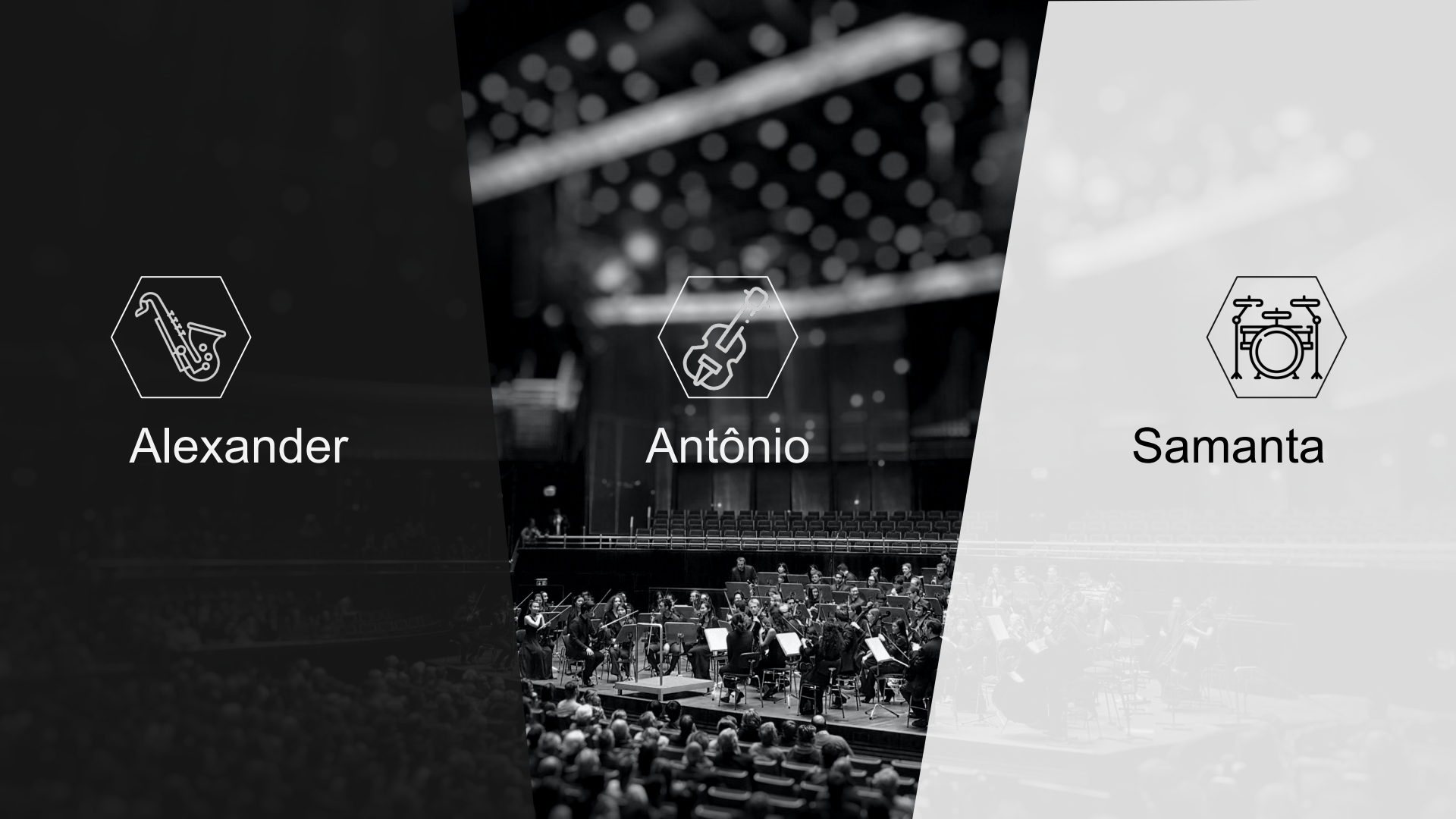
Orquestra CSIRT

A sintonia do Blue Team na resposta a incidentes e proteção corporativa


Alexander
Antônio
Samanta

Alexander

- Pai da Mama, Nick e Oli
- Apaixonado por segurança, trabalhando com Cyber há 23 anos, com foco em Identidade Digital e Defesa Cibernética
- Pós Graduado Segurança e Inteligência Cibernética
- Apaixonado por esportes (principalmente futebol), churrasco e cozinhar

Antônio

Samanta

Alexander

Antônio

- +19 anos em tecnologia sendo 10 com Segurança da Informação
- Pos graduando Segurança da Informação e Governança
- Resposta a Incidente, Análise de Artefatos, Arquitetura de CyberSecurity e Operação. Certicado ITIL / CHFI
- Head do MDR e contrabaixista nas horas livres

Samanta

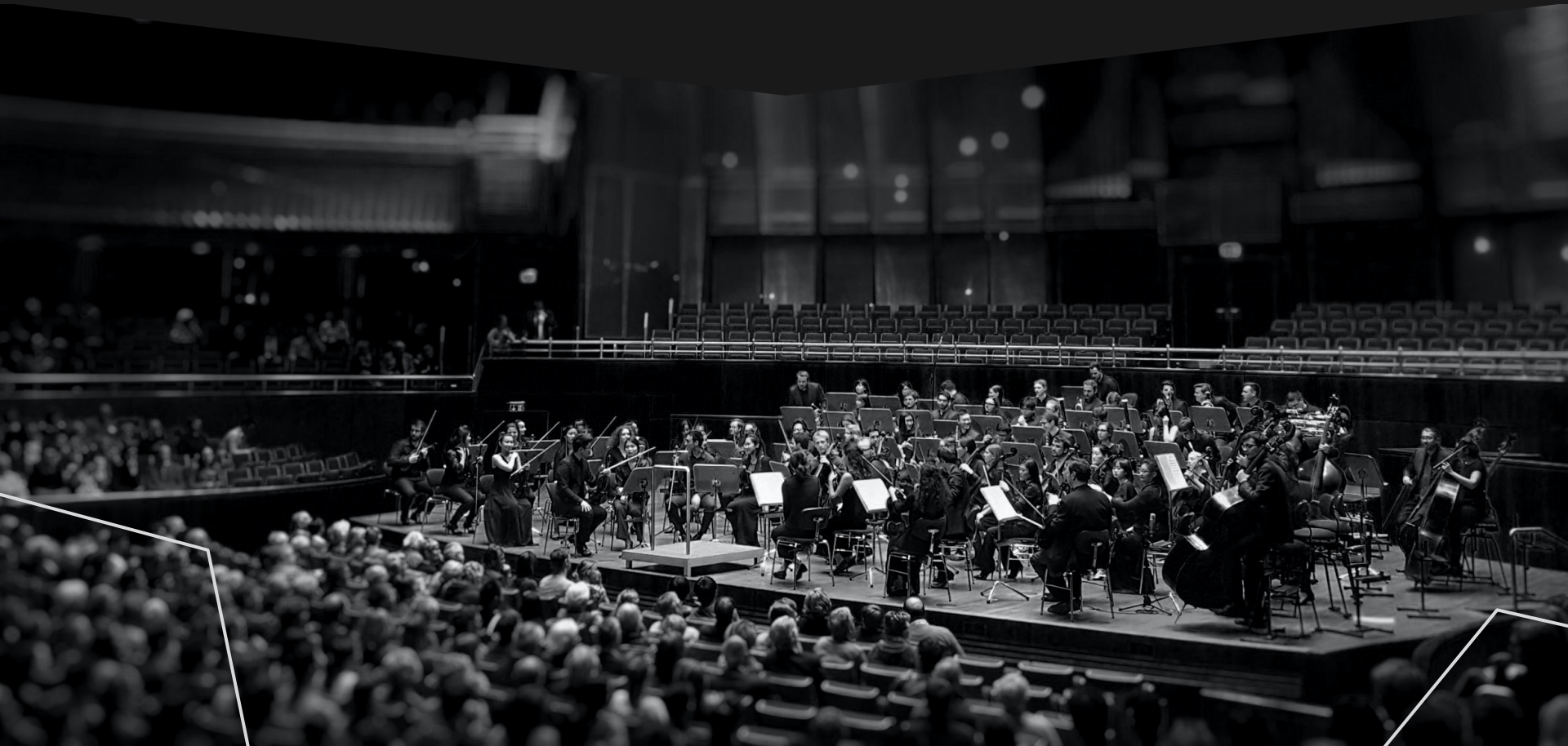
Alexander

Antônio

Samanta

- Bacharel em Ciência da Computação
- MBA em Governança, Riscos e Compliance
- Mestranda Inteligência Artificial
- +10 anos em Cybersegurança
- Threat Intelligence & Hunting

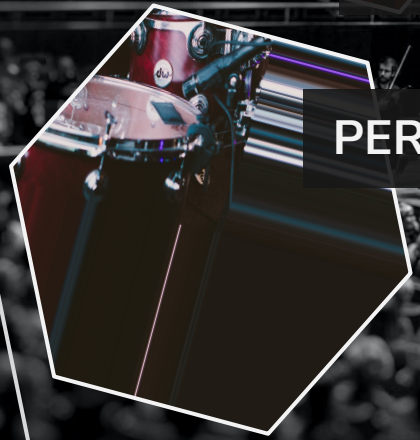
UMA ORQUESTRA É UM CONJUNTO DE VÁRIOS INSTRUMENTOS



ELA É COMPOSTA POR 4 TIPOS DE INSTRUMENTO

CORDA

MADEIRA



PERCUSSÃO

METAIS

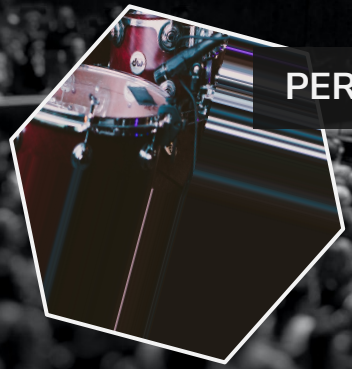
E CADA INSTRUMENTO CONTRIBUI EM SINTONIA DE ACORDO COM A SINFONIA NA PARTITURA E GUIADA POR UM MAESTRO

CORDA

PARTITURA

METAIS

MAESTRO



PERCUSSÃO

MADEIRA

DO MESMO JEITO FUNCIONA A RESPOSTA A INCIDENTES, QUE DEPENDE DE TODOS OS TIMES TRABALHANDO EM SINTONIA

01

HUNTING

Assim como os instrumentos de percussão, o Hunting é a base da detecção

Identificação de novas ameaças

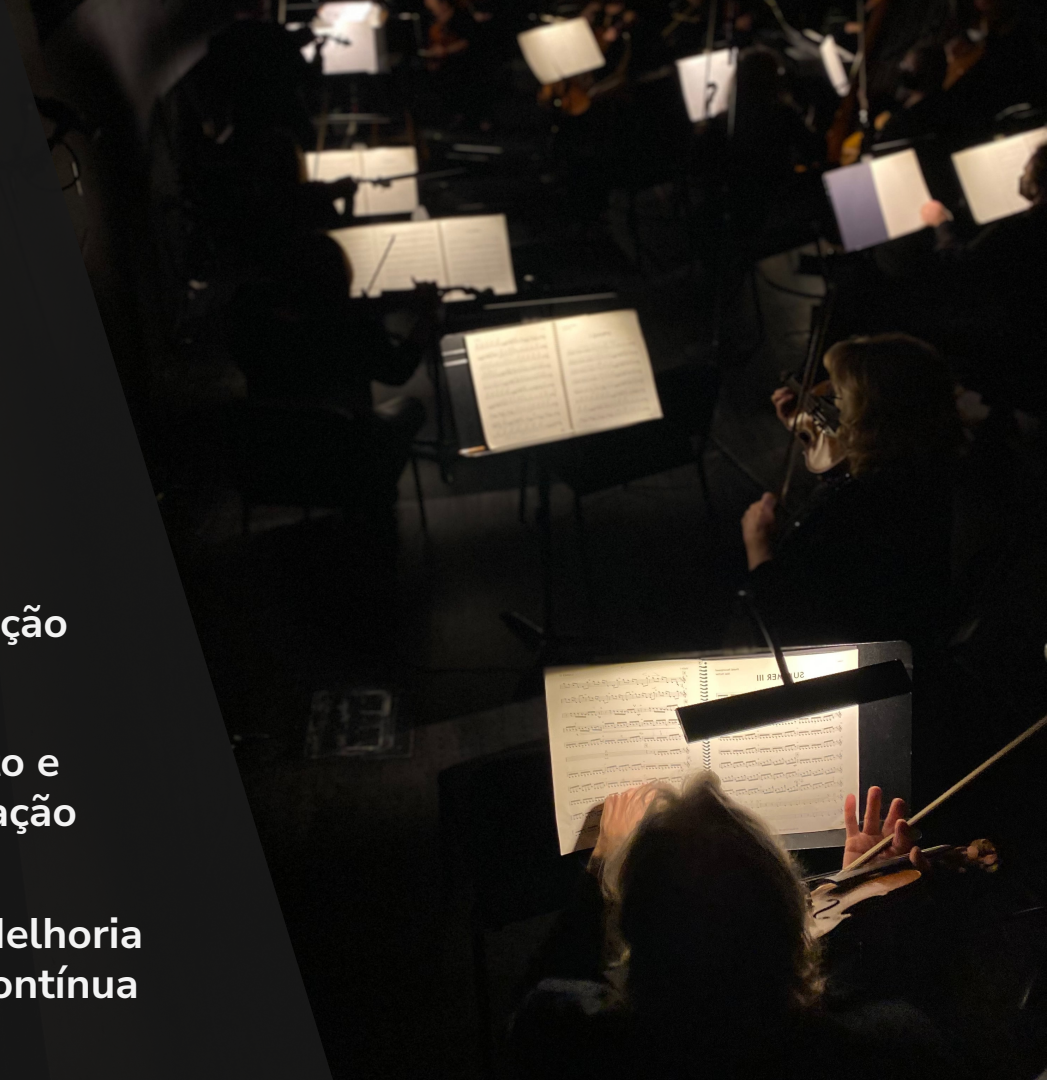
Desenvolvimento do alerta

Homologação e tunning

Documentação

Treinamento e implementação

Melhoria contínua



02

MDR (N1)

Os instrumentos de corda, assim como o MDR, são a linha de frente da equipe

MDR

-37%
Tempo de resposta

+30%
Alertas respondidos no SLA

ATUAÇÃO DO TIME

- Inicia os trabalhos e passa os primeiros ritmos para os times
- Documentação aqui é imprescindível
- Treinamentos e ensaios são os pontos chave
- Cultura de desenvolvimento interno
- Tomada de decisão rápida

03

CSIRT (N2 e N3)

Os instrumentos de madeira vem logo após os de corda junto dos metais, completando o centro da orquestraçao

CSIRT

Músicos que tiram melodia de ouvido

O playbook serve como norteador, o importante é que esse time saiba como a melodia está tocando e como deve ser seguido o ritmo.

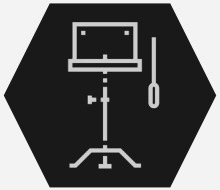
Revisão dos cases

Análise constante de falso positivos e causa raiz para construir e revisar documentação

Com treinamento constante integramos equipes técnicas e de segurança para responder incidentes

PARA QUE A RESPOSTA A INCIDENTES FUNCIONE EM SINCRONIA É PRECISO INTEGRAR TODOS OS TIMES

Treinamento



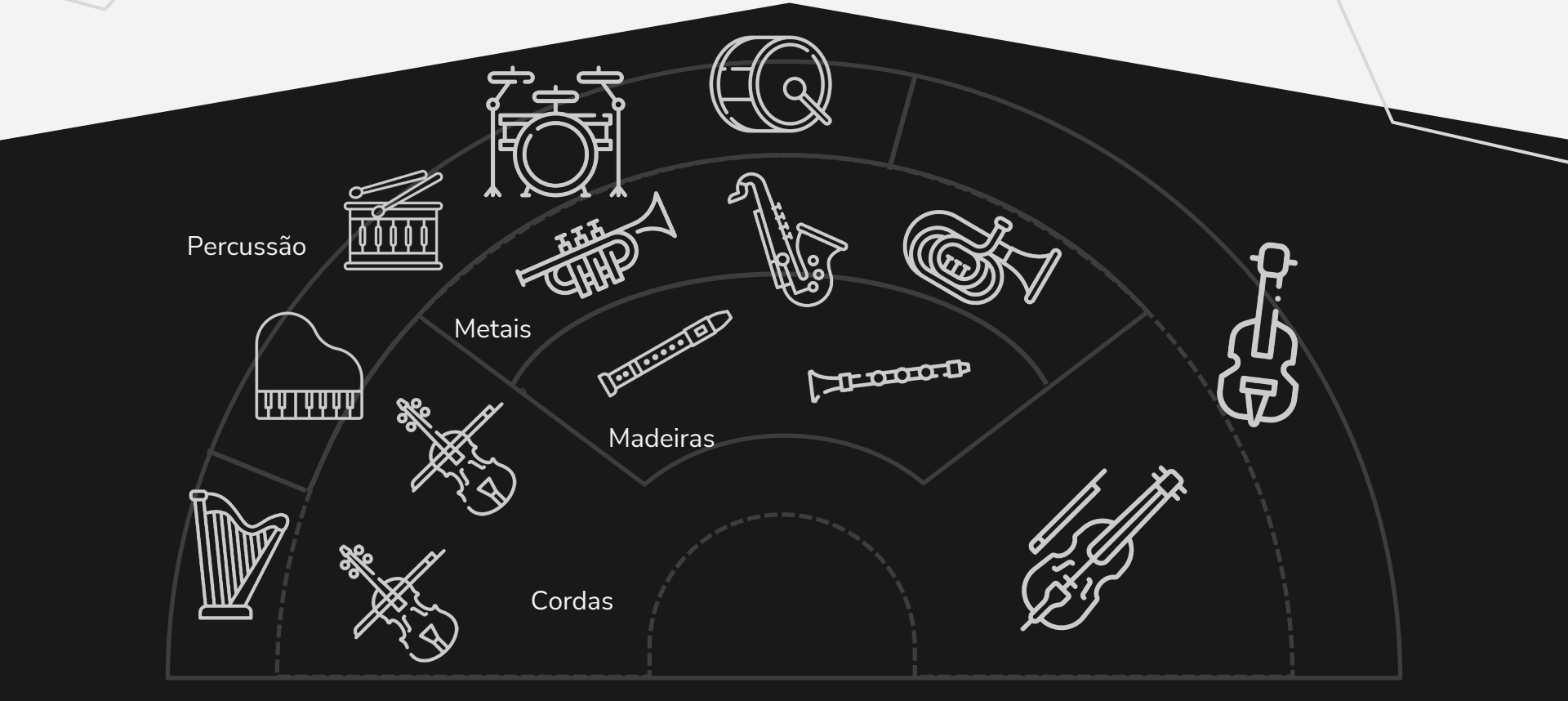
Liderança

Sinergia

Documentação

Integração

Os instrumentos da orquestra são utilizados em diferentes combinações, formando camadas musicais que, apesar das diferentes funções, trabalham em sintonia



Obrigado! Obrigada!