SOC-CSIRT INCM

Centro de Operações de Segurança do INCM

Miceles Chemane

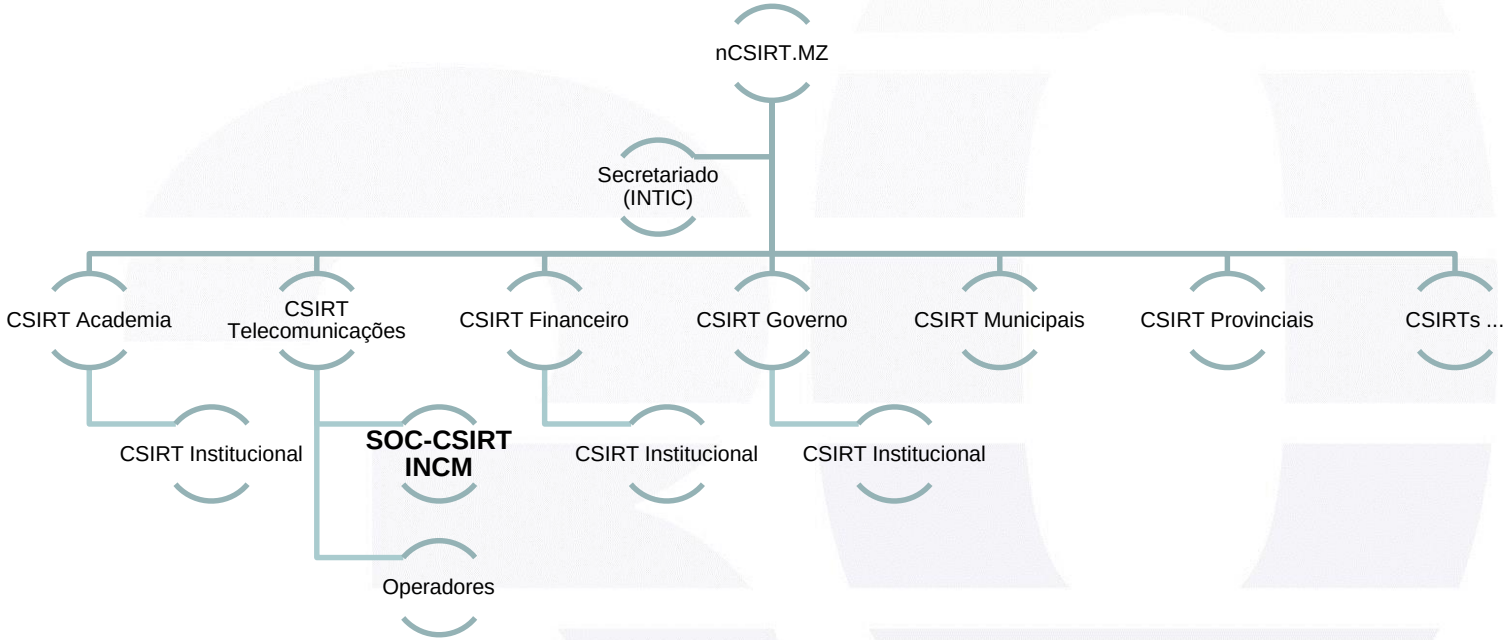
Data: 06 de Abril 2023

Introdução

- **Motivações:**
- Necessidade de estar em conformidade devido a interligação com os operadores e outras Instituições/organizações.
- Alinhamento com as iniciativas do Governo face a Segurança Cibernética
- **Prova de conceito:** 2020.
- **Ano de criação:** 2021.
- **Investimento:** Conjunto do Instituto Nacional das Comunicações (**INCM**) e Agência Nacional de Desenvolvimento Geo-Espacial (**ADE**).
- **Abrangência:** Infra-estrutura de TI do INCM (ADE, MTC e alguns Instituições tuteladas pelo MTC).
- **Capacidade actual:** identificação, colecta, armazenamento e análise de 1000 (mil) eventos por segundo.

Introdução (cont..)

- **Rede Nacional de CSIRTs**



- **Unidade de Controlo de Trafego de Telecomunicações (UCTT) –** Unidade do INCM responsável para criação do CSIRT do sector de telecomunicações.

SOC-CSIRT do INCM

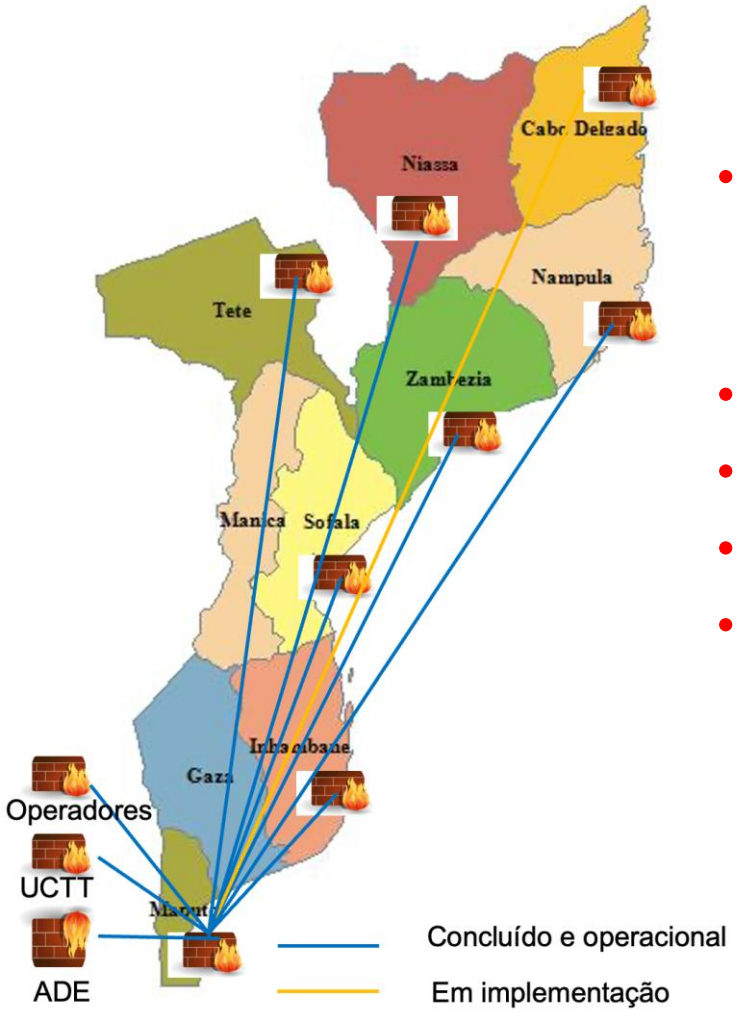
- **Funcionalidades/Serviços**
- Colecta e correlação de dados
- Detecção de ameaças
- Monitoria da segurança da rede, utilizadores e sistemas
- Triagem de alertas
- Gestão e resposta a incidentes

- **Interação**
- nCSIRT Nacional
- CSIRT do Governo de Moçambique
- CSIRT Academia
- Africa CERT - Comitê Africa de Cibersegurança
- FIRST - Fórum global de segurança e resposta a incidentes.

- **Contactos:**
- soc@incm.gov.mz
- +258-850503540, +258-844466066

SOC-CSIRT do INCM (cont..)

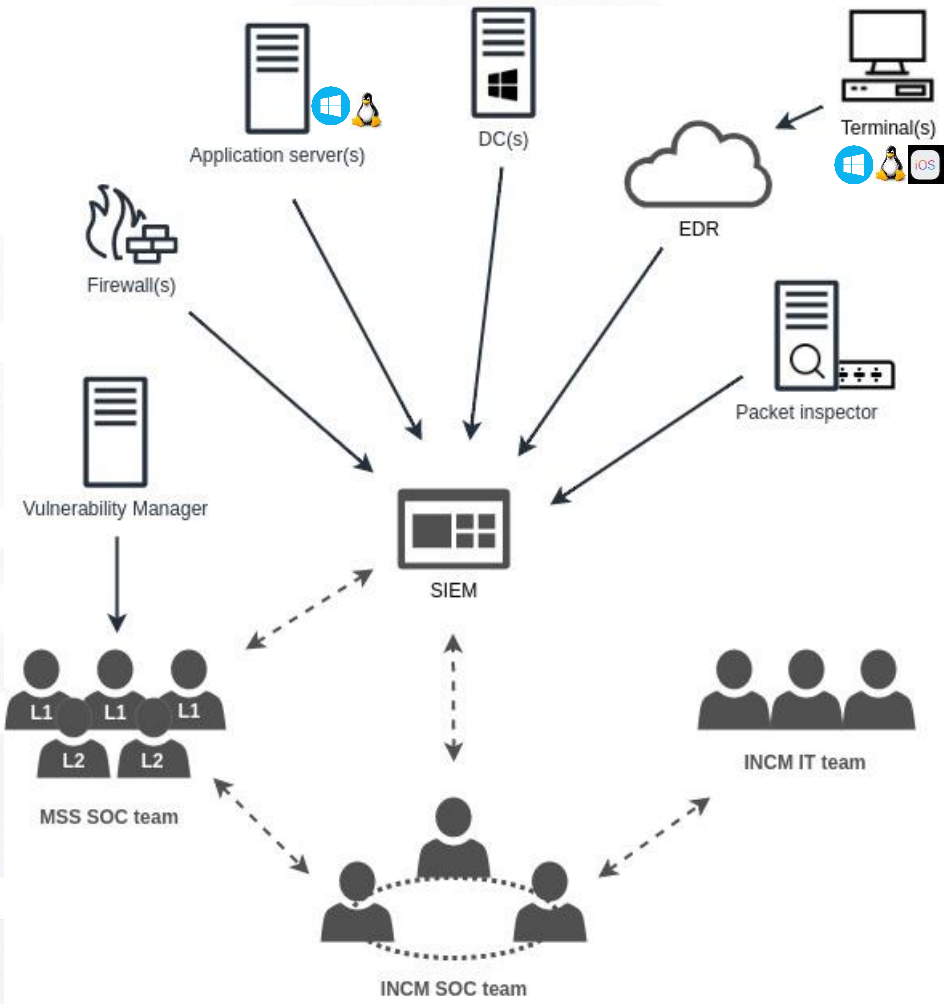
❖ Cobertura



- 190 Servidores virtuais
  - 98 na DMZ (Exposição - Internet)
- 10 Firewall
- +/- 720 dispositivos
- +/- 500 Utilizadores
- + de 1000 Sessões diariamente (plataformas online INCM)

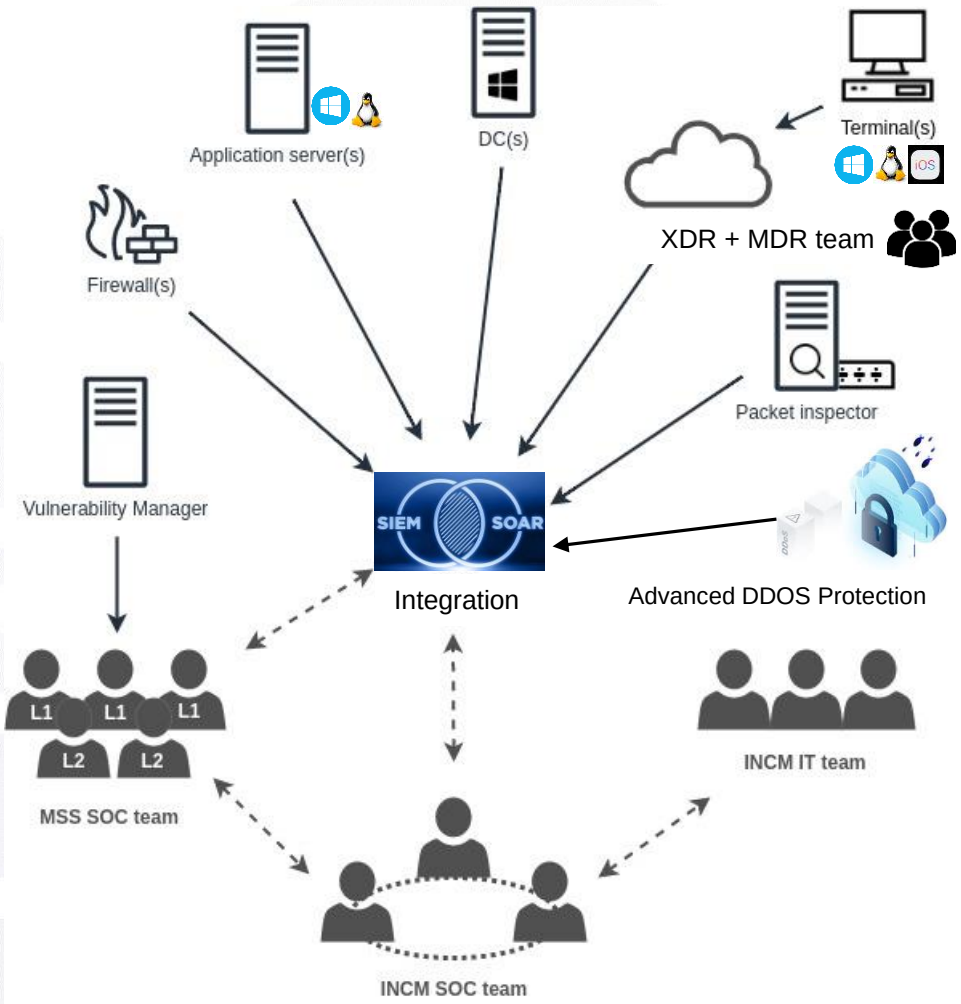
SOC-CSIRT do INCM (cont..)

- **MSS** - *Managed Security Services 12/7.*
- **EDR** - *Endpoint Detection and Response (todos dispositivos).*
- ***IDS/IPS*** - *Sistema de Detenção e Prevenção de Intrusões.*
- ***RTIR System*** - *Sistema de Gestão de Incidentes.*
- ***SIEM*** - *Gestão de Informações e Eventos de Segurança*



SOC-CSIRT do INCM (cont..)

- **MSS** - *Managed Security Services 12/7.*
- **XDR** - *Extended Detection and Response (todos dispositivos).*
- ***MDR*** *– Managed Detection and Response Service*
- ***IDS/IPS*** *- Sistema de Detenção e Prevenção de Intrusões.*
- ***RTIR System*** *- Sistema de Gestão de Incidentes.*
- ***SIEM*** *- Gestão de Informações e Eventos de Segurança*
- ***SOAR*** *– Orquestração, Automação e Resposta de Segurança.*
- ***DDOS*** *- Distributed denial-of-service*

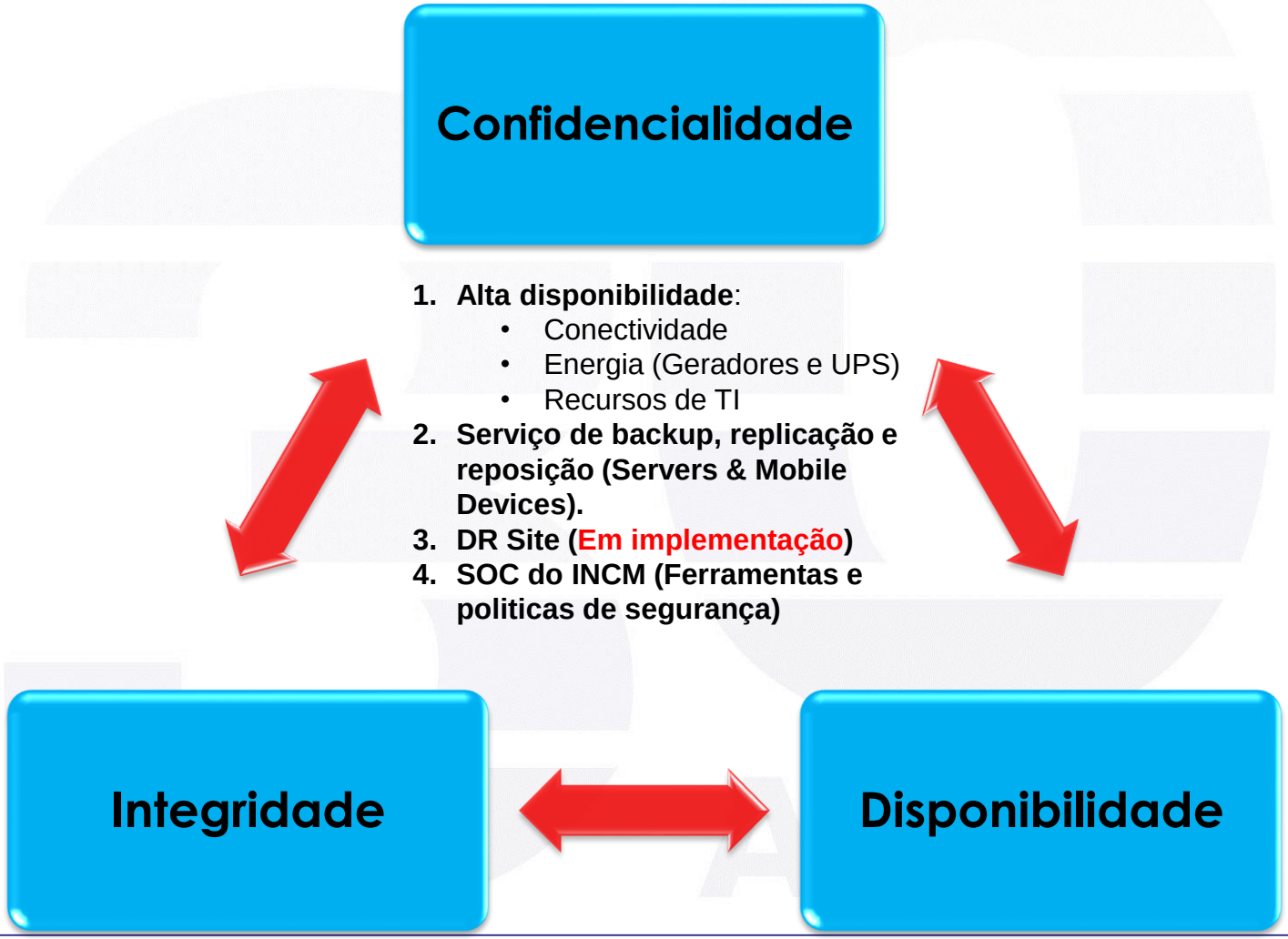


SOC-CSIRT do INCM (cont..)

- **Grandes Ataques ocorridos:**
  - ***Ransomware (Novembro de 2022)***
  - ***Bruteforce attack (Fev – Mar 2023)***
- ***Outros ataques:***
  - *Phishing*
  - *Spoofing*
  - *Trojan*
  - *Port Scanning*
  - *Botnet*
- *Lições aprendidas.*
- *Construção de uma base de dados de conhecimento.*

SOC-CSIRT do INCM (cont..)

❖ Infra-estrutura de TI Resiliente



Desafios

- Edução/Conscientização
- Capacitação a nível de gestão no que concerne a segurança cibernética
- Cursos especializados disponíveis a nível nacional
- Quadros nacionais especializados
- Adoção de politicas e procedimentos de segurança
- Investimentos

Muito Obrigado.