TLP:CLEAR

Estruturando Visão Gerencial e Dashboard para o MISP

Laboratório De Segurança Cibernética

FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

Introdução

Analista de Cybersecurity

FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

Laboratório de Segurança Cibernética — 2019

- Capacitação
- Simulação
- Inteligência
- Padronização
- Inovação

TLP:CLEAR

Laboratório

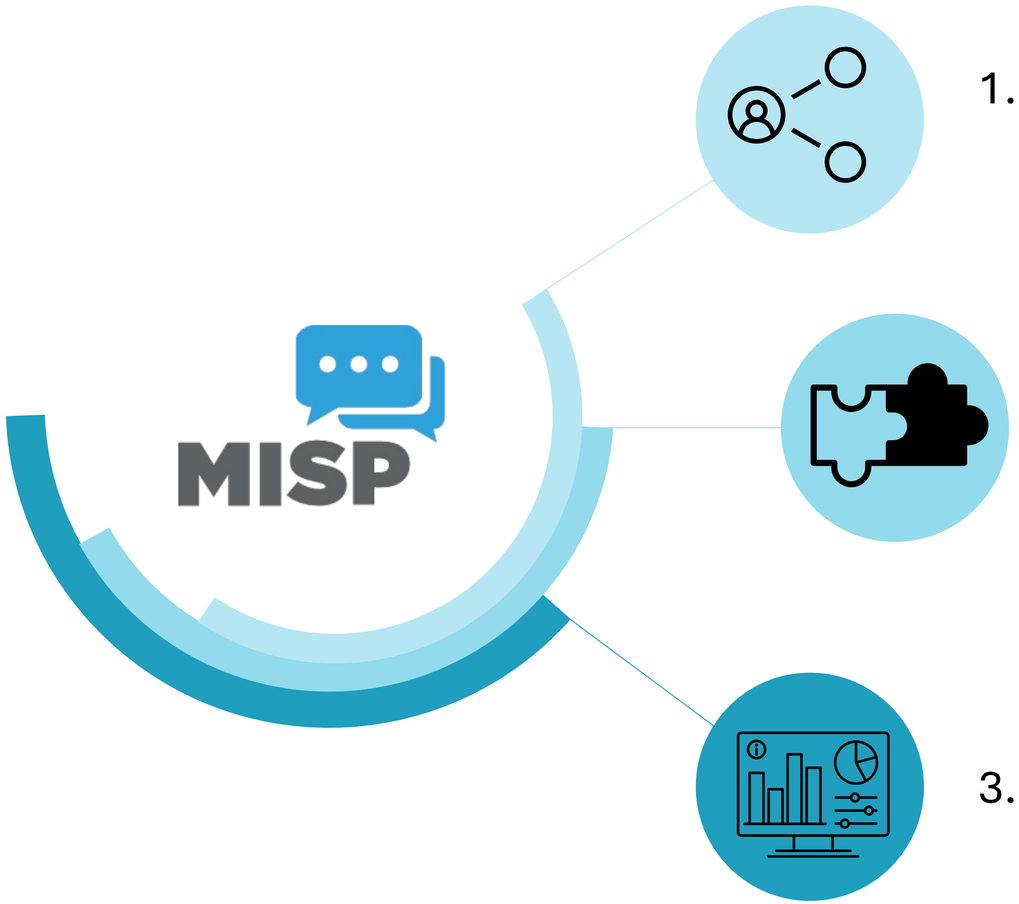
FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

Laboratório de Segurança Cibernética

Inteligência

- Relatórios Técnicos/Executivos
- Threat Intelligence Report
- Investigações
- **MISP**

OBJETIVO



1. Compartilhar evolução do uso do MISP
2. Encorajar integração com ferramentas externas
3. Dar visibilidade para os dados do MISP

PROVOCAÇÕES RECEBIDAS

O que temos no MISP atualmente?

O que está sendo compartilhado?

O que nós estamos compartilhando?

De quem estamos recebendo informações?

Como estão as contribuições das instituições?

SOLUÇÕES PROPOSTAS

MISP	01	**MIPS Dashboard**	❑ Já integrado com a instalação ❑ Menor possibilidade de customização rápida
	02	**ELK Stack**	❑ Maior tempo de implementação ❑ Maior complexidade na ingestão
	03	**AWS Opensearch**	❑ Similar ao ELK ❑ Maior custo e complexidade
	04	**Metabase**	❑ Interessante pela simplicidade e custo

PLANEJAMENTO E IMPLEMENTAÇÃO

Metabase

JAR File Local

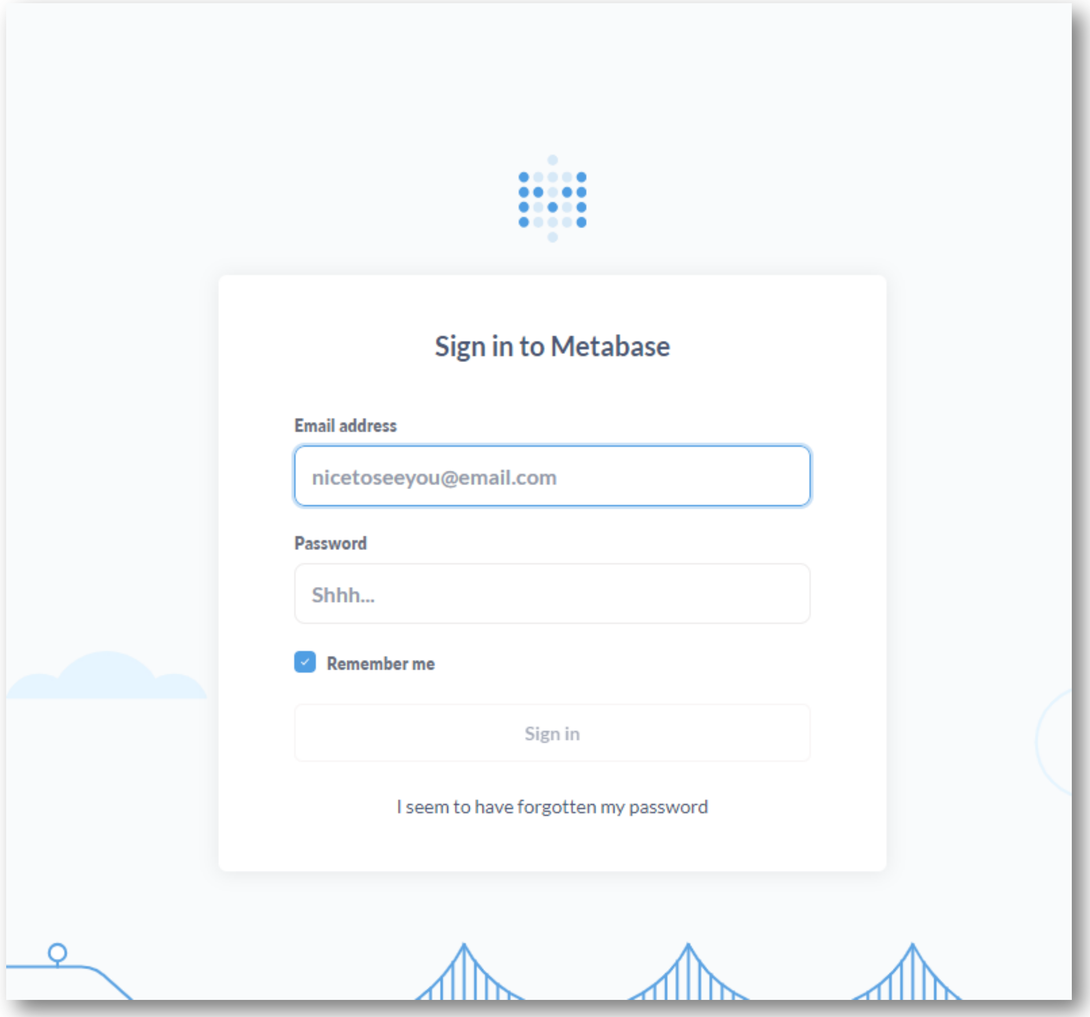
1. Instalar Java JRE
2. Baixar Metabase (JAR)
3. Executar

   java –jar metabase.jar
4. Acessar interface *http://localohst:3000*

   Outra porta pode ser configurada com a variável *MB_JETTY_PORT*

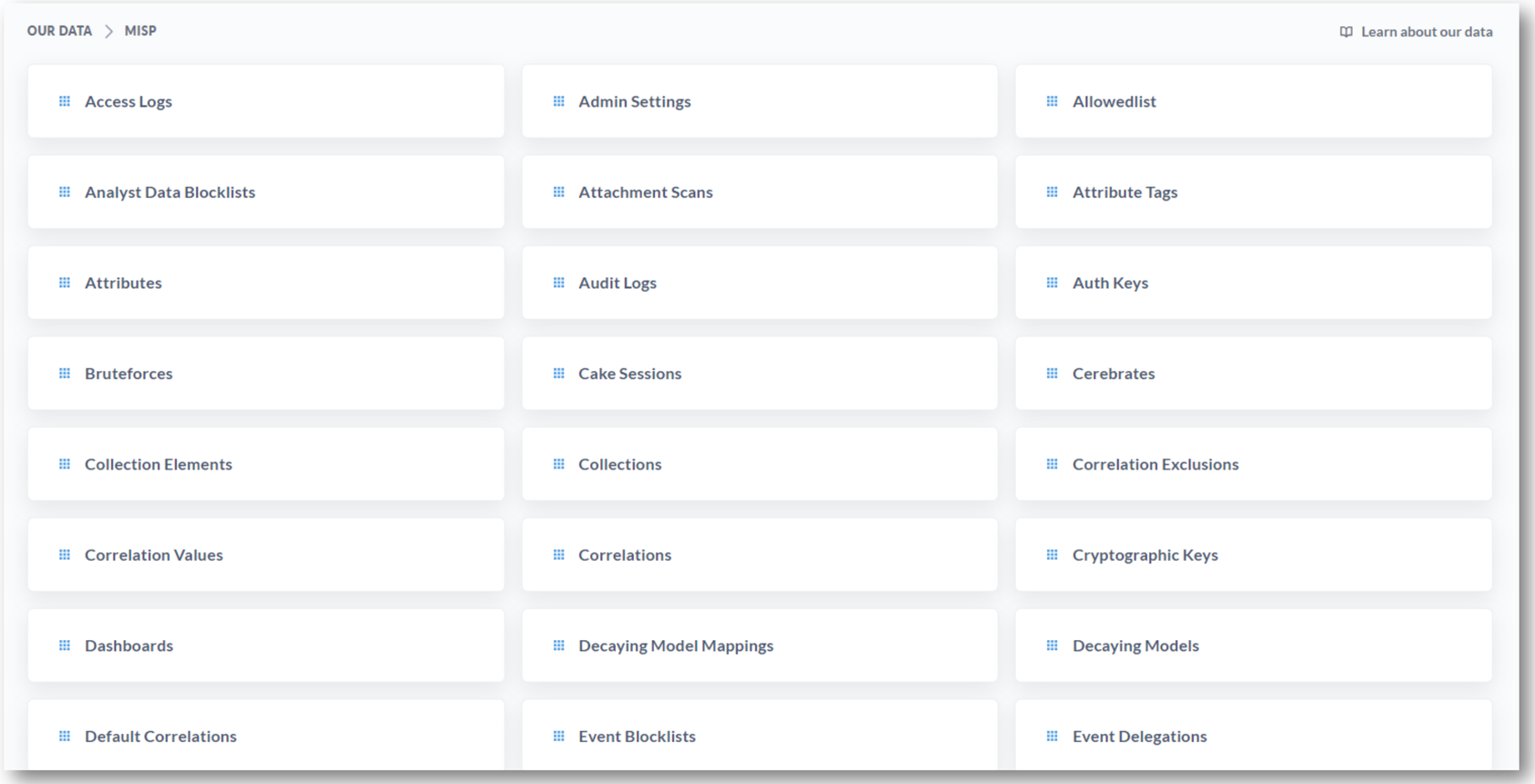
PLANEJAMENTO E IMPLEMENTAÇÃO

Metabase



PLANEJAMENTO E IMPLEMENTAÇÃO

Metabase



TLP:CLEAR

BANCO DE DADOS MISP

FEBRABAN

access_logs	admin_settings	allowedlist	analyst_data_blocklists	attachment_scans	attribute_tags	attributes	audit_logs	auth_keys	bruteforces
cake_sessions	cerebrates	collection_elements	collections	correlation_exclusions	correlation_values	correlations	cryptographic_keys	dashboards	decaying_model_mappings
decaying_models	default_correlations	event_blocklists	event_delegations	event_graph	event_locks	event_reports	event_tags	events	favourite_tags
feeds	fuzzy_correlate_ssdeep	galaxies	galaxy_cluster_blocklists	galaxy_cluster_relation_tags	galaxy_cluster_relations	galaxy_clusters	galaxy_elements	inbox	jobs
logs	news	no_acl_correlations	notes	noticelist_entries	noticelists	notification_logs	object_references	object_relationships	object_template_elements
object_templates	objects	opinions	org_blocklists	organisations	over_correlating_values	posts	regexp	relationships	rest_client_histories
roles	servers	shadow_attribute_correlations	shadow_attributes	sharing_group_blueprints	sharing_group_orgs	sharing_group_servers	sharing_groups	sighting_blocklists	sightingdb_orgs
sightingdbs	sightings	system_settings	tag_collection_tags	tag_collections	tags	tasks	taxii_servers	taxonomies	taxonomy_entries
taxonomy_predicates	template_element_attributes	template_element_files	template_element_texts	template_elements	template_tags	templates	threads	threat_levels	user_login_profiles
user_settings	users	warninglist_entries	warninglist_types	warninglists	workflow_blueprints	workflows			

TLP:CLEAR

CONSIDERAÇÕES FINAIS

- Não existe uma única melhor solução
- Temos várias formas de extrair indicadores
- Visibilidade para os compartilhamentos
- Apoio e justificative do investimento na estrutura

Perguntas?

TLP:CLEAR

Obrigado!

Henrique Kodama

henrique.kodama@febraban.org.br

linkedin.com/in/hskodama/

Laboratório

labsegciber@febraban.org.br

FEBRABAN