

CHEWY Company

Cloud Security Services Project

AGENDA

01

Our Team

02

Problem Domain

03

Project Overview

04

Process

05

Demo

06

Documentation

07

Final Thoughts

08

Q & A

Our Team



CSS
CLOUD SECURITY SERVICES

01

André Graça

02

Rodrigo Brasil

03

Ricardo Graça

04

Tiago Godinho

+++

André Graça

Age: 40

- Place of birth: Lisbon
- Married with 3 children
- Member of the Portuguese Navy since November 2001
- Specialized in Computer Technician and network administration in 2013 by the Navy.
- Specialized in cybersecurity in the area of offensive operations in 2023 by the EMGFA (General Staff of the Armed Forces) in partnership with the Polytechnic Institute of Beja.



Rodrigo Brasil

Age: 24

Place of birth: Angra do Heroísmo

IT Technician

Studied IT - Systems for 3 years, after graduation started working as an intern at a local secondary school for a year and half, while working there started to find interest in offensive cybersecurity, a few months passed finished the internship, tried my luck with code_for_all and now here i am.

<https://www.linkedin.com/in/rbrasil72/>



Ricardo Graça

Age: 32

Place of birth: Lisbon

Dental Technician

Cyber Security Student





Tiago Godinho

Age:

Place of birth:

(Talk a little bit about yourself here)

Problem Domain - Client Requirements

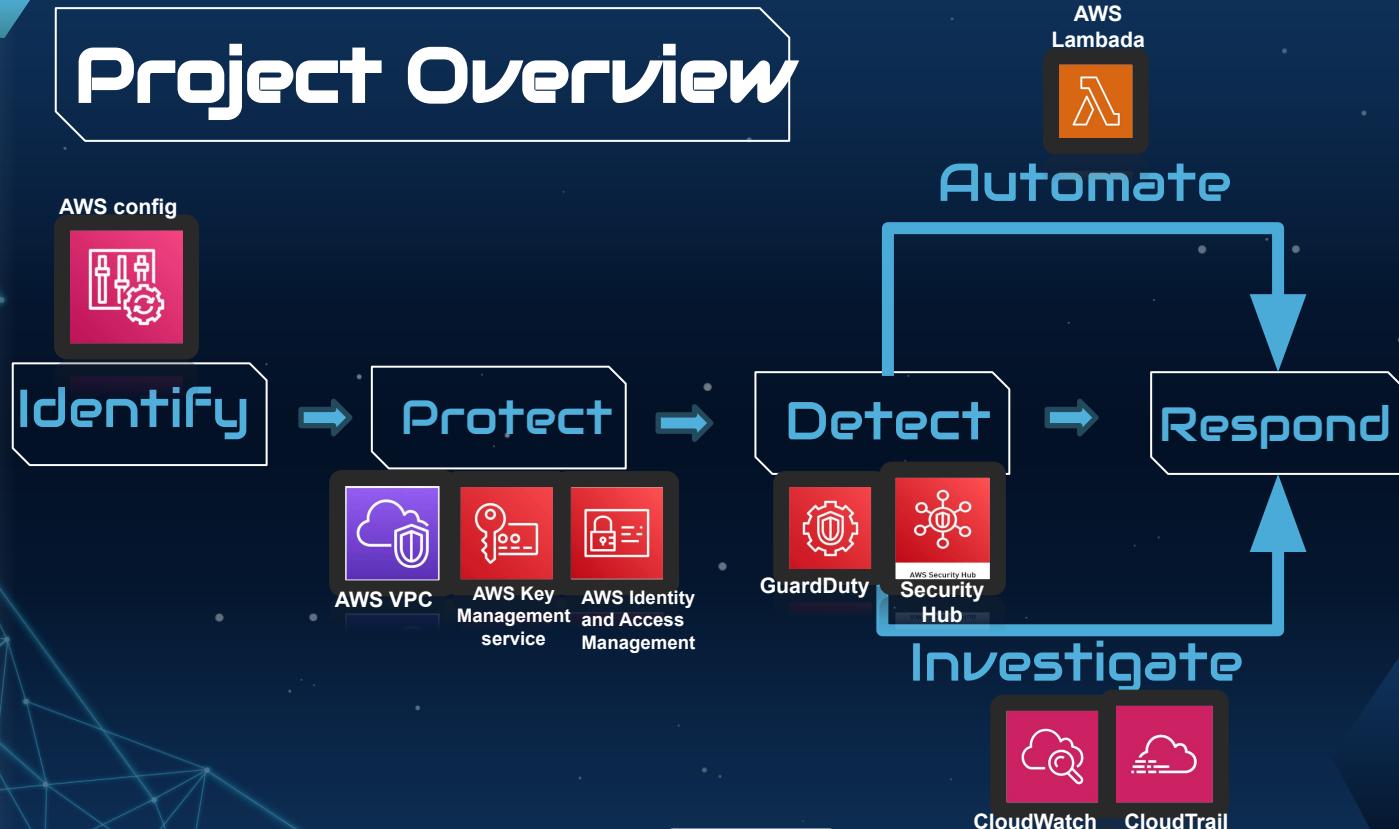
- The Chewy company with the expansion of customers to the international market is having problems with GDPR (consumer privacy regulations).
- However it has to implement some systems and processes to remain GDPR compliant so that customers know that the company takes PII/PCI data privacy seriously.
- Chewy wants to use AWS as ACP

WE need

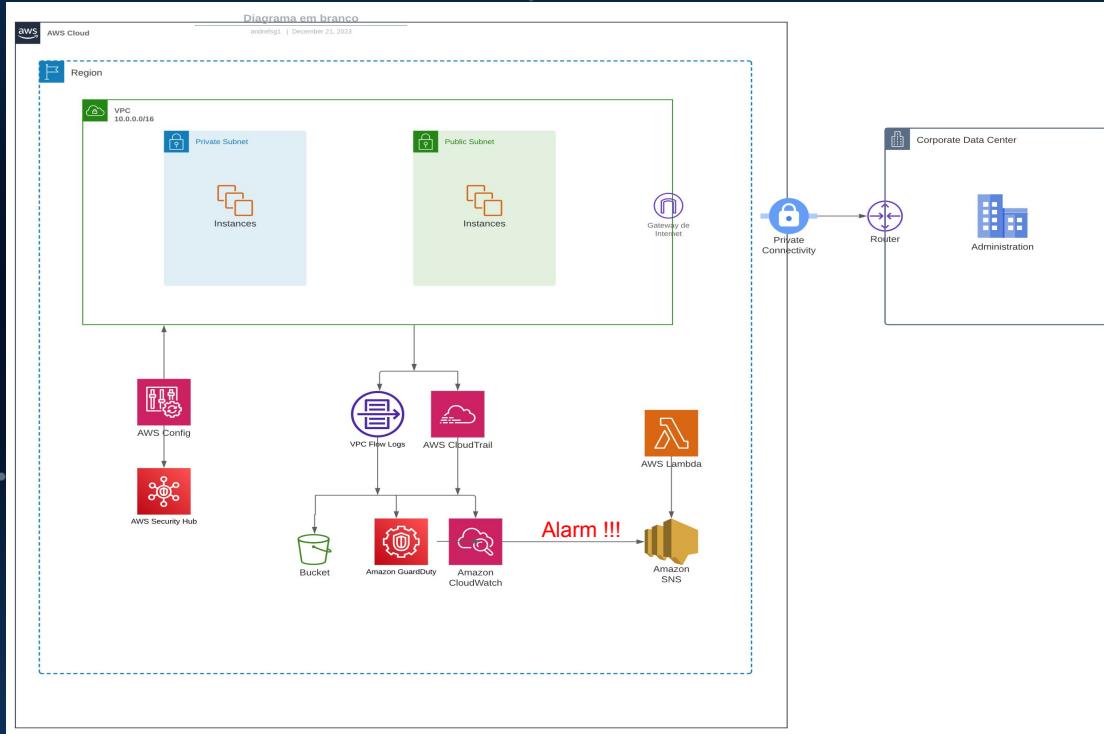
- Proper implementation of IAM Best Practices
- CIS-Compliant Data Server Containing PII/PCI Data
- SIEM/Log Aggregation System
- Cloud Monitoring via Flow Logs/Lambda
- Data Loss Prevention (DLP) Detection and Response



Project Overview



Network Topology AWS



Process - IAM (AWS Identity and Access Management)

- Create Group for AWS Admins With 'Administrator Access Permission'
- Create an User for all Tree AWS Admin and Allocate to AWS Admins Group
- Avoid Usage of Root Account
- Enable MFA for Root Account and All highly privileged users

Process AWS VPC

Users (5) Info

An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

	User name	Path	Groups	Last activity
<input type="checkbox"/>	Chewy-admin	/	1	
<input type="checkbox"/>	chewy-user1	/	1	
<input type="checkbox"/>	chewy-user2	/	1	
<input type="checkbox"/>	chewy-user3	/	1	
<input type="checkbox"/>	Chewy2-admin	/	1	

Root user has MFA

Having multi-factor authentication (MFA) for the root user improves security for this account.

CHEWY-Users Info

Summary

User group name: CHEWY-Users

Creation time: December 18, 2023, 20:50 (UTC)

Users (3) Info

Permissions

Permissions policies (2) Info

You can attach up to 10 managed policies.

	Policy name	Type
<input type="checkbox"/>	SecurityAudit	AWS managed - job function
<input type="checkbox"/>	ViewOnlyAccess	AWS managed - job function

CHEWY-Admins Info

Summary

User group name: CHEWY-Admins

Users (2) Info

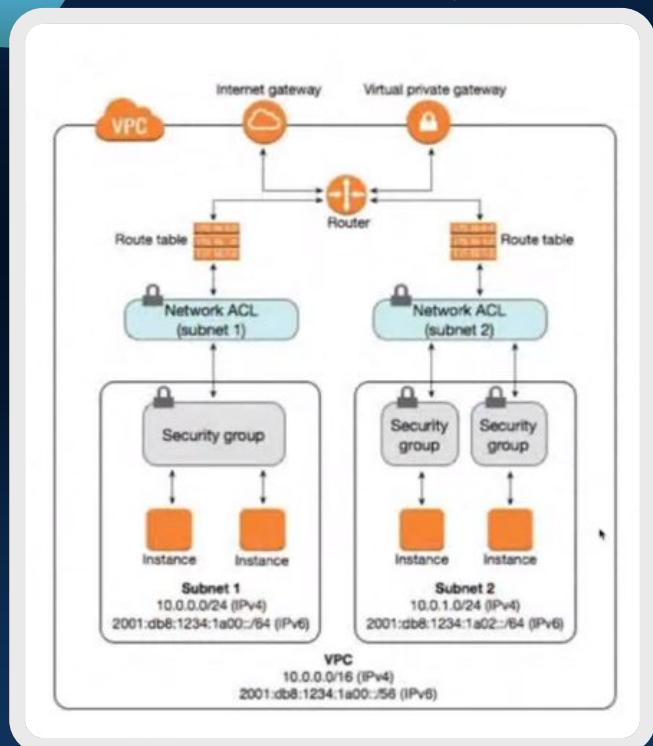
Permissions

Permissions policies (1) Info

You can attach up to 10 managed policies.

	Policy name
<input type="checkbox"/>	AdministratorAccess

Process - VPC



Public Security group Inbound:

IP version	Type	Protocol	Port range	source
IPv4	ssh	TCP	22	0.0.0.0/0
IPv4	All ICMP-IPv6	IPv6 ICMP	All	0.0.0.0/0
IPv4	All ICMP-IPv6	ICMP	All	0.0.0.0/0

Private Security group Inbound:

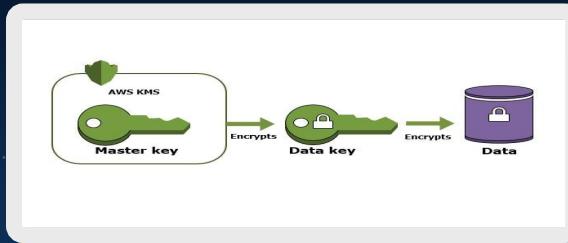
IP version	Type	Protocol	Port range	source
Ipv4	ssh	TCP	22	10.0.0.0/16

- **VPC/Subnets – Offer Network Segregation**
- **Security Groups – EC2 Virtual Firewall**
- **NACL – VPC Level Firewall**

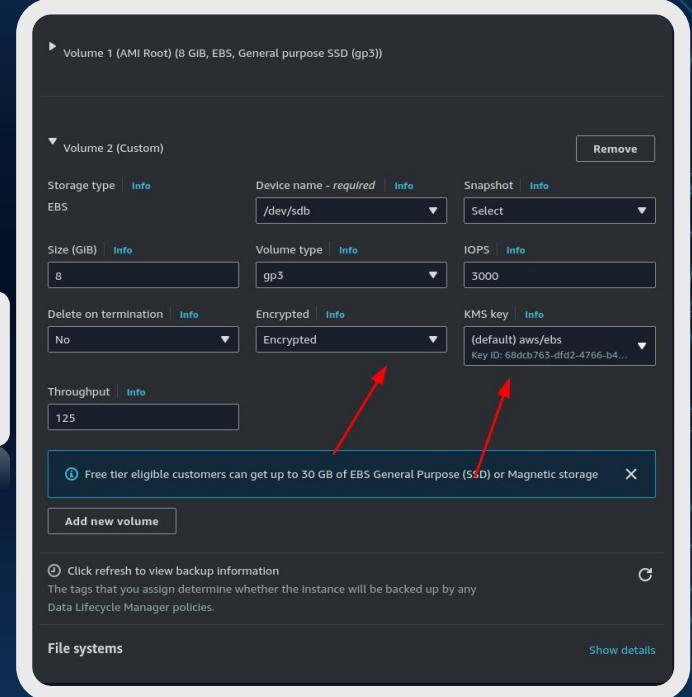
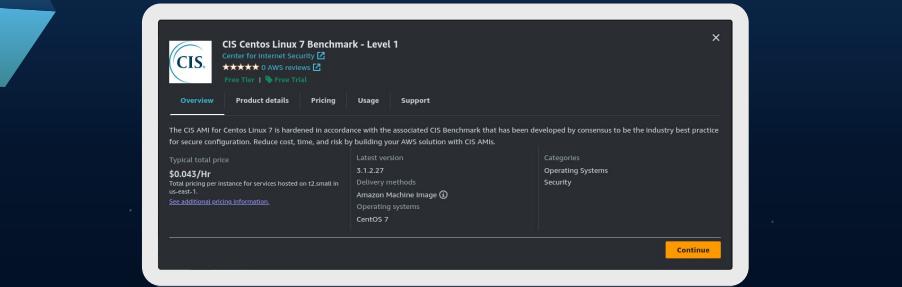


Process - EC2 and KMS

- Instances Hardened With CIS Benchmark AMI
- Security Groups Attached
- AWS EBS encryption uses AWS KMS keys when creating encrypted volumes.
- Different RSA Key Pair Attached to Each Machine



Process - EC2 and KMS



Key Management Service ☆

Securely Generate and Manage AWS Encryption Keys

Review

Key configuration

Key type Asymmetric	Key spec RSA_2048	Key usage Encrypt and decrypt
Origin AWS KMS	Regionality Single-Region key	

You cannot change the key configuration after the key is created.

Volume 1 (AMI Root) (8 GiB, EBS, General purpose SSD (gp3))

Volume 2 (Custom)

Storage type: EBS

Device name - required: /dev/sdb

Snapshot: Select

Size (GiB): 8

Volume type: gp3

IOPS: 3000

Delete on termination: No

Encrypted: Encrypted

KMS key: (default) aws/eks
Key ID: 68dcfb765-dfd2-4766-b4...

Throughput: 125

Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage

Add new volume

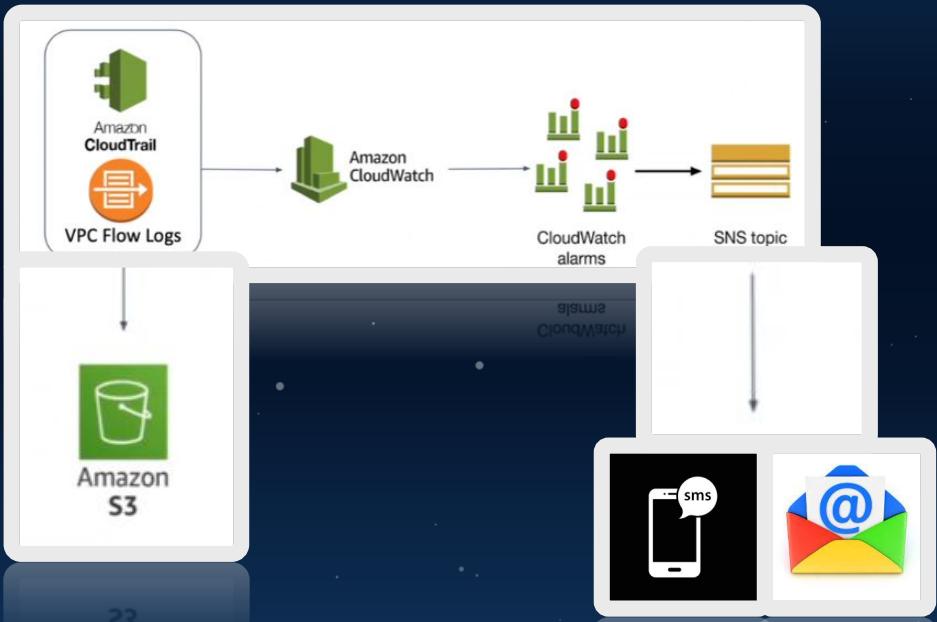
Click refresh to view backup information

The tags that you assign determine whether the instance will be backed up by any Data Lifecycle Manager policies.

File systems

Show details

Process - Monitoring and Alert

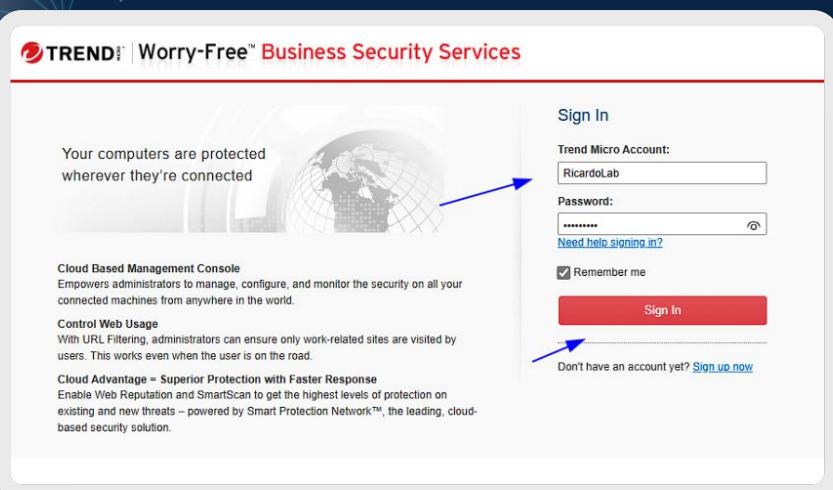


Process - DLP Controls

- Install a Trend Micro endpoint security agent software
- Baseline Evaluation
- Implementation of the DLP policy and Current Evaluation

+++

Process - DLP Controls



TREND Micro Worry-Free™ Business Security Services

Your computers are protected wherever they're connected

Cloud Based Management Console
Empowers administrators to manage, configure, and monitor the security on all your connected machines from anywhere in the world.

Control Web Usage
With URL Filtering, administrators can ensure only work-related sites are visited by users. This works even when the user is on the road.

Cloud Advantage = Superior Protection with Faster Response
Enable Web Reputation and SmartScan to get the highest levels of protection on existing and new threats – powered by Smart Protection Network™, the leading, cloud-based security solution.

Sign In

Trend Micro Account:

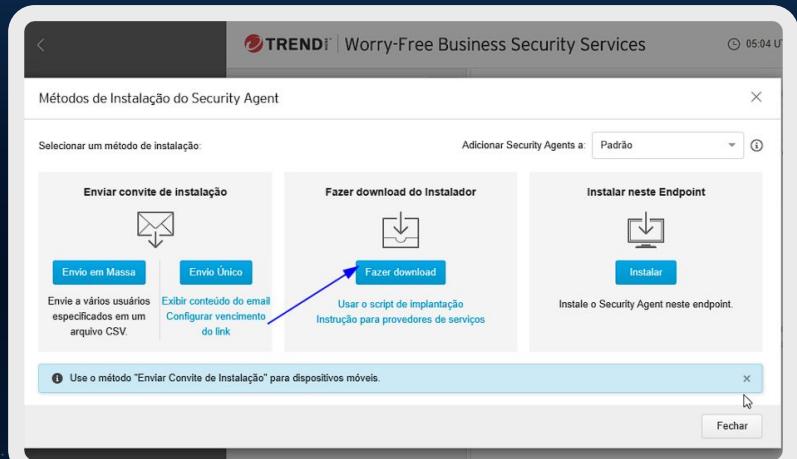
Password:

[Need help signing in?](#)

Remember me

Sign In

Don't have an account yet? [Sign up now](#)



TREND Micro Worry-Free Business Security Services

05:04 U

Métodos de Instalação do Security Agent

Selecionar um método de instalação:

Enviar convite de instalação

Fazer download do instalador

Instalar neste Endpoint

Enviar convite de instalação

Fazer download

Instalar

Envio em Massa

Envio Único

Exibir conteúdo do email

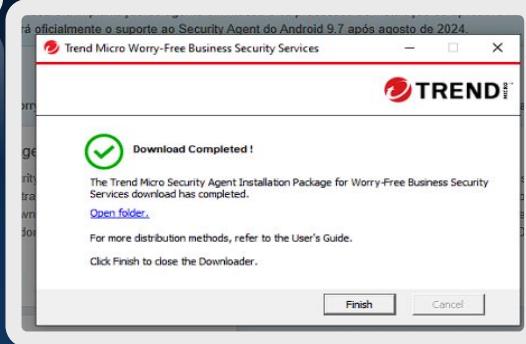
Configurar vencimento do link

Usar o script de implantação

Instrução para provedores de serviços

Instale o Security Agent neste endpoint.

Use o método "Enviar Convite de Instalação" para dispositivos móveis.



TREND Micro Worry-Free Business Security Services

Download Completed!

The Trend Micro Security Agent Installation Package for Worry-Free Business Security Services download has completed.

[Open folder](#)

For more distribution methods, refer to the User's Guide.

Click Finish to close the Downloader.

Finish **Cancel**



Process - DLP Controls

SSN	gender	birthdate	maiden name	last name	first name
172-32-1176	m	4/21/1958	Smith	White	Johnson
514-14-8905	f	12/22/1944	Amaker	Borden	Ashley
213-46-8915	f	4/21/1958	Pinson	Green	Marjorie
524-02-7657	m	3/25/1962	Hall	Munsch	Jerome
489-36-8350	m	1964/09/06	Porter	Aragon	Robert
514-30-2668	f	1986/05/27	Nicholson	Russell	Jacki
505-88-5714	f	1963/09/23	Mcclain	Venson	Lillian
690-05-5315	m	1969/10/02	Kings	Conley	Thomas
646-44-9061	M	1978/01/12	Kurtz	Jackson	Charles
421-37-1396	f	1980/04/09	Linden	Davis	Susan

address	city	state	zip	phone
10932 Bigge Rd	Menlo Park	CA	94025	408 496-7223
4469 Sherman Street	Goff	KS	66428	785-939-6046
309 63rd St. #411	Oakland	CA	94618	415 986-7020
2183 Roy Alley	Centennial	CO	80112	303-901-6123
3181 White Oak Drive	Kansas City	MO	66215	816-645-6936
3097 Better Street	Kansas City	MO	66215	913-227-6106
539 Kyle Street	Wood River	NE	68883	308-583-8759
570 Nancy Street	Morrisville	NC	27560	919-656-6779
1074 Small Street	New York	NY	10011	212-847-4915
4222 Bedford Street	Jasper	AL	35501	205-221-9156
3414 Gore Street	Houston	TX	77002	713-547-3414
515 Hillside Drive	Lake Charles	LA	70629	337-965-2982
4032 Arron Smith Drive	Kaunakakai	HI	96748	808-560-1638

Policies not enabled

Ricardo Graça <spitfirept91@gmail.com>
para ricardomachadograça ▾
05:03 (há 0 minutos)

Testing SSN CCN pfg

Um anexo • Verificado pelo Gmail

PDF sample-data.pdf

Process - DLP Controls

Configurações gerais

Ativar essa regra

Nome da regra: * SSN CCN

Descrição:

Modelo

Selecione modelos de Prevenção de perda de dados para definir o tipo de dados confidenciais a monitorar. [Saiba mais](#)

Todos os modelos ▾ euu

Modelo (3/18)

- EUA: Informações financeiras e bancárias
- EUA: Lei Sarbanes-Oxley
- EUA: NPI (National Provider Identifier)
- EUA: Número de identificação ABA
- EUA: PCI-DSS
- EUA: PII (Personally Identifiable Information)
- EUA: SB-1386
- EUA: SSN (Social Security Number)

Canal

Selecione os tipos de canais que o Prevenção de perda de dados monitora

- Canais de rede
- Canais de aplicativo e sistema

Crie regras de bloqueio e alertas

Crie regras de alerta

Regras de alerta que criou deve o Prevenção de perda de dados que bloqueia automaticamente

CRM

Canal

Selecione os tipos de canais que o Prevenção de perda de dados monitora

- Canais de rede
 - Clientes de e-mail
 - FTP
 - HTTP
 - HTTPS
 - Protocolo SMB
 - Aplicativos IM
 - Webmail

Escopo da transmissão

O Prevenção de perda de dados monitora as seguintes transmissões através de canais de rede selecionados.

- Todas as transmissões
 - Monitora dados transmitidos fora do computador host
- Somente transmissões fora da Rede local
 - Monitora dados transmitidos para qualquer destino fora da rede local (LAN) [\(i\)](#)

Configurações de Destino e Serviço

ATIVADO

Prevenção de perda de dados

A Prevenção de Perda de Dados monitora ou bloqueia transmissões de dados confidenciais pela rede.

Regras **Exceções**

Criar regras para Prevenção de perda de dados a fim de monitorar ou bloquear transmissões de dados confidenciais pela rede.

Regra	Modelo	Canal	Ação	Ativa
SSN CCN	EUA: Informações financeiras e ...	Aplicativos ponto a ponto, Aplicat...	Bloquear	<input checked="" type="checkbox"/>

CONTROLE DE ACESSO



Process - DLP Controls

TRENDI | Worry-Free Business Security Services

04:30 UTC+00:00 RicardoLal

Security Agents

- Todos os Agentes de Segurança** (1)
- Grupos Manuais**
 - Servidor (Padrão) (0)
 - Dispositivo (Padrão) (1)
- Agentes de Segurança Desatual...** (0)
- Endpoints Não Gerenciados** (0)

DESKTOP-H453C12

Verificações **Tarefas**

Informações **Eventos** (green arrow)

Detecções de Risco à Se... **Últimos 7 dias** **Ameaça/Violação**

Recebido	Categoria	Ameaça/Violaçã...	Caminho do Arq...	Ação/Resultado	Usuário	Detalhes
22/12/2023 04...	Prevenção de ...	SSN CCN	C:\Users\Lab\ID...	Bloqueado	Lab	
22/12/2023 04...	Prevenção de ...	SSN CCN	C:\Users\Lab\ID...	Bloqueado	Lab	
21/12/2023 21...	Prevenção de ...	SSN CCN	C:\Users\Lab\ID...	Bloqueado	Lab	
21/12/2023 16...	Prevenção de ...	SSN CCN	C:\Users\Lab\ID...	Bloqueado	Lab	
21/12/2023 16...	Prevenção de ...	SSN CCN	C:\Users\Lab\ID...	Bloqueado	Lab	
21/12/2023 16...	Prevenção de ...	SSN CCN	C:\Users\Lab\ID...	Bloqueado	Lab	
21/12/2023 15...	Prevenção de ...	SSN CCN	C:\Users\Lab\ID...	Bloqueado	Lab	
21/12/2023 15...	Prevenção de ...	SSN CCN	C:\Users\Lab\ID...	Bloqueado	Lab	
21/12/2023 15...	Prevenção de ...	SSN CCN	C:\Users\Lab\ID...	Bloqueado	Lab	
21/12/2023 15...	Prevenção de ...	SSN CCN	C:\Users\Lab\ID...	Bloqueado	Lab	

Detalhes dos logs de prevenção de perda de dados

Canal: Webmail (Gmail)
Gerado: 22/12/2023 04:15:19
Recebido: 22/12/2023 04:17:18

Endpoint

Nome do endpoint: DESKTOP-H453C12
Domínio: -
Usuário: Lab
Nome do grupo: Dispositivo (Padrão)

Regras Violadas

Regra	Modelo	Ação/Resultado
SSN CCN	US. SSN (Social Security Number) US. PI (Perso...	Transmissão de dados bloqueada

Detecção

Processo: C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
Origem: C:\Users\Lab\Desktop\sample-data.pdf
Destino: mail.google.com/mail/u/0/#inbox?compose=Dmwn\WtMnXdfHrqZVkmppmDhKVDDDjssFbwPvlfhxRR|DGRPmLMDJzbNwFxStXmJJRRtqKfwgV
URL: mail.google.com/mail/u/0/#inbox?compose=Dmwn\WtMnXdfHrqZVkmppmDhKVDDDjssFbwPvlfhxRR|DGRPmLMDJzbNwFxStXmJJRRtqKfwgV
Usuário de FTP: -
Classe do arquivo: text
Tamanho do arquivo/dados: 53.6 KB (54 902 bytes)
Emissor do email: -
Assunto do email: -
Destinatários do email: -

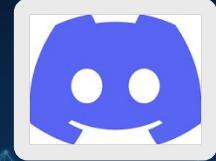
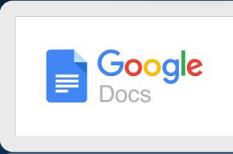
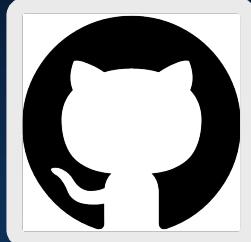
Resources & Thanks

- Github Organization: <https://github.com/Cloud-Security-Services>
- Google docs :https://drive.google.com/drive/folders/1ebJZDQex0466qEpAmkxGuLJ7v2rArOFB?usp=drive_link
- Amazon web Services: <https://aws.amazon.com/console/>

Shout out and thank you to those that have helped contributed to the process of this project



+++



+++

Questions?