CRIANDO SUA SANDBOX

COM INTEGRAÇÃO NO MISP

CAIQUE
BARQUETA

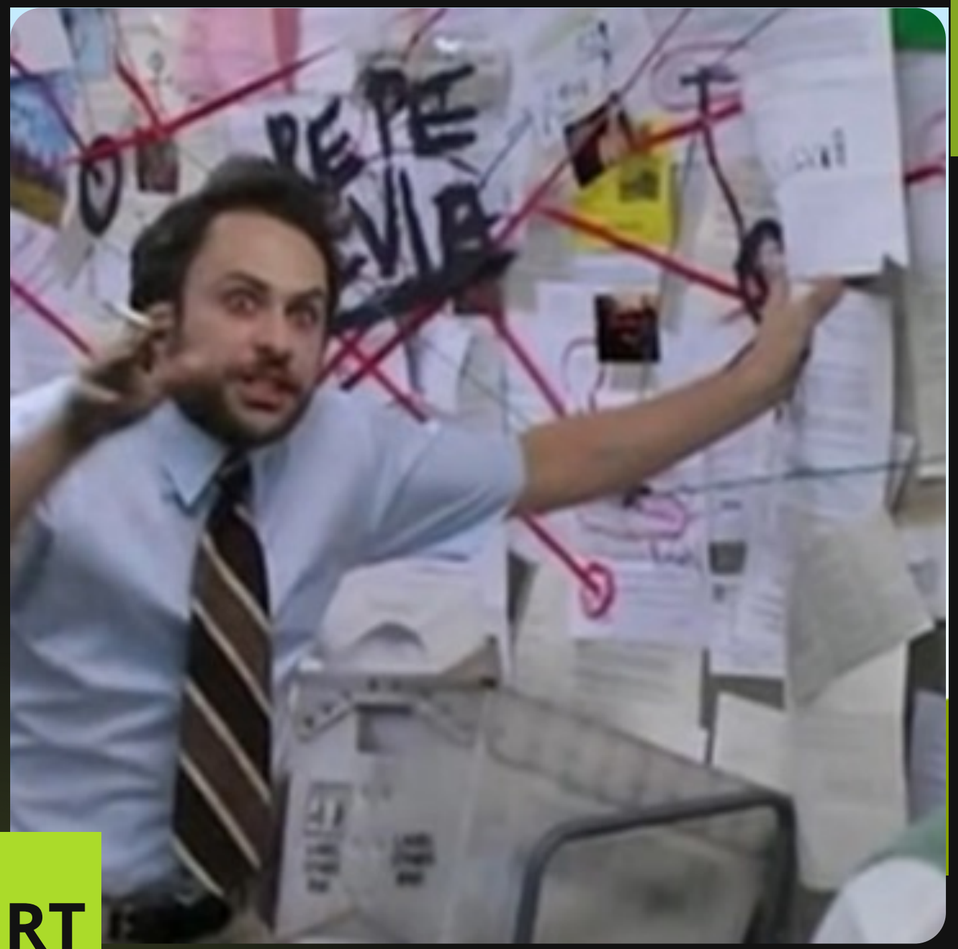
TLP:CLEAR

QUEM SOU EU?

Especialista em Inteligência de Ameaças na ISH Tecnologia
Professor e Palestrante
(Cursos de Malware/DFIR/Intel)
Pesquisador de Grupos de Ransomwares
Algumas certificações...

TLP:CLEAR

TLP:CLEAR



AGENDA

01 Principais dores;

02 O que é a Cuckoo?

03 Instalação (Cuckoo e MISP)

04 Integração e Automatização

05 Dicas finais

CSIRT

Fórum

PRINCIPAIS DORES

- Privacidade dos dados enviados para análises;
- Contratação de APIs e ferramentas para isso;
- Compras de mais acessos para departamentos;
- E muito mais...

SANDBOX da CISA

CISA criou a sandbox para coleta de dados e arquivos visando enriquecer a sua base de dados

PRESS RELEASE

CISA Announces Malware Next-Gen Analysis

Released: April 10, 2024

RELATED TOPICS: MALWARE, PHISHING, AND RANSOMWARE, CYBERSECURITY BEST PRACTICES, CYBER THREATS AND ADVISORIES

O QUE É CUCKOO SANDBOX?

Ferramenta de Análise Automática de Malware (*Open-Source*)

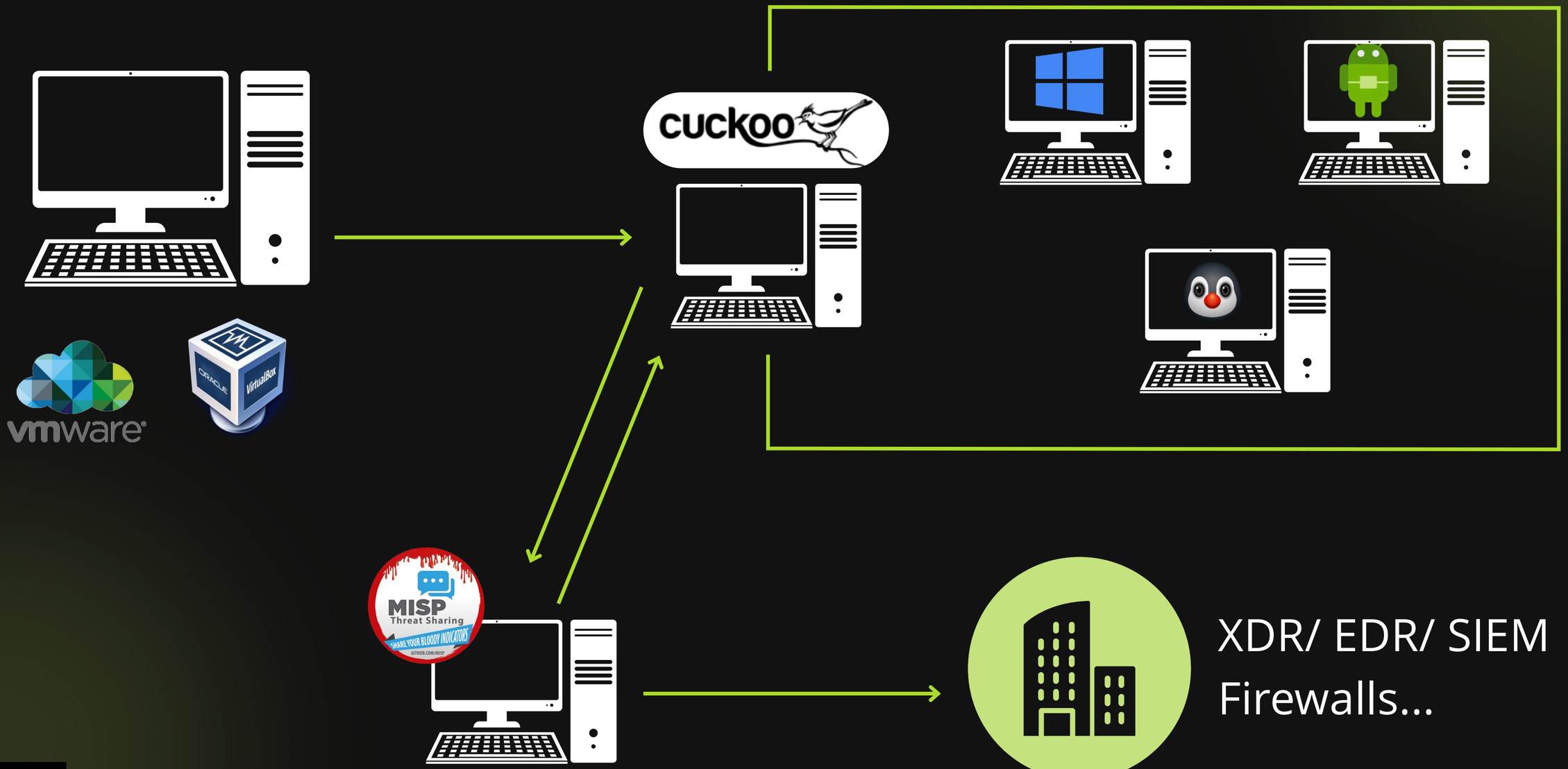
Executa arquivos em ambientes isolados “**Sandbox**”.

Inicio do projeto Google Summer of Code em **2010** (Projeto Honeynet) e desenvolvido pelo Claudio “nex” Guarnieri;

Última atualização foi na versão 2.0.6 em **2018**;

.exe, .dll, .pdf, .doc*, url, .html, .php, .cpl, .vbs, .zip, .jar, .py, .apk...

INFRAESTRUTURA



TLP:CLEAR

INSTALAÇÃO CUCKOO

01 Para teste local e também validação:

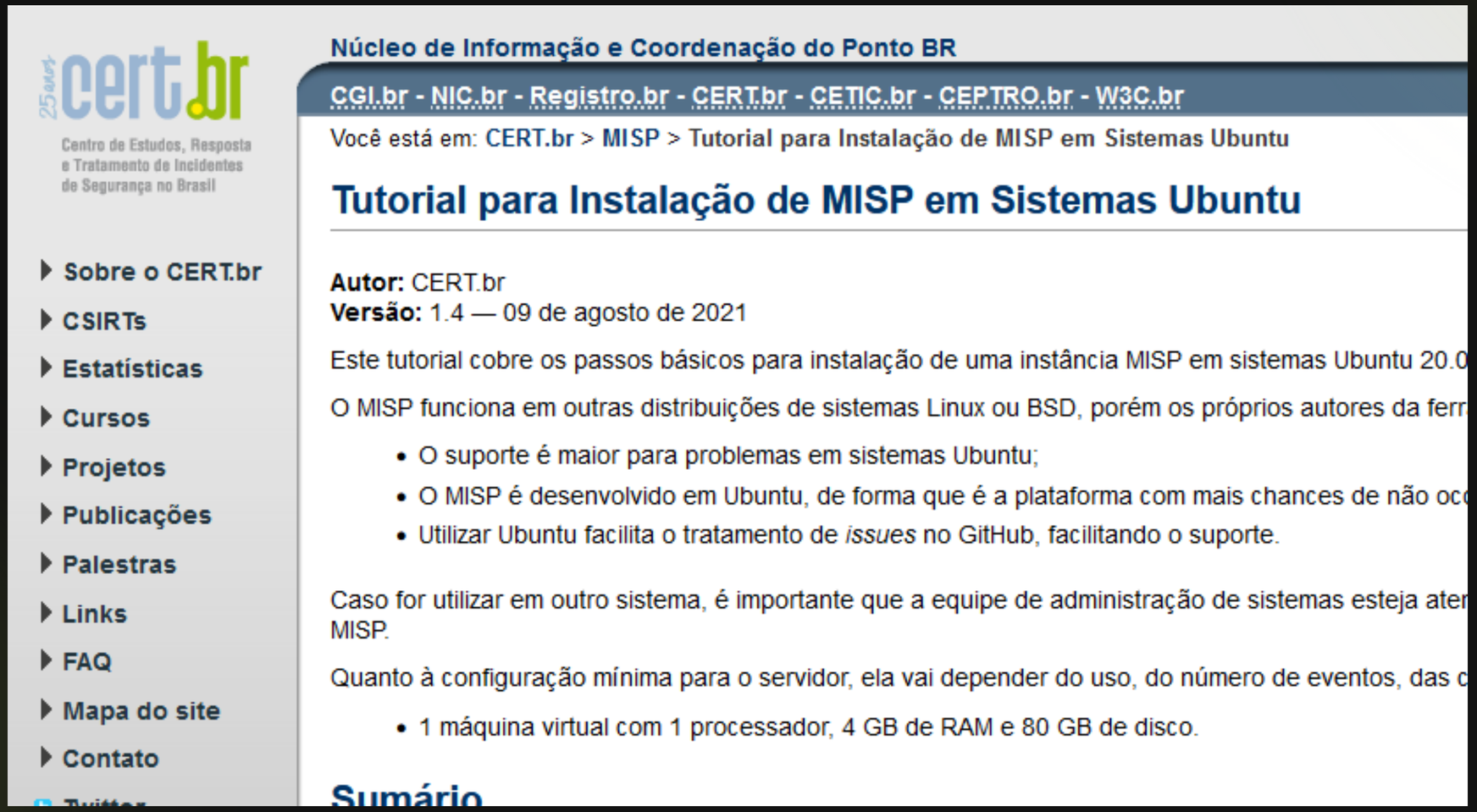
- Ubuntu Desktop 18.04.6 LTS server;
- Núcleos do processador 2 a 4 (ou +);
- Memória: 6GB (ou +);
- Armazenamento 100GB (ou +);
- Conexão para realizar via SSH;

Falhas... muitas falhas...

TLP:CLEAR

INSTALAÇÃO MISP

02



cert.br
Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil

- Sobre o CERT.br
- CSIRTs
- Estatísticas
- Cursos
- Projetos
- Publicações
- Palestras
- Links
- FAQ
- Mapa do site
- Contato

Núcleo de Informação e Coordenação do Ponto BR

CGI.br - NIC.br - Registro.br - CERT.br - CETIC.br - CEPTRO.br - W3C.br

Você está em: CERT.br > MISP > Tutorial para Instalação de MISP em Sistemas Ubuntu

Tutorial para Instalação de MISP em Sistemas Ubuntu

Autor: CERT.br
Versão: 1.4 — 09 de agosto de 2021

Este tutorial cobre os passos básicos para instalação de uma instância MISP em sistemas Ubuntu 20.0

O MISP funciona em outras distribuições de sistemas Linux ou BSD, porém os próprios autores da ferr

- O suporte é maior para problemas em sistemas Ubuntu;
- O MISP é desenvolvido em Ubuntu, de forma que é a plataforma com mais chances de não oc
- Utilizar Ubuntu facilita o tratamento de *issues* no GitHub, facilitando o suporte.

Caso for utilizar em outro sistema, é importante que a equipe de administração de sistemas esteja ater
MISP.

Quanto à configuração mínima para o servidor, ela vai depender do uso, do número de eventos, das c

- 1 máquina virtual com 1 processador, 4 GB de RAM e 80 GB de disco.

Sumário

INTEGRAÇÃO CUCKOO + MISP

```
[misp]
enabled = yes
url = https://192.168.2.40/
apikey = 31sgFVxTYXOtbjDG1ypERXxbN756Qc2BLjboxfQq

# Maximum amount of IOCs to look up (hard limit).
maxioc = 100
```

03 Consulta se o **Indicador** está no MISP (em algum evento)

processing.conf
reporting.conf

04 Envia os dados após análise da cuckoo para o MISP através de **criação de evento**.

Configurar detalhes do evento e criação de atributos

```
[misp]
enabled = ys
url =
apikey = 31sgFVxTYXOtbjDG1ypERXxbN756Qc2BLjboxfQq

# The various modes describe which information should be submitted to MISP,
# separated by whitespace. Available modes: maldoc ipaddr hashes url.
mode = maldoc ipaddr hashes url

distribution = 0
analysis = 0
threat_level = 4

# The minimum Cuckoo score for a MISP event to be created
min_malscore = 0

tag = Cuckoo
upload_sample = no
```

INTEGRAÇÃO CUCKOO + MISP

05 Precisa habilitar as opções de **“Enriquecimento” e “Importação”** no MISP para que aceite o evento da cuckoo e também possa realizar o envio para a Cuckoo caso seja imputado pelo MISP.

Recommended	Plugin.Import_cuckooimport_enabled	false	**[Enable or disable the cuckooimport module.]** Import a Cuckoo archive (zipfile or bzip2 tarball), either downloaded manually or exported from the API (/tasks/report/{task_id}/all).
Recommended	Plugin.Import_cuckooimport_restrict	No organisation selected.	Restrict the cuckooimport module to the given organisation.

Enrichment

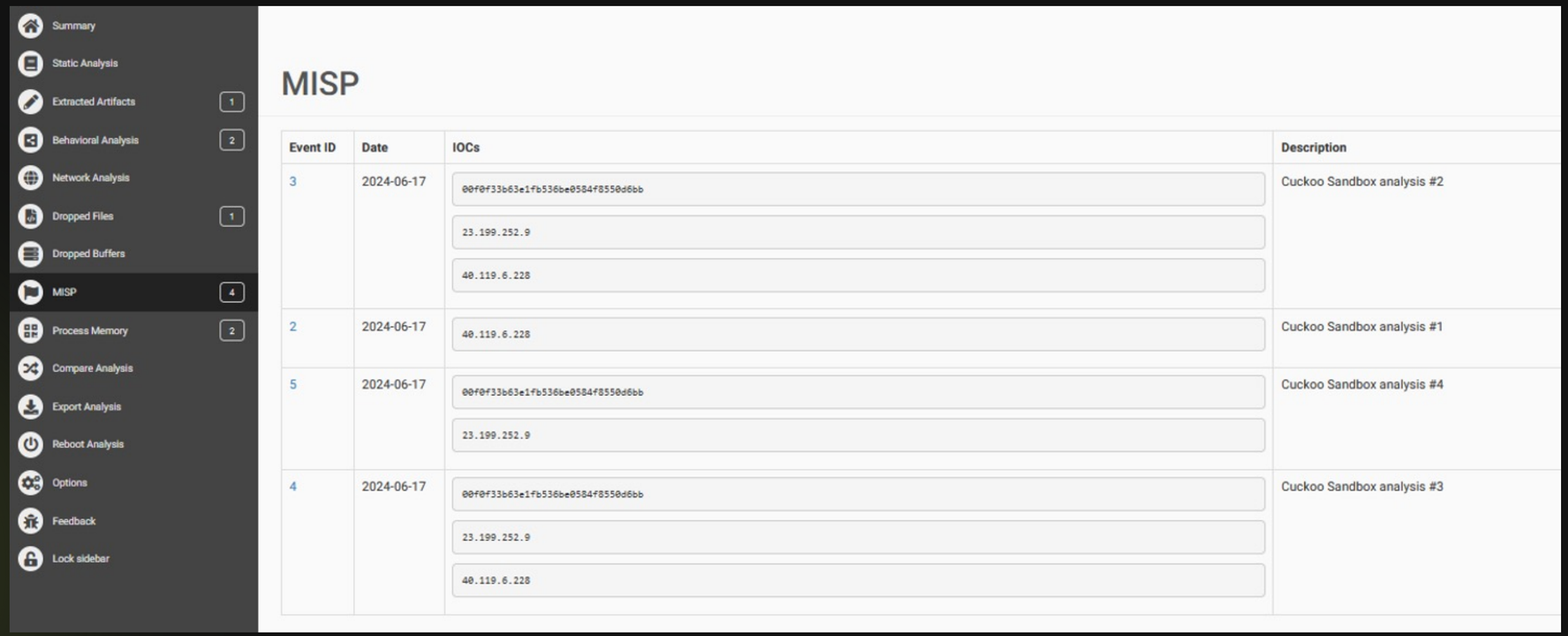
Recommended	Plugin.Enrichment_cuckoo_submit_enabled	false	**[Enable or disable the cuckoo_submit module.]** Submit files and URLs to Cuckoo Sandbox
Recommended	Plugin.Enrichment_cuckoo_submit_restrict	No organisation selected.	Restrict the cuckoo_submit module to the given organisation.
Recommended	Plugin.Enrichment_cuckoo_submit_api_url		Set this required module specific setting.
Recommended	Plugin.Enrichment_cuckoo_submit_api_key		Set this required module specific setting.

TLP:CLEAR

INTEGRAÇÃO CUCKOO + MISP

06

Observe que a Cuckoo quando habilitada a consulta, é possível identificar a **correlação** dos eventos no resultado da análise de acordo com a pesquisa no MISP sobre os indicadores.



INTEGRAÇÃO CUCKOO + MISP

6.1 back-end

```
2024-06-17 20:19:42,725 [cuckoo.core.scheduler] INFO: Using "virtualbox" as machine manager
2024-06-17 20:19:43,054 [cuckoo.machinery.virtualbox] DEBUG: Stopping vm 192.168.56.1011
2024-06-17 20:19:43,158 [cuckoo.machinery.virtualbox] DEBUG: Restoring virtual machine 192.168.56.1011 to its current snapshot
2024-06-17 20:19:43,251 [cuckoo.core.scheduler] INFO: Loaded 1 machine/s
2024-06-17 20:19:43,264 [cuckoo.core.scheduler] INFO: Waiting for analysis tasks.
2024-06-17 20:25:50,990 [cuckoo.core.scheduler] DEBUG: Processing task #1
2024-06-17 20:25:50,996 [cuckoo.core.scheduler] INFO: Starting analysis of FILE "script_test.ps1" (task #1, options "procmemdump=yes,route=
internet")
2024-06-17 20:25:51,013 [cuckoo.core.scheduler] INFO: Task #1: acquired machine 192.168.56.1011 (label=192.168.56.1011)
2024-06-17 20:25:51,013 [cuckoo.core.resultserver] DEBUG: Now tracking machine 192.168.56.101 for task #1
2024-06-17 20:25:51,013 [cuckoo.core.plugins] DEBUG: Started auxiliary module: Replay
2024-06-17 20:25:51,021 [cuckoo.auxiliary.sniffer] INFO: Started sniffer with PID 8548 (interface=vboxnet0, host=192.168.56.101)
2024-06-17 20:25:51,022 [cuckoo.core.plugins] DEBUG: Started auxiliary module: Sniffer
2024-06-17 20:25:51,042 [cuckoo.machinery.virtualbox] DEBUG: Starting vm 192.168.56.1011
2024-06-17 20:25:51,253 [cuckoo.machinery.virtualbox] DEBUG: Restoring virtual machine 192.168.56.1011 to its current snapshot
2024-06-17 20:25:54,936 [cuckoo.core.guest] INFO: Starting analysis #1 on guest (id=192.168.56.1011, ip=192.168.56.101)
2024-06-17 20:25:55,939 [cuckoo.core.guest] DEBUG: 192.168.56.1011: not ready yet
2024-06-17 20:25:56,943 [cuckoo.core.guest] DEBUG: 192.168.56.1011: not ready yet
2024-06-17 20:25:57,951 [cuckoo.core.guest] DEBUG: 192.168.56.1011: not ready yet
2024-06-17 20:25:58,001 [cuckoo.core.guest] DEBUG: 192.168.56.1011: not ready yet
2024-06-17 20:25:59,538 [cuckoo.core.guest] INFO: Guest is running Cuckoo Agent 0.10 (id=192.168.56.1011, ip=192.168.56.101)
2024-06-17 20:25:59,586 [cuckoo.core.guest] DEBUG: Uploading analyzer to guest (id=192.168.56.1011, ip=192.168.56.101, monitor=latest, size
=3884763)
2024-06-17 20:26:00,528 [cuckoo.core.resultserver] DEBUG: Task #1: live log analysis.log initialized.
2024-06-17 20:26:01,659 [cuckoo.core.resultserver] DEBUG: Task #1 is sending a BSON stream
2024-06-17 20:26:02,373 [cuckoo.core.resultserver] DEBUG: Task #1 is sending a BSON stream
2024-06-17 20:26:05,181 [cuckoo.core.guest] DEBUG: 192.168.56.1011: analysis #1 still processing
2024-06-17 20:26:10,234 [cuckoo.core.guest] DEBUG: 192.168.56.1011: analysis #1 still processing
2024-06-17 20:26:15,296 [cuckoo.core.guest] DEBUG: 192.168.56.1011: analysis #1 still processing
2024-06-17 20:26:20,376 [cuckoo.core.guest] DEBUG: 192.168.56.1011: analysis #1 still processing
```

```
ng now (2.4.106). Please upgrade PyMISP.
2024-06-17 20:36:51,539 [cuckoo.core.plugins] DEBUG: Executed processing module "MISP" for task #2
2024-06-17 20:36:51,540 [cuckoo.core.plugins] DEBUG: Executed processing module "TLSMasterSecrets" for task #2
2024-06-17 20:36:51,541 [cuckoo.core.plugins] DEBUG: Executed processing module "Debug" for task #2
2024-06-17 20:36:51,555 [cuckoo.core.plugins] DEBUG: Running 542 signatures
2024-06-17 20:36:51,808 [cuckoo.core.plugins] DEBUG: Analysis matched signature: allocates_rwx
2024-06-17 20:36:51,809 [cuckoo.core.plugins] DEBUG: Analysis matched signature: generates_crypto_key
2024-06-17 20:36:51,809 [cuckoo.core.plugins] DEBUG: Analysis matched signature: recon_fingerprint
2024-06-17 20:36:51,809 [cuckoo.core.plugins] DEBUG: Analysis matched signature: antivm_memory_available
2024-06-17 20:36:51,809 [cuckoo.core.plugins] DEBUG: Analysis matched signature: process_martian
2024-06-17 20:36:51,810 [cuckoo.core.plugins] DEBUG: Analysis matched signature: memdump_urls
2024-06-17 20:36:52,115 [cuckoo.core.plugins] DEBUG: Executed reporting module "JsonDump"
WARNING [api.py:112 - __init__() ] The version of PyMISP recommended by the MISP instance (2.4.190) is newer than the one you're using now
(2.4.106). Please upgrade PyMISP.
2024-06-17 20:36:52,207 [pymisp] WARNING: The version of PyMISP recommended by the MISP instance (2.4.190) is newer than the one you're usi
ng now (2.4.106). Please upgrade PyMISP.
2024-06-17 20:36:52,464 [cuckoo.reporting.misp] DEBUG: tag event: Global tag Cuckoo(6) successfully attached to Event(3).
2024-06-17 20:36:53,277 [cuckoo.core.plugins] DEBUG: Executed reporting module "MISP"
2024-06-17 20:36:53,432 [cuckoo.core.plugins] DEBUG: Executed reporting module "MongoDB"
2024-06-17 20:36:53,432 [cuckoo.core.scheduler] INFO: Task #2: reports generation completed
2024-06-17 20:36:53,437 [cuckoo.core.scheduler] INFO: Task #2: analysis procedure completed
```

INTEGRAÇÃO CUCKOO + MISP

07 A tag nativa utilizada pela sandbox é a **Cuckoo** e **não publica o evento**

Problemas do *type* para o atributo: **filename|hash**

Payload delivery	filename|sha256	b94afe6c399ec6561ef55b11ce00c220a8b138dd4dc2ae1f286f98f55b72b717.bat b94afe6c399ec6561ef55b11ce00c220a8b138dd4dc2ae1f286f98f55b72b717		File submitted to Cuckoo
Payload delivery	filename|sha1	b94afe6c399ec6561ef55b11ce00c220a8b138dd4dc2ae1f286f98f55b72b717.bat fb9134664be4e69a7d7bd0228c1b06d20b42ec6f		File submitted to Cuckoo
Payload delivery	filename|md5	b94afe6c399ec6561ef55b11ce00c220a8b138dd4dc2ae1f286f98f55b72b717.bat 730ece1c0e692c783e28bfb7b7fc6cce		File submitted to Cuckoo

INTEGRAÇÃO CUCKOO + MISP

08 A rotina para disponibilizar como feed é realizar a **manipulação de eventos** no MISP + consulta no **Virus Total** e disponibilizar para .txt

```
# Defina a URL e a chave API do MISP
misp_url="URL do MISP"
misp_key="APYKey"

# Defina o JSON para a consulta
json_query='{
    "returnFormat": "text",
    "to_ids": "1||0",
    "published": false,
    "tags": "Cuckoo",
    "type": "filename|sha256||filename|md5||filename|sha1"
}'
```

```
misp@misp-cliente:~/feed$ ./script1.1.sh
Hashes únicos encontrados foram salvos em /home/misp/feed/hashes.txt
misp@misp-cliente:~/feed$ cat hashes.txt
08868b57e0ff782198f011700d76fe102aad7bbd66dfcac1d30929865b8d856a
0fb86a8ba8fdf57990c283080a671c1320cbcdfd0e8b5f5a250d9c38a6fce305
2357ecbcf3b566c76c839daf7ecf2681
593e63f9b46b3551fc3671ce17426cafbb26ebe5
730ece1c0e692c783e28bfb7b7fc6cce
7f0e85440e7ec1f44a4f827475e93d2e5dc101f66f2068ca71af9beaf9a75800
89d9b7c3eff0a15dc9dbbfe2163de7d5e9479f58
98f1794a6f97401dcab18bdb033736dd
b94afe6c399ec6561ef55b11ce00c220a8b138dd4dc2ae1f286f98f55b72b717
e01ea8093ebe546ea93a1274112bf18b
fb9134664be4e69a7d7bd0228c1b06d20b42ec6f
fd97f02244f56707f65e45becb38bfc50a22350e
```

Extração de eventos com a tag: Cuckoo e não publicados e os atributos do evento filename|hash do evento. Realizei o tratamento para deixar disponível **apenas as *hashes*.**

TLP:CLEAR

INTEGRAÇÃO CUCKOO + MISP

09 O segundo é a consulta no **Virus Total** e obter o resultado dos scans, enriquecer o evento, adicionar tags e publicar o evento.

```
Processando hash: 08868b57e0ff782198f011700d76fe102aad7bbd66dfcac1d30929865b8d856a, S
Atributo md5 adicionado ao evento com ID: 203
Tag Kaspersky adicionada ao objeto 95d932c4-2274-46dc-843c-5d8e760144c2
Tag Sophos adicionada ao objeto 95d932c4-2274-46dc-843c-5d8e760144c2
Tag Symantec adicionada ao objeto 95d932c4-2274-46dc-843c-5d8e760144c2
Tag TrendMicro adicionada ao objeto 95d932c4-2274-46dc-843c-5d8e760144c2
Atributo sha1 adicionado ao evento com ID: 204
Tag Kaspersky adicionada ao objeto 6f939841-9217-47db-9e4e-5a24f7ed85f2
Tag Sophos adicionada ao objeto 6f939841-9217-47db-9e4e-5a24f7ed85f2
Tag Symantec adicionada ao objeto 6f939841-9217-47db-9e4e-5a24f7ed85f2
Tag TrendMicro adicionada ao objeto 6f939841-9217-47db-9e4e-5a24f7ed85f2
Atributo sha256 adicionado ao evento com ID: 205
Tag Kaspersky adicionada ao objeto 14cbeaab-3207-42cb-9951-a55c11a3aa49
Tag Sophos adicionada ao objeto 14cbeaab-3207-42cb-9951-a55c11a3aa49
Tag Symantec adicionada ao objeto 14cbeaab-3207-42cb-9951-a55c11a3aa49
Tag TrendMicro adicionada ao objeto 14cbeaab-3207-42cb-9951-a55c11a3aa49
```

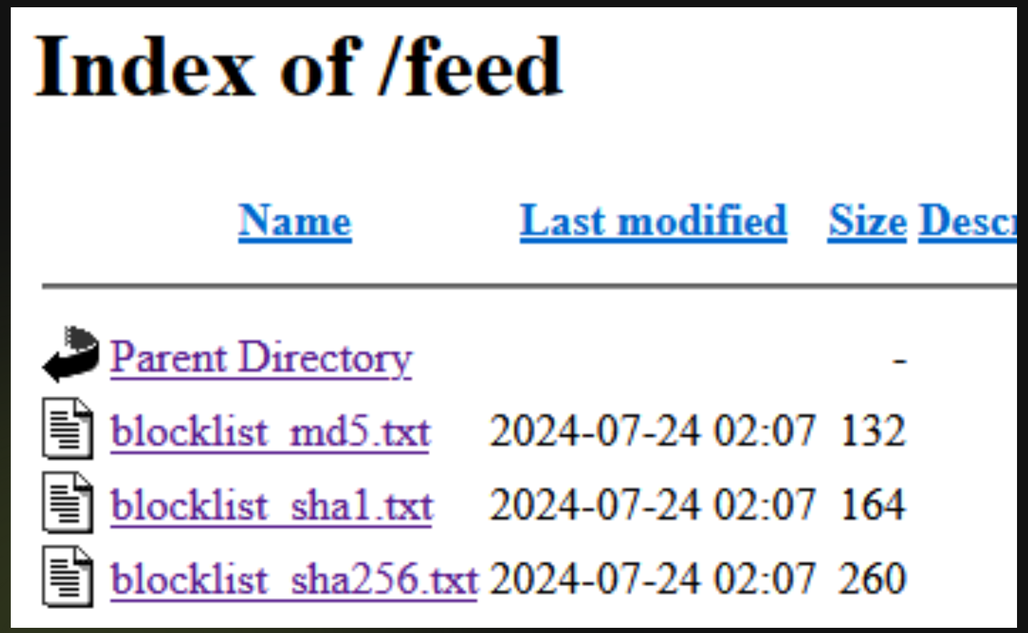
sha256	7f0e85440e7ec1f44a4f827475e93d2e5dc101f66f2068ca71af9beaf9a75800	Kaspersky x, Microsoft x, Sophos x, Symantec x	Consulta no Virus Total: 55/67
md5	e01ea8093ebe546ea93a1274112bf18b	Kaspersky x, Microsoft x, Sophos x, Symantec x	Consulta no Virus Total: 55/67
sha1	593e63f9b46b3551fc3671ce17426cafbb26ebe5	Kaspersky x, Microsoft x, Sophos x, Symantec x	Consulta no Virus Total: 55/67

41 | tlp:amber+strict | feed_cuckoo | CSIRT | 12 | 4 | 2024-07-24 | Feed do Cuckoo - CSIRT Forum - 2024-07-24 | All

TLP:CLEAR

INTEGRAÇÃO CUCKOO + MISP

10 O ultimo é para disponibilizar como feed para FIREWALLS/EDR/XDR/SOAR que consomem arquivos em formato **.txt**



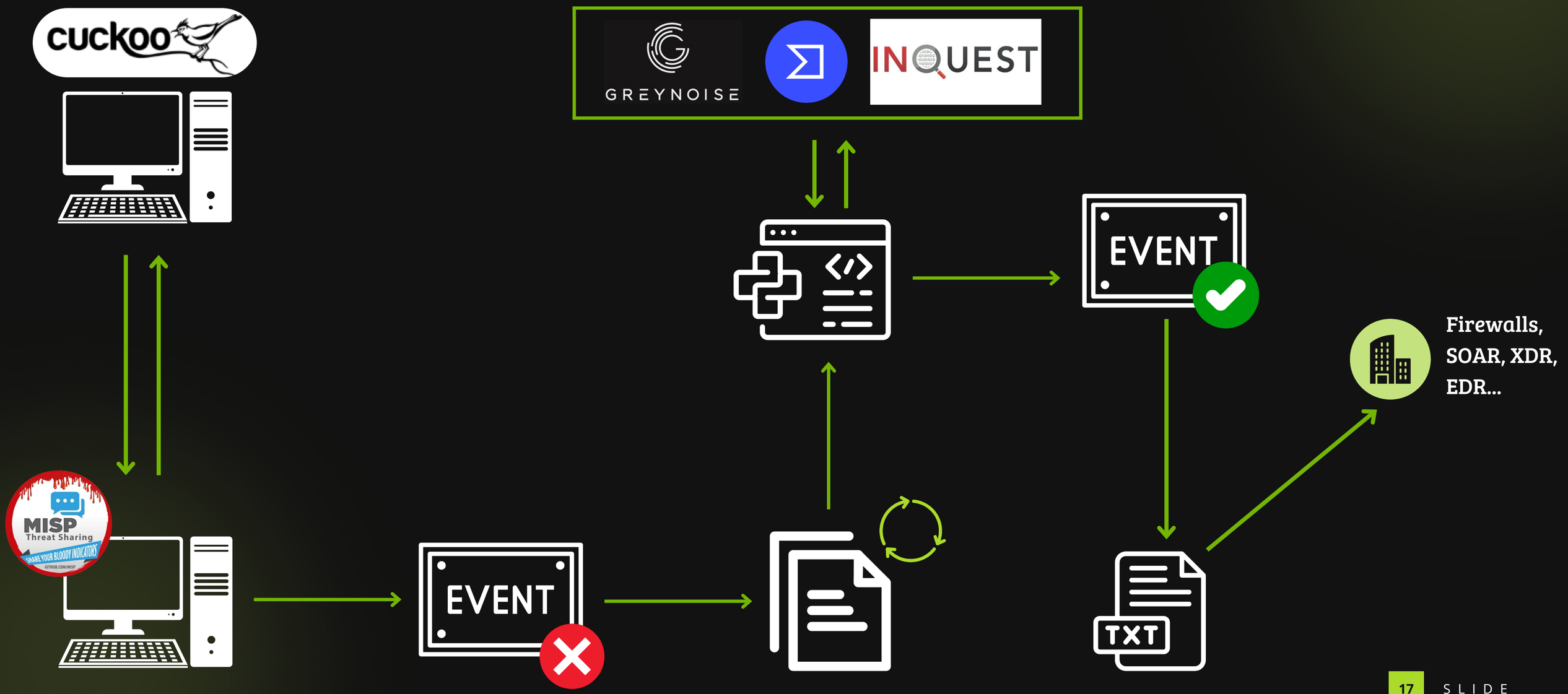
Index of /feed

Name	Last modified	Size	Desc
Parent Directory		-	
blocklist_md5.txt	2024-07-24 02:07	132	
blocklist_sha1.txt	2024-07-24 02:07	164	
blocklist_sha256.txt	2024-07-24 02:07	260	

```
08868b57e0ff782198f011700d76fe102aad7bbd66dfcac1d30929865b8d856a
0fb86a8ba8fdf57990c283080a671c1320cbcdfd0e8b5f5a250d9c38a6fce305
7f0e85440e7ec1f44a4f827475e93d2e5dc101f66f2068ca71af9beaf9a75800
b94afe6c399ec6561ef55b11ce00c220a8b138dd4dc2ae1f286f98f55b72b717
```

INFRAESTRUTURA

TLP:CLEAR



NOVAS POSSIBILIDADES

Centralizando as informações no MISP, você pode:

- Script para **automação** de validação dos IoCs em serviços
- Usar **novas ferramentas** como servidor DHCP (simular C2), Volatility2 na análise da Cuckoo, vários SOs...
- Criar um fluxo de entrega dos **Firewalls/ EDR e outras soluções**...
- Novos sensores como **Honeypots** para criação de eventos com dados obtidos pelos coletores (tema para outra palestra)
- Criação de base de Indicadores **exclusivos** na organização.

REFERÊNCIAS

https://blog.rootshell.be/2017/01/25/quick-integration-misp-cuckoo/

https://www.cisa.gov/news-events/news/cisa-announces-malware-next-gen-analysis

https://www.cert.br/misp/tutorial-ubuntu/

https://cuckoo.sh/docs/installation/index.html

https://github.com/crocodyli/BR-Forum-CSIRTs

TLP:CLEAR

MUITO OBRIGADO