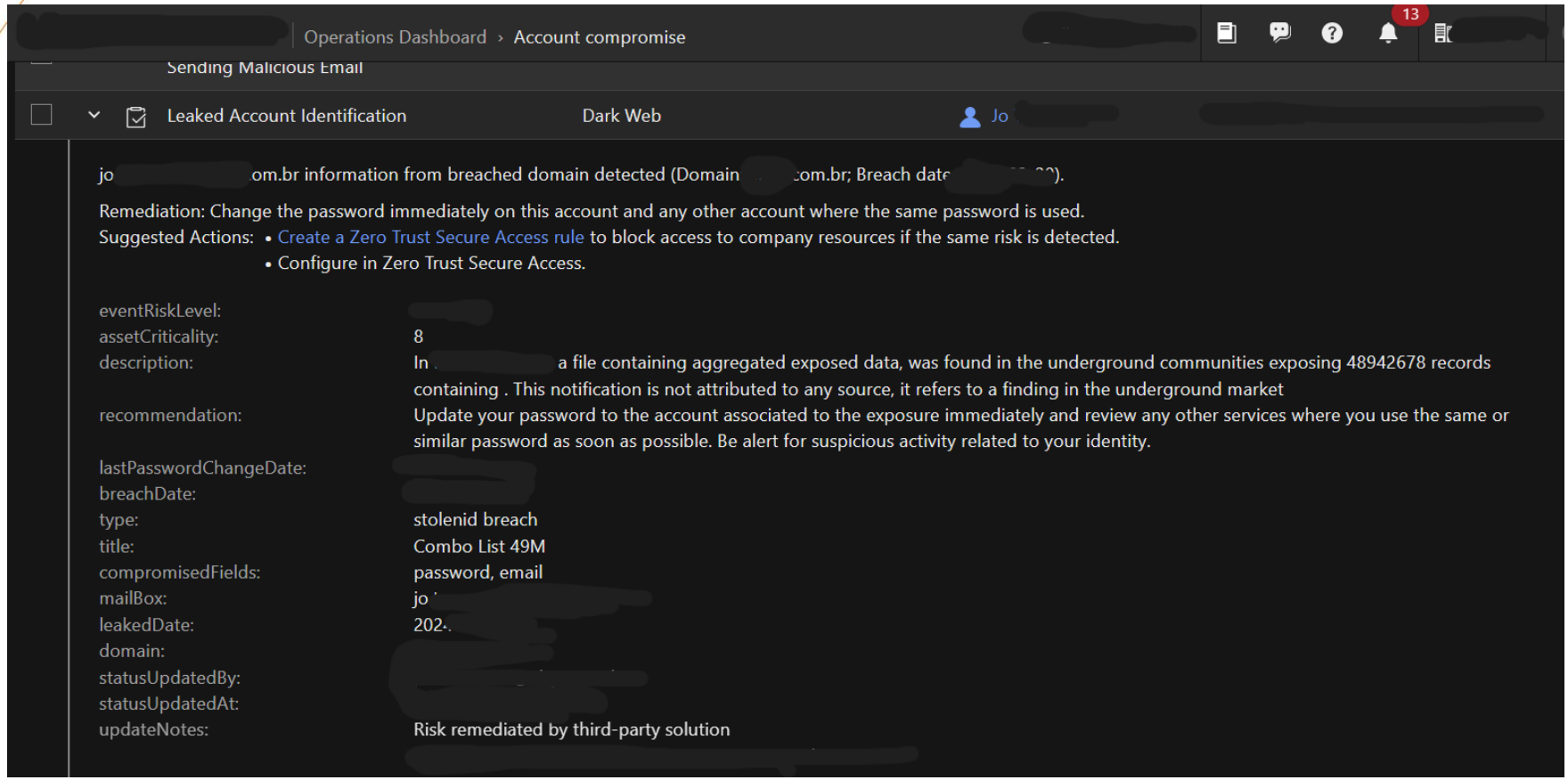
Erros e acertos

Cenário de um Incidente Cibernético GRAVE!

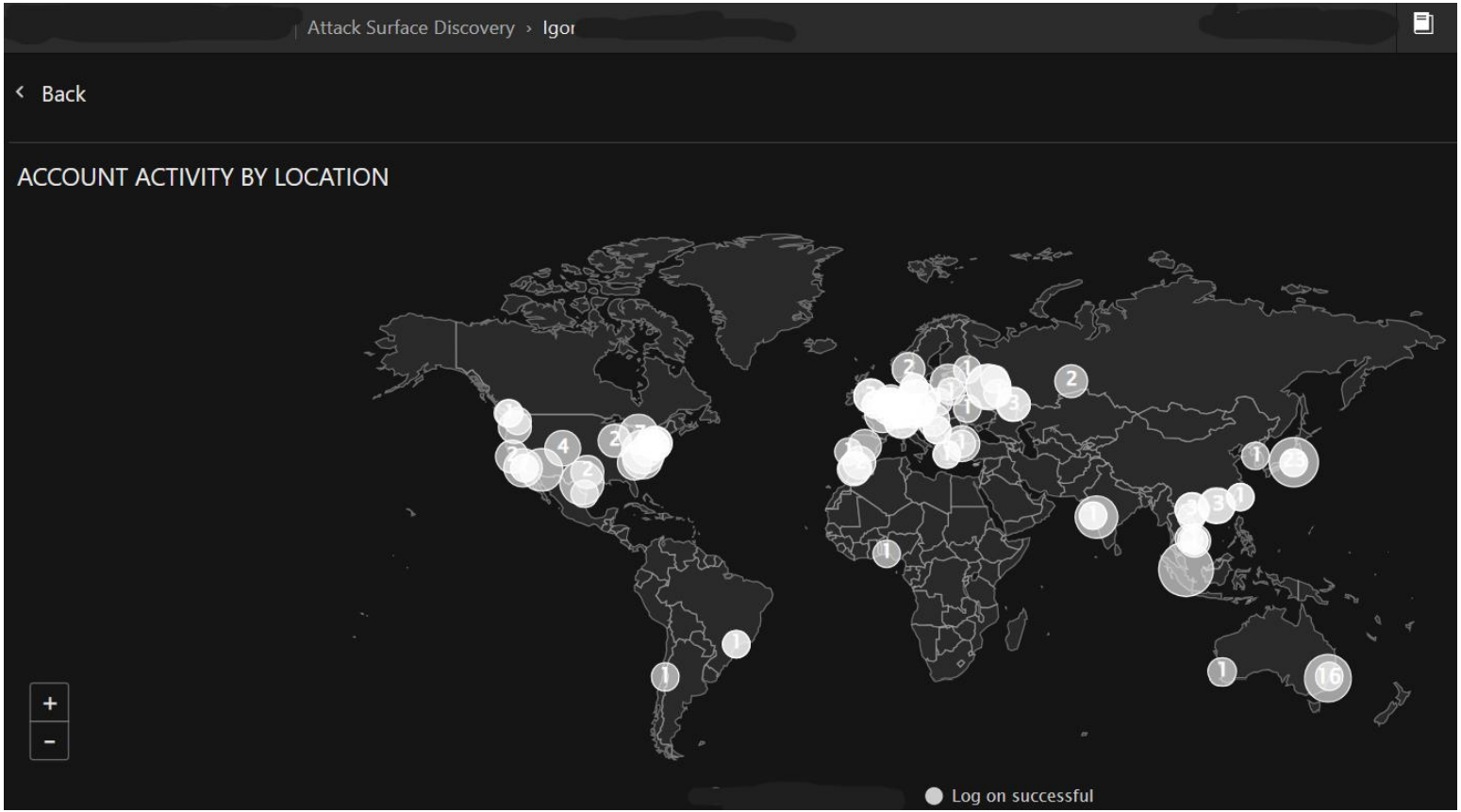
- Indústria no interior de São Paulo (2.500 colaboradores – 3 Plantas – 3 turnos);
- TIC com 19 colaboradores entre Suporte Infraestrutura, Sistemas Industriais e Sistemas Administrativos;
- 6 ambientes de TI interligados, 3 On-premises e 3 em diferentes Nuvens (AWS/Azure e Oracle);
- Ambiente tecnológico desatualizado (2 anos apenas com patches críticos em SO);
- Equipe de TI sobrecarregada, apenas horário comercial, foco em projetos demandados pelo negócio.
- Segurança Cibernética como subtarefa do analista de infraestrutura e na consultoria esporádica de LGPD;

- Invasão da rede local, com criptografia dos ambientes de 2 plantas (3 ambientes de TI), sem exfiltração de dados;
- Início da invasão na madrugada de um feriado brasileiro que pegava de 5ª a domingo;
- Ataque iniciado a partir do vazamento de uma credencial e senha de um usuário gestor, usada em site de apostas;
- Antivírus, firewall e administração de contas e senhas sem integração e sem padronização entre plantas;
- 43 servidores das 2 principais plantas criptografados, todo backup em nuvem criptografado, rede administrativa e de manufatura paralisada por 52 dias.
- Auditoria e questionamento da ANPD, da imprensa especializada e dos parceiros e fornecedores críticos.
- Em menos de 24 horas a conta já era utilizada preparando para o ataque em todo submundo cibernético.
- O feriado no Brasil com descanso da equipe de TI permitiu que o ambiente fosse atacado sem despertar a desconfiança.
- Registro em LOG por 90 dias porém sem rotina de verificação e análise dos LOGs;

Cenário de um Incidente Cibernético GRAVE!



Cenário de um Incidente Cibernético GRAVE!



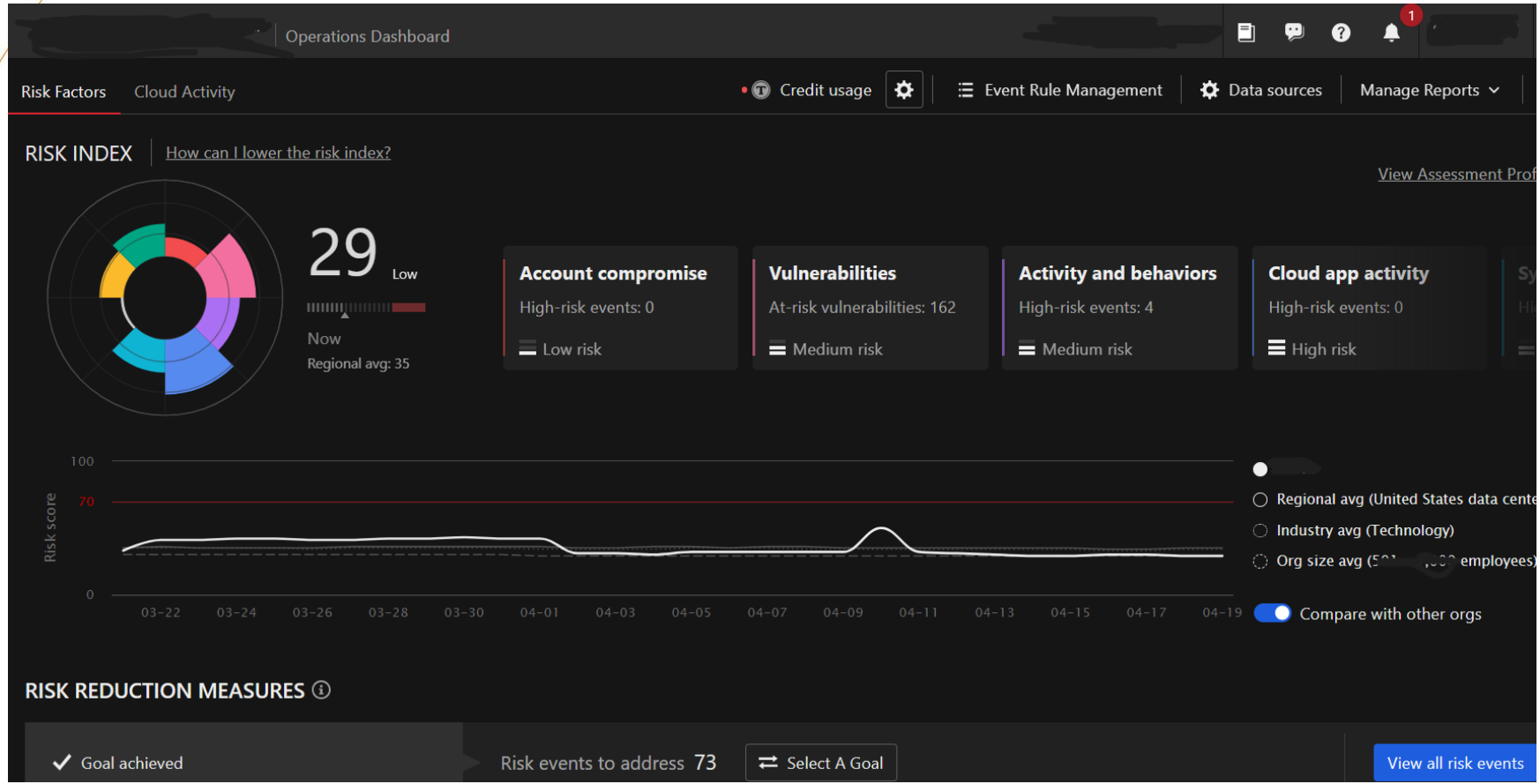
Cenário de um Incidente Cibernético GRAVE!

- Resgate pedido para descriptografar o ambiente US$ 2.400.000,00 por 90 dias.
- Paralização de todas as operações administrativas, comerciais e industriais, perda de receita e aumento nos custos operacionais estimados em R$3.500.000,00
- Custo financeiro da reconstrução total dos ambientes de tecnologia afetados e da investigação/forense. R$ 2.800.000,00;
- 11 ações de responsabilização civil e 2 processos em andamento que podem resultar em multas e indenizações por questões de privacidade.

Principais ações e controles adotados, após incidente.

- Contratação de empresa especializada para defesa de crimes digitais;
- Implementação de estrutura de segurança cibernética (SOC 24x7) e de segurança da informação (CISO-AAS);
- Reconstrução de toda estrutura de usuários, computadores, servidores e rede com segmentação e isolamento das redes por firewalls integrados com IDSP, IPS, Antivírus e Gerenciados de Contas e Senhas;
- Modificação e implantação de políticas mais severas para uso de recursos de TI e para comportamento cibernético;
- Implantação da equipe de Auditoria e Compliance de TI e Segurança da Informação para monitoramento e gestão de riscos cibernéticos;

Cenário de um Incidente Cibernético GRAVE!



ABAC
ASSOCIAÇÃO BRASILEIRA DE ADMINISTRADORAS DE CONSÓRCIOS

Obrigado!