HIKARI – Hunting Integrado: Kompetição e Aprendizado em Resposta a Incidentes

Lourenço Alves Pereira Júnior

Sidnei Barbieri

Caio Marcos Chaves Viana

Leonardo Gonçalves Chahud

ITA

Contextualização

Avanço científico é inerentemente bottom-up

Contextualização

Desenvolvimento de pesquisa em IDS: host e network

Muitos avanços científicos de modo pontual

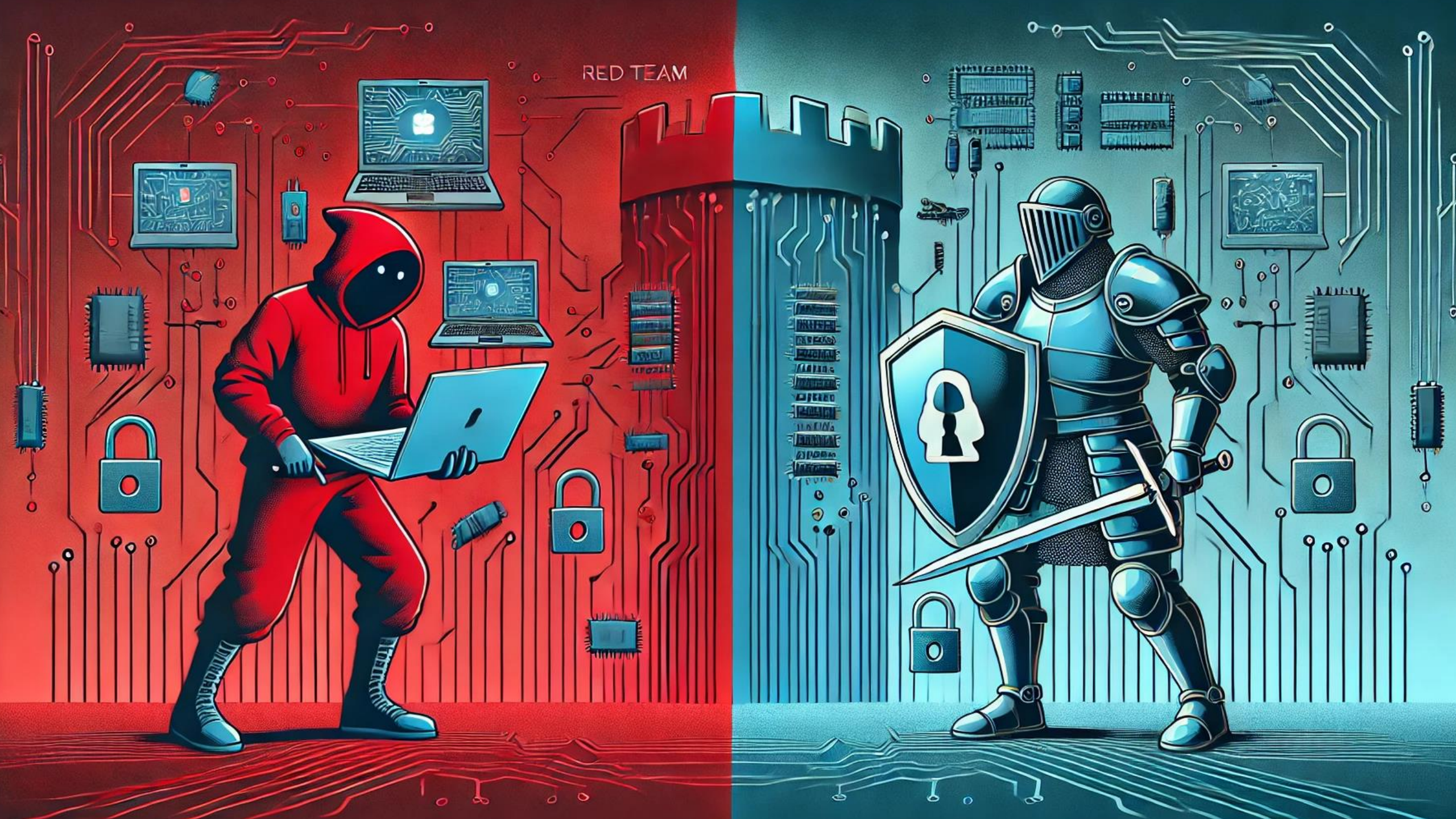
Componentes para de um sistema maior: o SOC

GAP tecnológico:

Falta uma solução integrada para threat hunting

Assimetria

ATAQUE vs. DEFESA


RED TEAM

Problema

Como diminuir essa assimetria?

Solução: HIKARI

Ambiente para profissionais de cibersegurança

CTF + SIEM

gamificado + operação de defesa

Objetivo

Ambiente que mimetiza o dia a dia de um SIEM

- Investigações cibernéticas
- Treinamento para equipes de defesa (Blue Team)
- Foco análise de logs de sistemas
- Permite a criação de exercícios com múltiplos times

Vantagem comercial

Soluções	Regionalização	Caça de ameaças	Ambiente Simulado Realista	Gerência de competições	Direcionada para Educação	Precificação
Cyber Range Solutions	x	x	x	x	x	Soluções fechadas
Hack The Box		x	x	x		Assinatura
Immersive Labs		x	x	x	x	Assinatura
RangeForce		x	x	x	x	Assinatura
Security Onion		x				Código aberto
HIKARI	*x*	*x*	*x*	*x*	*x*	*Código aberto*

Estruturação

Abordagem para alcançar o objetivo, três núcleos:

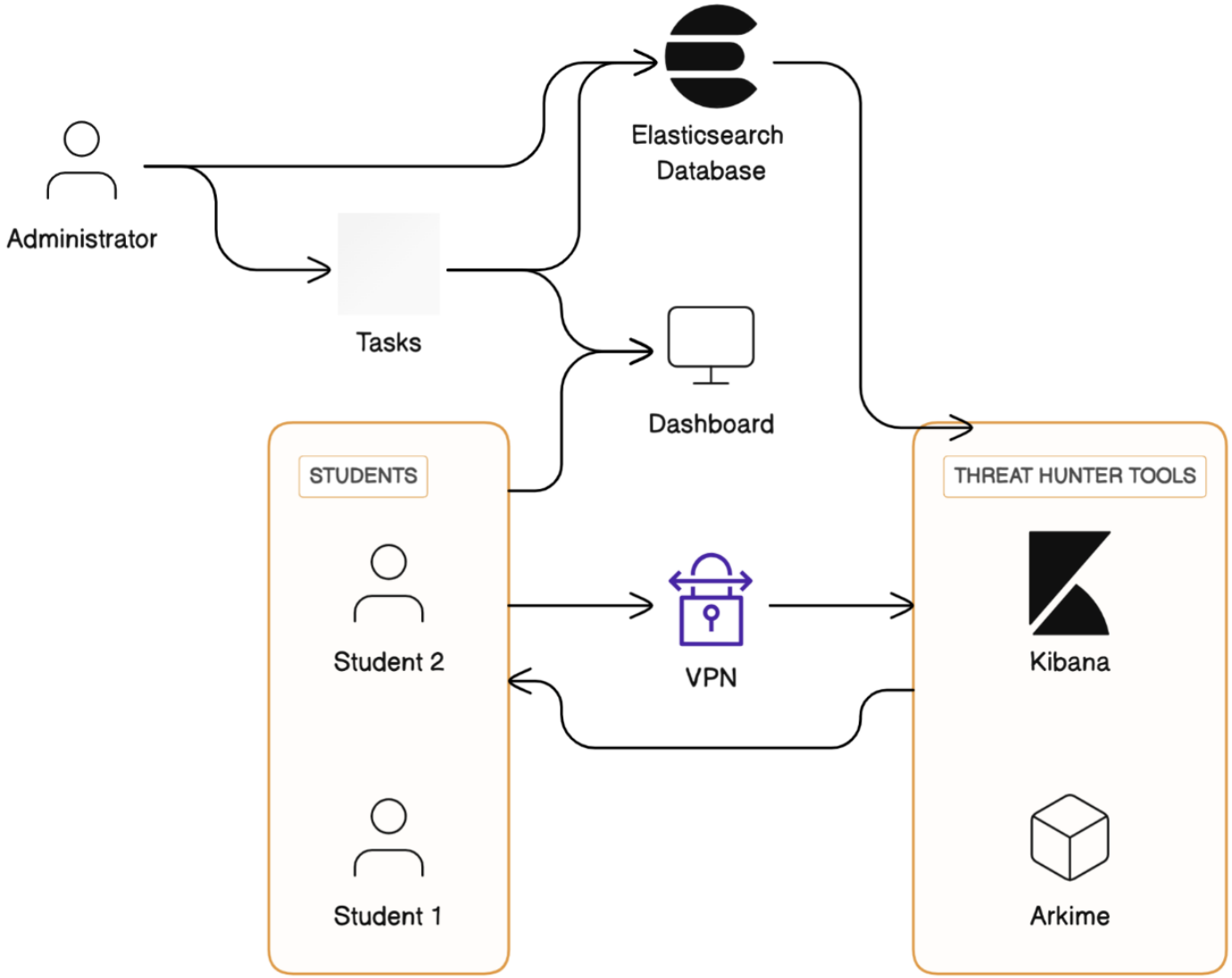
gestão dos recursos computacionais,

conjuntos de dados e

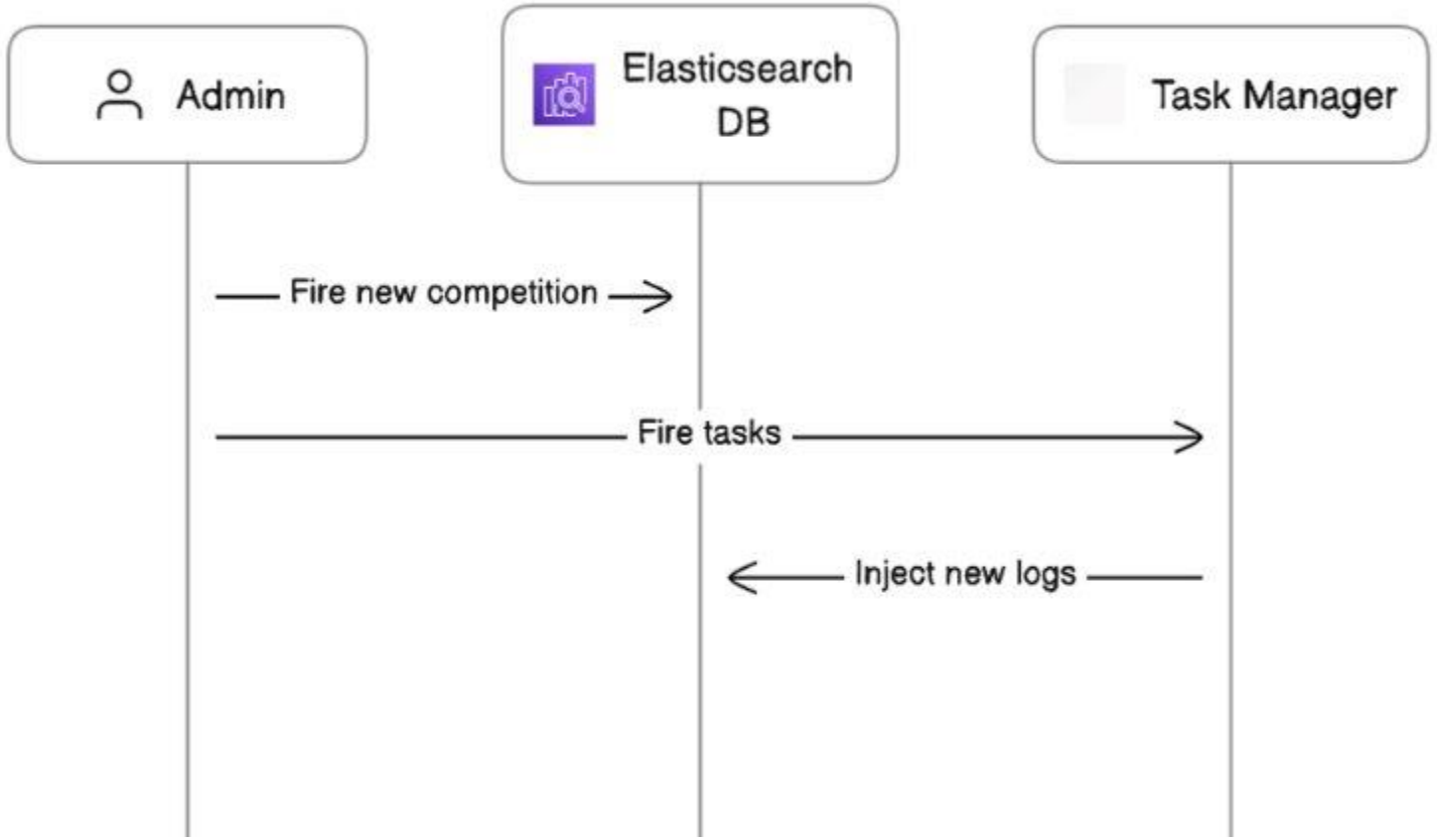
interface operacional

Integração: aumento do nível de prontidão tecnológica

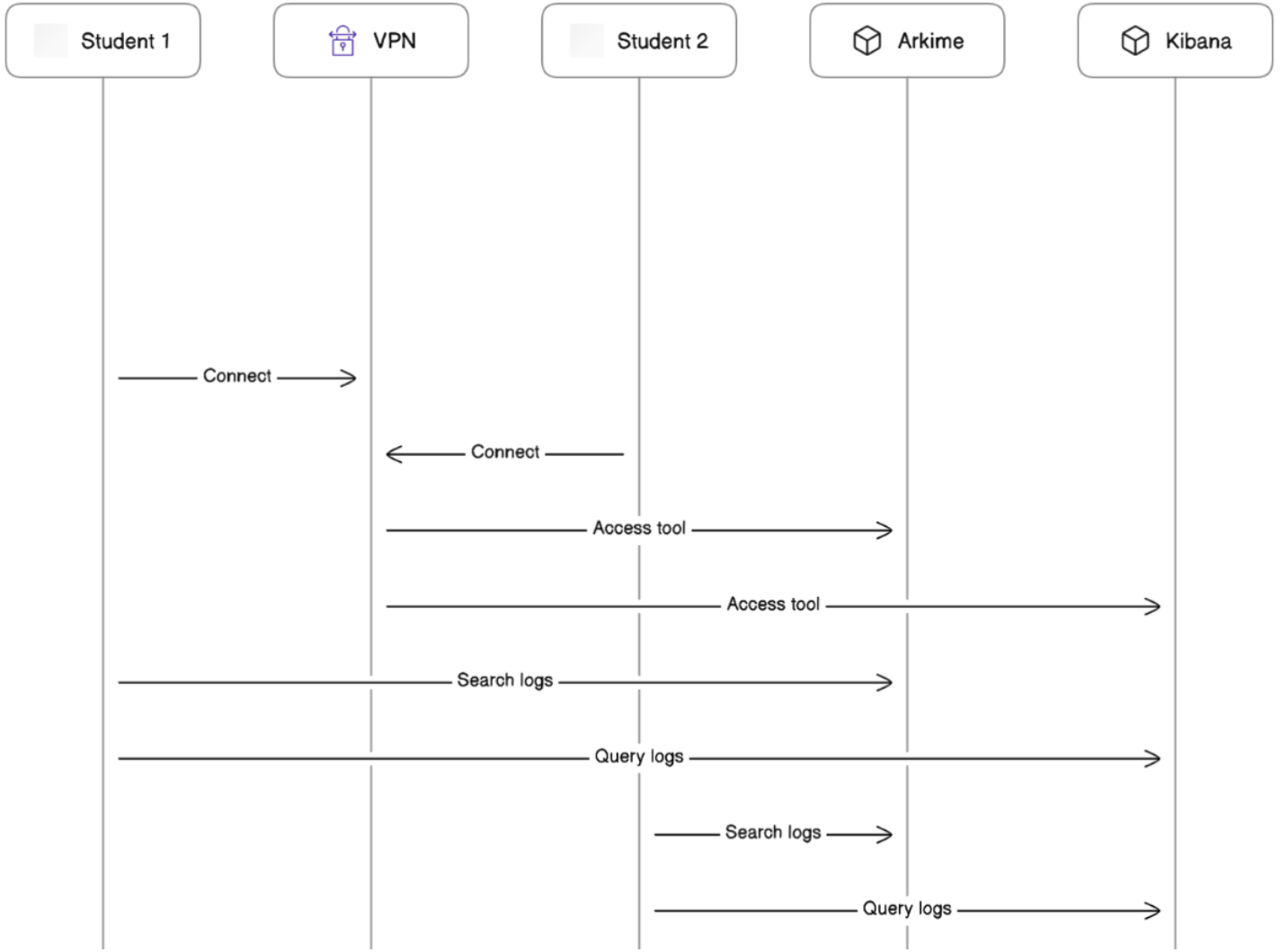
HIKARI


Elasticsearch
Database
Administrator
Tasks
Dashboard
STUDENTS
THREAT HUNTER TOOLS
Student 2
VPN
Kibana
Student 1
Arkime

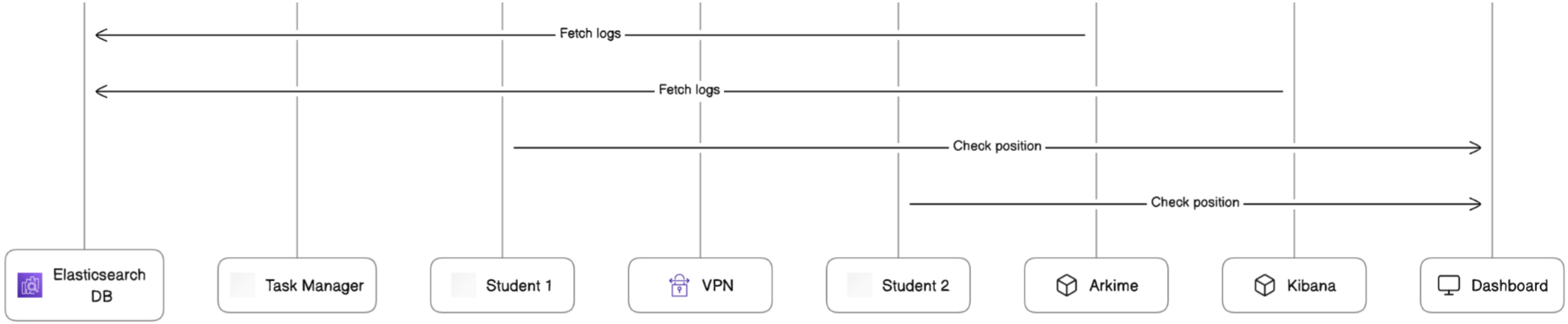
HIKARI - operacional

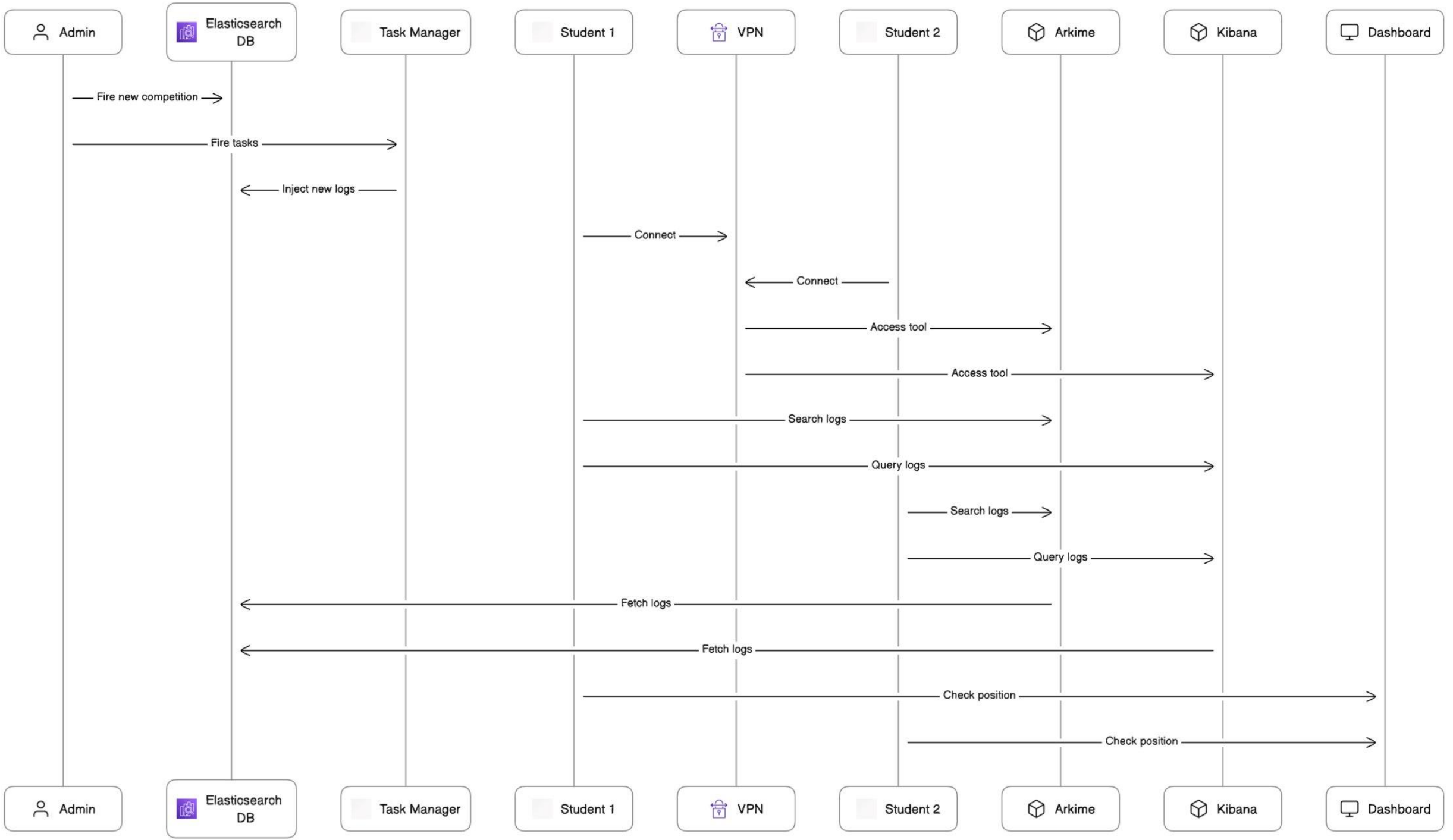


HIKARI - operacional



HIKARI - operacional

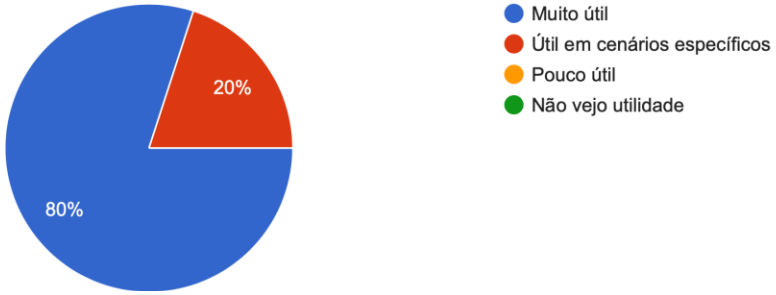



Admin
Elasticsearch DB
Task Manager
Student 1
VPN
Student 2
Arkime
Kibana
Dashboard
Fire new competition
Fire tasks
Inject new logs
Connect
Connect
Access tool
Access tool
Search logs
Query logs
Search logs
Query logs
Fetch logs
Fetch logs
Check position
Check position
Admin
Elasticsearch DB
Task Manager
Student 1
VPN
Student 2
Arkime
Kibana
Dashboard

Avaliação com 13 alunos do laboratório (disciplina de cibersegurança do ITA)

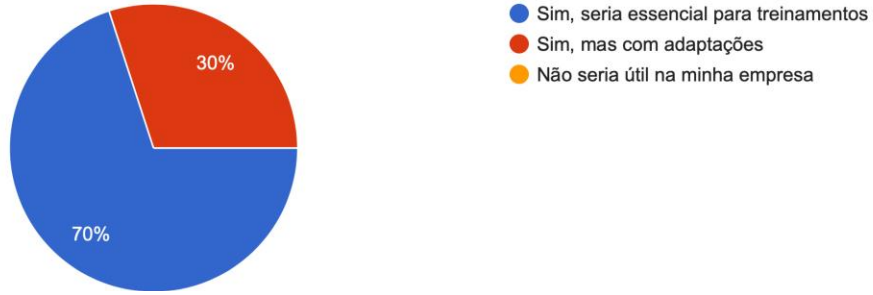
O HIKARI é útil para treinamento em análise de logs e resposta a incidentes?

10 respostas



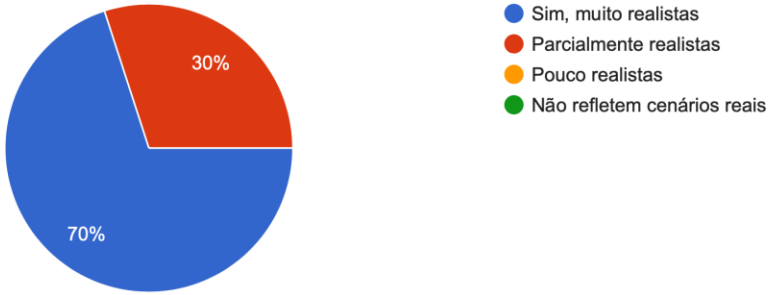
O HIKARI pode ser aplicado na rotina de treinamento de equipes de Blue Team?

10 respostas



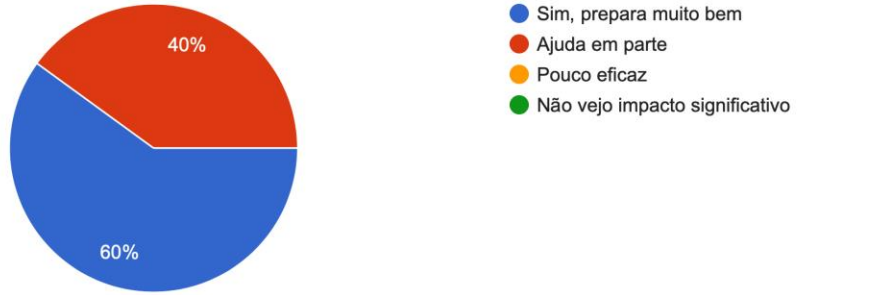
Os desafios do HIKARI refletem situações reais enfrentadas por equipes de Blue Team?

10 respostas



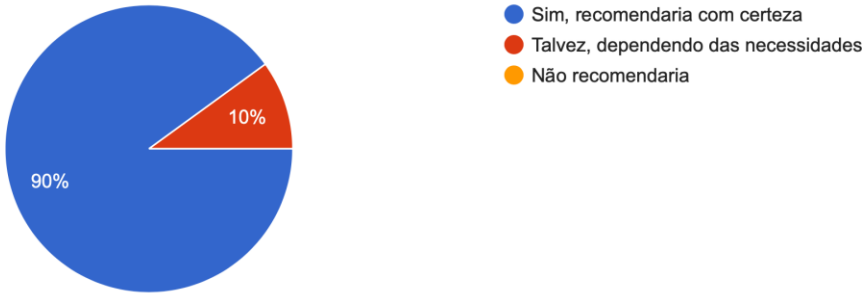
Na sua opinião, o HIKARI ajuda a preparar equipes para lidar com incidentes cibernéticos reais?

10 respostas



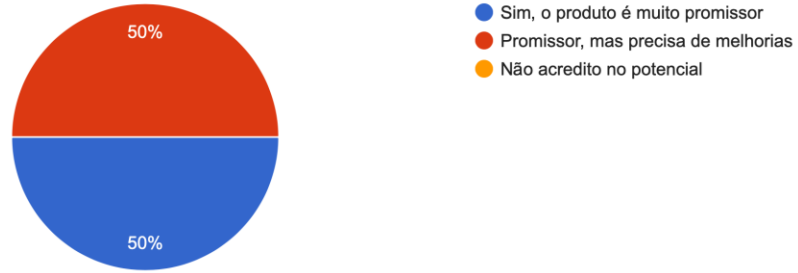
O HIKARI é um produto que você recomendaria para o treinamento de equipes de Blue Team?

10 respostas



Você acredita que o HIKARI pode se tornar uma ferramenta de destaque no mercado de segurança cibernética?

10 respostas



Feedback dos competidores

Aplicabilidade e Utilidade

- 80% consideram o HIKARI útil.
- 70% consideram essencial para treinamentos de Blue Teams.
- Sugestões:
  - Adicionar análise de tempo para investigação de flags.
  - Criar interface para gestores e banco de desafios prontos.

Feedback dos competidores

Relevância e Realismo

- 70% consideram os desafios realistas.
- 40% afirmam que prepara bem para incidentes.
- Sugestões:
  - Geração de logs em tempo real.
  - Registro de queries (KQL).
  - Níveis de desafio para ampliar a variedade.

Feedback dos competidores

Potencial de Negócio

- 90% recomendam para treinamentos.
- 50% acreditam que o produto é promissor.
- Sugestões:
  - Adicionar ambiente virtual para configuração e análise de logs.
  - Introdução ao Kibana.
  - Interface de gestão para criação de desafios.

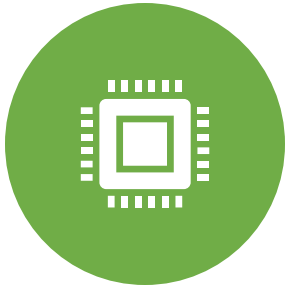
Feedback dos competidores

Comentários Gerais

- Código-fonte disponível facilita o uso corporativo.
- Melhorias sugeridas para busca no Kibana.
- Expansão de funcionalidades para maior aplicabilidade.

HIKARI – principais marcos

Fase 1 – nivelamento e setup básico do ambiente – JAN-MAR



Fase 2 - primeiros testes no ambiente e início da codificação - ABR-MAIO

Fase 3 - Estruturação dos datasets e fontes de dados – JUN-SET

Fase 4 – testes de desenvolvimento e alunos; refinamento – OUT-DEZ

Contribuições

DATASETS!

Melhoria sobre a utilidade de datasets disponíveis

https://securitydatasets.com/ e https://www.detectionlab.network/

Parceria: SICOOB, PRODEMGE e VALE

HACKERS DO BEM

OBRIGADO

ljr@ita.br

Slides extras: desafios da primeira competição

Técnicas abordadas

Cenários reais enfrentadas por profissionais da área de segurança (Blue Team).

Permite o exercício das habilidades com tarefas interativas e desafiadoras.

- **Network Scanning:** Testa a compreensão de ameaças de rede e identificação de vulnerabilidades, enfatizando a importância do reconhecimento inicial em investigações.
- **Web Exploits:** Foca em identificar e explorar vulnerabilidades em aplicações web, preparando os participantes para proteger ambientes contra ataques modernos.
- **EDR Analysis:** Avalia a capacidade de detectar e mitigar ameaças utilizando ferramentas de detecção e resposta de endpoints, um aspecto crítico da defesa cibernética.
- **Ransomware Behavior:** Analisa comportamentos semelhantes a ransomware, permitindo que os participantes reconheçam ataques em estágio inicial e minimizem impactos.

Desafio 1: Scanner Fantasma

- **Categoria:** Network Scanning
- **Descrição:** Um scanner fantasma está sondando a rede, tentando descobrir hosts ativos e portas abertas. Use suas habilidades para identificar o IP do scanner antes que ele vá embora!
- **Dica:** Procure por um IP que aparece consistentemente em múltiplas requisições com características de varredura.

- **Solução:** flag{10.6.36.27}
- **Sugestão de Query no Kibana:** Event Name: "Firewall Deny"
- **Arquivo JSON:** dataset-alsd.json

Desafio 2: Reconhecimento e exploração

- **Categoria:** Web Exploits
- **Descrição:** Alertas de segurança indicam que um atacante realizou reconhecimento seguido de exploração de vulnerabilidades. Descubra o IP do atacante para capturar a flag!
- **Dica:** Verifique IPs que aparecem em atividades de reconhecimento e, em seguida, em tentativas de exploração. Concentre-se em sequências de eventos suspeitas.

- **Solução:** flag{87.120.115.119}
- **Sugestão de Query no Kibana:** Event Name: "HTTP"
- **Arquivo JSON:** dataset-eap.json

Desafio 3: atividade suspeita no EDR

- **Categoria:** EDR Analysis
- **Descrição:** Uma atividade suspeita foi detectada por seu EDR em múltiplos sistemas. Sua tarefa é localizar o IP do sistema comprometido para ajudar na mitigação da ameaça!
- **Dica:** Concentre-se em IPs associados a eventos críticos que ocorrem repetidamente e indicam possível comprometimento.

- **Solução:** flag{192.168.10.101}
- **Sugestão de Query no Kibana**: CS-Severity \(custom\): "Critical" AND Low Level Category: "Suspicious Activity"
- **Arquivo JSON:** dataset-edr.json

Desafio 4: comportamento de ransomware

- **Categoria:** Ransomware Behavior
- **Descrição:** Sinais de comportamento de ransomware foram detectados em um de seus sistemas. Encontre o IP do sistema afetado e ajude a equipe a interromper o ataque antes que seja tarde!
- **Dica:** Procure por atividades que indicam criptografia em massa ou comportamentos incomuns de arquivos em sistemas específicos.

- **Solução:** flag{10.11.17.10}
- **Sugestão de Query no Kibana:** Event Name: "Ransomware Behaviour"
- **Arquivo JSON:** dataset-rbmws.json