METODOLOGIA PARA INTELIGÊNCIA DE AMEAÇAS CIBERNÉTICAS COM INTEGRAÇÃO DE SENSORES

João Alberto Pincovscy e João José Costa Gondim
Pós Graduação em Engenharia Elétrica (PPEE), Departamento de Elétrica Engenharia, Universidade de Brasília (UnB), Brasília-DF 70910-900, Brasil

RESUMO

Identificar ataques em redes de computadores é uma tarefa complexa, dada a enorme quantidade de máquinas, diversidade e grande volume de dados. A Inteligência de Ameaças Cibernéticas consiste na coleta e produção de conhecimento sobre ameaças nos sistemas de defesa das redes. Neste cenário, encontramos os Sistemas de Detecção de Intrusão de rede que especificamente analisam o tráfego de rede e, através de assinaturas, detectam anomalias, gerando registros para os operadores do sistema. A proposta deste trabalho é apresentar uma metodologia para gerar conhecimento sobre Inteligência de Ameaças, a partir dos registros de sensores de rede, coletando Indicadores de Ameaças ou Comprometimento e enriquecendo-os para alimentar Plataformas de Compartilhamento de Inteligência de Ameaças. Nossa metodologia acelera o processo de tomada de decisão, pois incorpora um repositório público e atualizado de assinaturas já no coletor, eliminando a fase de identificação de ameaças em uma etapa adicional. Para a demonstração e avaliação da metodologia foi realizada uma prova de conceito que contemplou todo o ciclo da identificação de ameaças.

PALAVRAS-CHAVE

Inteligência de Ameaças, Detecção de Intrusão, Análise de Anomalias, Indicadores de Ameaças

1. INTRODUÇÃO

A *Internet* se popularizou e cresceu exponencialmente, resultando na *Internet* das Coisas (IoT – *Internet of Things*) que, nos últimos anos, contribuiu a um aumento significativo da computação em nuvem, cidades inteligentes e Indústria 4.0, aumentando também a superfície de ataque oferecida e a diversidade dos mesmos (Abdullahi *et al.*, 2022). Na esfera da Inteligência de Estado, as ameaças evoluíram para as conhecidas Ameaças Persistentes Avançadas (APT- *Advanced Persistent Threat*), com ataques avançados, furtivos, contínuos e de longo prazo em redes de alvos específicos (Zhou *et al.*, 2022).

Diante deste cenário, qualquer dispositivo que se conecte na *Internet* pode ser vetor de invasão ou alvo, com milhares de dispositivos gerando um volume enorme de registros sobre a conectividade dos mesmos. Assim, existe a necessidade dos serviços de Inteligência de Ameaças Cibernéticas (CTI - *Cyber Threat Intelligence*) (Elmellas, 2016) para analisar e filtrar os dados identificando possíveis ataques. O principal objetivo é apoiar as organizações na compreensão dos riscos e ameaças conhecidas, APTs e ameaças desconhecidas chamadas de dia zero ou *zero-day* (Zhou *et al.*, 2022) (Schlette *et al.*, 2021).

Os sistemas de Inteligência existentes carecem de mecanismos para coleta e classificação preliminar da informação (Marchio, 2014), sendo que em CTI são utilizados sensores que comumente fazem parte dos sistemas de *firewall* das redes (Cheswick e Bellovin, 1994).

Como veremos a seguir, apesar dos avanços recentes na coleta, análise e armazenamento de indicadores de incidentes empregados em CTI (Abdullahi *et al.*, 2022)(Albasheer *et al.*, 2022), as soluções adotadas como suporte para coleta não são otimizadas para identificação e correlação com Indicadores de Ameaças. Os Indicadores de Ameaças podem ser Indicadores de Comprometimento (IoC - *Indicator of Compromise*) ou Indicadores de Ataque (IoA - *Indicator of Attack*), ou ambos (Siebert, 2020). Além disso, os IoCs necessitam de informações adicionais para serem mais facilmente avaliados em Plataformas de Compartilhamento de Inteligência de Ameaças (TISP - *Threat Intelligence Sharing Platforms*) (Sander e Hailpern, 2015).

Este artigo propõe a integração de Sistemas de Detecção de Intrusão (IDS - *Intrusion Detection System*) ou Sistemas de Prevenção de Intrusão (IPS - *Intrusion Prevention System*) (Nam e Kim, 2018) para coleta, utilizando assinaturas em um primeiro estágio e comportamento de aplicações em *honeypots* (Hoepers, Steding-Jessen e Montes, 2003). Assim, gerando registros de possíveis ataques ou comprometimentos e seguida o enriquecimento dos dados dos registros através da coleta de informações complementares relevantes. Sua principal contribuição é apresentar uma metodologia para gerar conhecimento sobre Inteligência de Ameaças, a partir dos registros de sensores de rede, juntamente com uma prova de conceito.

Este artigo está organizado em seções. Na Seção 2 são apresentadas definições e trabalhos correlatos, seguida da Seção 3 que apresenta a metodologia. Na Seção 4 é apresentada a prova de conceito juntamente com os resultados e sua discussão. As conclusões são apresentadas na Seção 5.

2. DEFINIÇÕES E TRABALHOS CORRELATOS

Seguem algumas definições relevantes juntamente com trabalhos relacionados.

2.1 Processo de Geração de Inteligência de Ameaças

Informação de ameaça é qualquer informação que ajude a organização a se proteger de uma ameaça ou detectar as atividades de um atacante. Times de segurança necessitam de um alto grau de maturidade para serem capazes de interpretar dados técnicos de coletas de forma estruturada e assim produzir CTI. O processo de geração de inteligência de ameaças pode ser descrito como Coleta, Processamento, Análise, Inserção e Disseminação (de Melo e Silva *et al.*, 2020). Sucintamente: a coleta envolve a extração e junção de dados, que são apenas fatos ou indicadores; o processamento trabalha na formatação e combinação dos dados, objetivando responder perguntas específicas para gerar informação; a análise avalia os dados e informações de forma conjunta para auxiliar na descoberta de padrões e na produção de inteligência acionável; a implantação visa garantir o suporte para a tomada de decisão contra ameaças de forma proativa; e a disseminação compartilha o conhecimento gerado com partes interessadas.

2.2 Modelo de Dados

Na pesquisa, em busca do modelo de dados mais adequado, encontramos um estudo que se encaixa perfeitamente em nossa metodologia, chamado de método 5W3H (*What, Who, Why, When, Where, How, How much and How long*) (de Melo e Silva *et al.*, 2020). Este método subsidia a tomada de decisão em relação à escolha dos dados a serem enriquecidos.

O método é originalmente conhecido como 5W2H (*What, Who, Why, When, Where, How, How much*). Ele é aplicado em diferentes áreas com o objetivo avaliar um determinado elemento (Burger *et al.*, 2014). O método 5W3H é uma extensão do 5W2H e se mostrou interessante porque além de tratar do registro em todas as suas dimensões também trata da persistência (*how long*). Assim, este método possibilita a caracterização completa de uma ameaça.

Na adequação a este trabalho, "*What*" é usado para definir o elemento em análise. Em CTI pode ser traduzido como a classificação da ameaça. Podem-se criar diversos parâmetros de classificação desde tipos de ameaças até grupos de assinaturas utilizadas na coleta. Em seguida temos o "*Where*" que pode caracterizar a origem. O "*When*" fornece o momento do registro caracterizado pela data e hora do evento. "*How*" fornece o método ou as Técnicas, Táticas e Procedimentos (TTPs) utilizadas pela ameaça. Em toda evidência de ameaça ou incidente é essencial a atribuição da ação a um autor, caracterizado pelo "*Who*". Para uma atribuição mais assertiva é importante buscar definir o "*Why*", contextualizando o cenário através das motivações do evento. Outra questão a ser respondida é a intensidade do evento respondida pelo "*How much*". E, por fim, a duração do evento respondida pelo "*How long*".

2.3 Critérios para Enriquecimento dos Dados

Para definir os critérios para enriquecimento dos dados foram levados em consideração a usabilidade e a relevância da informação agregada. A escolha dos dados a serem enriquecidos é estratégica para subsidiar tomadas de decisão em tempo real, utilização em regras e políticas de defesa da rede, ou robustecer investigações posteriores. Várias fontes de dados podem ser utilizadas para o enriquecimento de Indicadores de Ameaças, tais como redes sociais (Kristiansen *et al.*, 2020), registros de Sistema de Nomes de Domínio (DNS), identificação de prefixos de roteamento que correspondem a um sistema autônomo (AS), *hashs* em repositórios de análise de *malwares* (Botacin, Ceschin e Grégio, 2021), dentre outras.

No caso de Indicadores de Ameaças, existem dados básicos a serem avaliados como endereços IP, nomes de domínio, servidores de domínio, elementos comportamentais de *malware*, cabeçalhos de *e-mail*, dentre outros. Os indicadores contêm um ou mais elementos que contextualizam a ameaça. O contexto pode incluir *time stamps* ("*When*"), por quanto tempo ficaram ativos ("*How long*"), indicação de gravidade do incidente, bem como informações sobre o mecanismo e a dinâmica de um ataque (por exemplo, processo de infecção, disseminação e atuação de um *malware*). Assim foi criado um modelo de dados, priorizando o Endereço IP de origem do fluxo, o Domínio de DNS ou o endereço de *e-mail*, nesta ordem.

2.4 Trabalhos Correlatos

A Tabela 1 a seguir sintetiza os trabalhos mais relevantes, que utilizaram as mesmas ferramentas de IDS e TISP, utilizadas na prova de conceito. E a Tabela 2 mostra as características mais relevantes de cada trabalho.

Tabela 1. Resumo dos trabalhos mais relevantes

Artigo	**Resumo**
(Masip-Bruin *et al.*, 2021)	FISHY usa a coleta de IDS e um sistema para identificação, categorização, classificação e enriquecimento de IoCs usando ML (*Machine Learning*) para sistemas IoT.
(Mironeanu *et al.*, 2021)	ECAD apresenta um novo conceito para integrar ML (*Machine Learning*) e ferramentas analíticas em uma solução de prevenção e detecção de intrusão em tempo real.
(Koloveas *et al.*, 2021)	INTIME é um *framework* integrado baseado em *Machine Learning* e *Deep Learning.*
(Panwar *et al.*, 2017)	A proposta iGen identifica IoCs usando uma Rede Neural Convolucional.
(Kim *et al.*, 2018)	CyTIME é uma estrutura para gerenciar dados CTI e coletar dados de repositórios externos através de canais padronizados. Automaticamente gera regras de segurança.
(Sworna, Islam e Babar, 2022)	A solução APIRO consiste em construção de APIs (*Application Programming Interface*) para de coleta de dados e um modelo de Rede Neural Convolucional para gerar CTI.

Tabela 2. Principais características da Metodologia Proposta

Artigo	(Masip-Bruin *et al.*, 2021)	(Mironeanu *et al.*, 2021)	(Koloveas *et al.*, 2021)	(Panwar *et al.*, 2017)	(Kim *et al.*, 2018)	(Sworna, Islam e Babar, 2022)	**Esta Proposta**
Identifica Ataques em Tempo Real	NÃO	SIM	NÃO	NÃO	NÃO	SIM	**SIM**
Identifica Comprometimento	SIM	SIM	SIM	SIM	SIM	SIM	**SIM**
Utiliza assinaturas de IDS	NÃO	NÃO	NÃO	NÃO	NÃO	NÃO	**SIM**
Gera regras para IDS ou *Firewall*	NÃO	NÃO	NÃO	NÃO	SIM	NÃO	**SIM**
Integra com TISPs	NÃO	SIM	SIM	SIM	SIM	SIM	**SIM**

3. METODOLOGIA PROPOSTA

A proposta é a implantação de sensores para a coleta de anomalias utilizando assinaturas pré selecionadas, alinhadas com a política de segurança e com a estratégia de negócios da organização. Conhecendo o padrão de tráfego na rede podemos escolher as assinaturas e identificar as anomalias. Assim, todos os registros gerados são Indicadores de Ameaças. Além da utilização dos sensores tradicionais que utilizam as assinaturas, se propõe também a possível utilização de *honeypots*, com serviços correlatos aos da organização instalados para registro em tempo real das ameaças às possíveis vulnerabilidades. A Figura 1, criada pelo autor, apresenta a Metodologia Proposta.

Alguns dados dos registros vindos dos sensores são complementados através de um processamento automatizado de enriquecimento, em apoio à Equipe de Tratamento e Resposta à Incidentes de Rede (CSIRT - *Computer Security Incident Response Team*) (Hoepers, Steding-Jessen e Montes, 2003). Este processamento agrega outras informações para melhor investigação da anomalia. Como exemplo, podemos citar o endereço IP (*Internet Protocol*) de origem (*"Who"*). O enriquecimento deste dado pode resultar em um Nome de Domínio Completamente Qualificado (FQDN - *Fully Qualified Domain Name*) através do acesso nas bases raiz do Sistema de Nomes de Domínio (DNS - *Domain Name System*) na *Internet*.

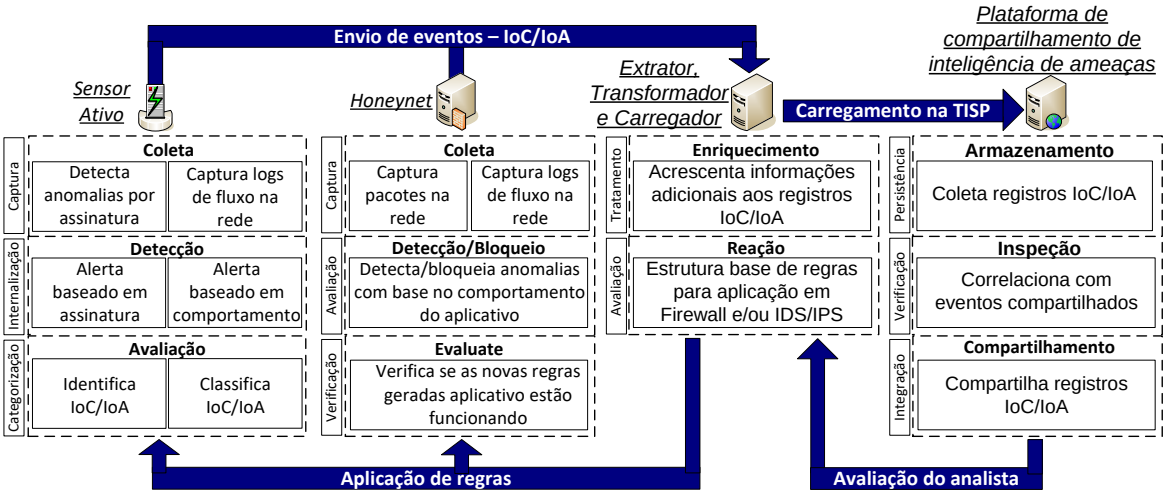

Figura 1. Metodologia Proposta. Fonte: o autor

O FQDN pode identificar imediatamente país de origem e sistema autônomo associado, acelerando a investigação ou a tomada de decisão no caso de ataques. Na avaliação de ataques com TTPs específicas a serviços da organização, uma investigação mais detalhada deve ser feita pela CSIRT sendo subsidiada pelo enriquecimento dos dados. Após o enriquecimento, o registro é carregado na TISP para verificação de outras ocorrências envolvendo informações que constam no registro, sendo possível duas situações: se existirem eventos já relatados, é uma confirmação de ameaça e a equipe de segurança cibernética passa a acompanhar e monitorar o evento como ataque e, se for o caso, ajustar as regras existentes; caso contrário, pode ser um falso positivo ou uma tentativa de ataque de dia zero. Então, é feito o acompanhamento dos registros na TISP aguardando possíveis outros eventos correlatos. No caso da identificação de um ataque, podemos aplicar os protocolos de resposta existentes. Em uma última etapa, todos os registros devem ser armazenados em Plataformas de Compartilhamento de Inteligência de Ameaças (TISPs) para possibilitar o armazenamento com acompanhamento do evento observando novas correlações obtidas dos compartilhamentos das informações de CTI.

4. PROVA DE CONCEITO

4.1 Arquitetura da Prova de Conceito

Para uma atuação efetiva configuramos o sensor IDS coletando tráfego em um *switch* entre o roteador externo e o *firewall*, conforme Figura 2, criada pelo autor. Assim a coleta ocorre antes de qualquer filtro ou intervenção. Entretanto nessa posição o sensor IDS ficaria muito vulnerável a ataques, então configuramos o sensor para apenas executar a coleta tráfego em modo promíscuo, situação em que ele não responde a conexões. Colocamos uma máquina com serviço *web* como espelho do repositório de assinaturas protegida pelo *firewall*, atualizando as assinaturas diariamente. Assim o sensor busca estas assinaturas na *intranet* e atualiza seu contexto.

O sensor envia os indicadores de ameaças para um sistema de armazenamento de registros na *intranet*, também protegido pelo *firewall*, onde são enriquecidos. Em seguida os indicadores de ameaça já enriquecidos seguem diretamente para o MISP ou podem ser aplicados no *firewall*.

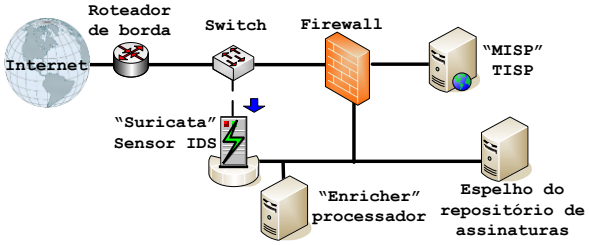

Figura 2. Arquitetura da prova de conceito. Fonte: o autor

O sensor escolhido para a coleta é o Suricata IDS (OISF, 2020). O Suricata pode realizar a coleta de todo o tráfego ou apenas o registro baseado em assinaturas. Levando em consideração a agilidade e otimização das informações que serão produzidas, focaremos apenas nos registros baseados em assinaturas, que já fornecem uma pré-classificação dos eventos. Assim, foram considerados apenas com os registros da atividade já classificada como anômala e aderente à política de segurança da organização.

Na proposta, leva-se em conta a base de assinaturas existentes no repositório *Emerging Threats* <https://rules.emergingthreats.net/>. Neste repositório as assinaturas são disponibilizadas já classificadas e categorizadas por tipo de Indicador de Ameaça. Todos os dias o repositório é atualizado aproximadamente às 22:00 UTC, com todas as informações identificadas com carimbo de tempo no formato *Universal Sortable Date Time Pattern* "Z" e com registro de horário estendido "T", perfazendo o formado YYYY-MM-DDTHH:MM:SSZ (*Date Time Format Info. Universal Sortable Date Time Pattern*, sem data).

4.1.1 Sensor: Suricata e *Emerging Threats*

O repositório de assinaturas da *Emerging Threats* é totalmente compatível e configurável no IDS Suricata (Schreiber, Meehan e Langston, 2020), contando com um conjunto de regras pré-classificadas em grupos de ameaças. Todas atividades conhecidamente suspeitas, potencialmente maliciosas ou claramente hostis, pela comunidade de segurança cibernética. Assim, tem-se um mecanismo de *download* diário desta base de Inteligência de Ameaças no formato de regras aplicadas como assinaturas no IDS (Alcantara *et al.*, 2021).

4.1.2 TISP: MISP

O elemento configurado como Plataforma de Compartilhamento de Inteligência de Ameaças (TISPs) é o MISP. O software Suricata e o MISP foram localizados em documentos acadêmicos atuais, sendo este o motivo da escolha (Masip-Bruin *et al.*, 2021)(Mironeanu *et al.*, 2021)(Koloveas *et al.*, 2021). Assim a prova de conceito atende a todos os elementos propostos na metodologia contemplando a coleta, avaliação, enriquecimento, estruturação e compartilhamento dos Indicadores de Ameaças.

4.1.3 Enriquecimento dos Dados: *Enricher*

Um mecanismo para enriquecimento de dados é um programa com a função de adicionar informações aos dados dos registros, facilitando a interpretação e análise das informações. Na prova de conceito apresentada, utilizou-se uma versão adaptada do *Enricher* (Sousa, Gondim e Albuquerque, 2021), mas poderia ser usado qualquer sistema que buscasse em repositórios informações complementares relevantes para os Indicadores de Ameaça. A opção pelo *Enricher* foi devido a sua simplicidade na implantação no *framework* e o acesso a seu código fonte. Originalmente o *Enricher* busca nos registros do Suricata em formato JSON, por um dos três tipos de parâmetros iniciais de busca: endereço IP, domínio de DNS, ou endereço de *e-mail*, sendo usado apenas o primeiro na nossa prova de conceito. Assim, o programa busca o endereço IP que é pesquisado nas bases raiz do DNS (*root DNS*) e em seguida verificado no *site* <https://www.ipvoid.com/> (Company, 2010), conforme apresentado no fluxograma da Figura 3, criada pelo autor. Em seguida o programa fará a conexão com a TISP criando um novo evento com o endereço IP informado.

O objetivo pretendido desta prova de conceito é a construção de um modelo funcional da metodologia e demonstrar as atividades, segundo o fluxo descrito na Figura 3. O fluxo de análise dos registros gerados pelos sensores (IDS/IPS, *Honeypots* ou *Firewall*) deve seguir o fluxograma apresentado na Figura 3.

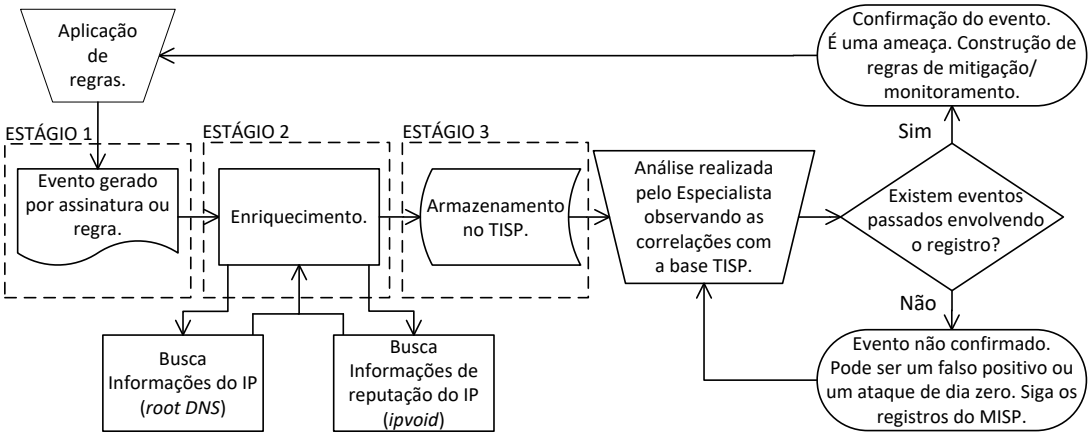

Figura 3. Fluxo proposto para a Gestão de Ameaças. Fonte: o autor

4.2 Resultados

Após a implementação da prova de conceito em laboratório foram obtidos vários registros em formato JSON, mas com muitos registros de controle como de rastreamento das comunicações DNS, alertas de monitoração para controle de TLS e conexões HTTP, conforme observamos na Figura 4. Portanto, foi necessária a filtragem antes do envio para o *Enricher*, para seleção apenas dos alertas com possíveis ameaças.


```
{"timestamp":"2022-07-17T00:42:07.343213-0300","flow_id":665765112921261,"event_type":"dns","src_ip":"164.163.0.226","src
{"timestamp":"2022-07-17T00:42:07.360540-0300","flow_id":665765112921261,"event_type":"dns","src_ip":"8.8.8.8","src_port"
{"timestamp":"2022-07-17T00:42:26.375458-0300","flow_id":705180029048897,"event_type":"http","src_ip":"164.163.0.226","sr
{"timestamp":"2022-07-17T00:42:31.913314-0300","flow_id":1089446458403915,"event_type":"dns","src_ip":"8.8.4.4","src_port
{"timestamp":"2022-07-17T00:42:31.916031-0300","flow_id":1295055132817983,"event_type":"dns","src_ip":"164.163.0.226","sr
{"timestamp":"2022-07-17T00:42:31.933368-0300","flow_id":1295055132817983,"event_type":"dns","src_ip":"8.8.4.4","src_port
{"timestamp":"2022-07-17T00:42:33.392280-0300","flow_id":480574714805336,"event_type":"dns","src_ip":"164.163.0.226","src
{"timestamp":"2022-07-17T00:42:33.420062-0300","flow_id":480574714805336,"event_type":"dns","src_ip":"8.8.8.8","src_port"
{"timestamp":"2022-07-17T00:42:35.398086-0300","flow_id":2242211385901759,"event_type":"alert","src_ip":"2.16.15.88","src
{"timestamp":"2022-07-17T00:42:46.320116-0300","flow_id":2203973292787548,"event_type":"alert","src_ip":"69.164.45.64","s
{"timestamp":"2022-07-17T00:42:53.003577-0300","flow_id":622471845549742,"event_type":"tls","src_ip":"164.163.0.226","src
{"timestamp":"2022-07-17T00:43:14.297231-0300","flow_id":217933172345103,"event_type":"alert","src_ip":"89.248.165.169","
{"timestamp":"2022-07-17T00:43:35.856565-0300","flow_id":1382698239594997,"event_type":"alert","src_ip":"89.248.165.169",
```


Figura 4. Registro gerado pelo IDS, antes da filtragem

Para uma melhor análise das ameaças, foi realizada uma filtragem nos registros, buscando apenas as entradas com alertas efetivos gerados pelas assinaturas, e dentre estas apenas as informações de interesse, tais como *timestamp*, *src_ip*, *signature* e *category*, conforme Figura 5. Para melhor observação dos alertas, foram transformadas no seguinte formato de registro:


```
{"timestamp":"2022-07-17T00:42:35.398086-0300","src_ip":"2.16.15.88","signature":"ET SCAN Sipvicious Scan","category":"Attempted Information Leak"}
{"timestamp":"2022-07-17T00:42:46.320116-0300","src_ip":"69.164.45.64","signature":"ET TOR Known Tor Exit Node Traffic group 21","category":"Misc Attack"}
{"timestamp":"2022-07-17T00:43:14.297231-0300","src_ip":"89.248.165.169","signature":"ET DROP Dshield Block Listed Source group 1","category":"Misc Attack"}
{"timestamp":"2022-07-17T00:43:35.856565-0300","src_ip":"89.248.165.169","signature":"ET DROP Dshield Block Listed Source group 1","category":"Misc Attack"}
```


Figura 5. Registro após realizada a filtragem

A seguir, foi realizada a análise dos registros, classificando-os por *signature* e por IP utilizando um *script python3* desenvolvido especificamente para esta finalidade, conforme Figura 6. Assim, foram obtidos os alertas com mais entradas no registro que em seguida foram submetidos ao enriquecimento (*Enricher*).

```
In [13]: #Monta um novo dataframe apenas com o IP e a assinatura tratada e remove as duplicadas
         df_ip = df_all_files[["src_ip","signature_parsed"]].drop_duplicates(ignore_index=True)

         print(df_ip)

                src_ip    signature_parsed
         0      2.16.15.88  ET SCAN Sipvicious
         1    69.164.45.64        ET TOR Known
         2  89.248.165.169     ET DROP Dshield

In [14]: #Conta a quantidade de vezes que o ip aparece para cada assinatura tratada
         df_count = df_ip.groupby(['src_ip'])['src_ip'].count()
         print(df_count)

         src_ip
         2.16.15.88        1
         69.164.45.64      1
         89.248.165.169    1
         Name: src_ip, dtype: int64
```

Figura 6. Classificação do registros filtrados, pronto para envio ao *Enricher*

Após a carga no MISP, no dia seguinte observou-se, que um endereço IP foi correlacionado com outros dois eventos já relatados por outras organizações que executam o compartilhamento de registro com nosso CTIR, conforme Figura 7. Na figura foram omitidos dados que identifiquem o sistema em produção.

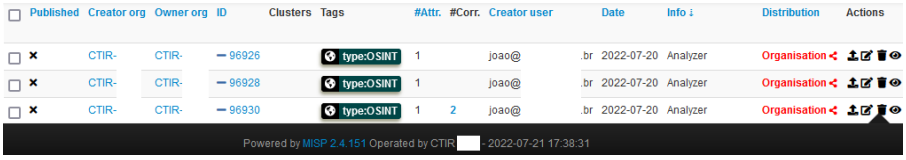

Figura 7. Alertas transformados em eventos no MISP (imagem sanitizada por se tratar de sistema em produção)

4.2.1 Discussão

De acordo com o fluxo da Figura 3, no primeiro estágio a utilização dos dados do sensor coletor IDS com assinaturas atualizadas acelerou a coleta de informações com qualidade, através de regras com assinaturas que fornecem registros de Indicadores de Ameaças minimamente categorizados e organizados. Por se tratar de coleta e análise em tempo real, foi possível identificar ataques em andamento. Deve-se registrar que na filtragem dos registros produzidos pelo IDS, imediatamente foram identificados os possíveis IoC e IoA. Dessa forma, houve um ganho de eficiência no processo.

No segundo estágio realizou-se um processamento do *Enricher* para enriquecimento destes registros com a coleta de informações complementares relevantes, que facilitou a identificação dos ataques por analistas. Ao final deste estágio não houve uma filtragem buscando qualidade de informações obtidas do enriquecimento, uma vez que se optou pela carga de todos os dados obtidos na TISP para posterior avaliação.

Finalmente, no terceiro estágio, houve a carga dos dados no MISP. Ficou evidente que a decisão de não realizar a filtragem após o *Enricher* foi acertada, pois a base de eventos do MISP, identificou rapidamente os registros que já possuíam histórico. Assim, foram identificados os indicadores e os possíveis falsos positivos.

5. CONCLUSÃO

A arquitetura proposta desenvolveu de um *framework* metodológico para a geração e análise sistemática dos registros com identificação de padrões anômalos e a derivação de regras de detecção codificadas por meio de assinaturas. Como prova de conceito, foi realizada a implementação da arquitetura atingindo os objetivos da proposta satisfatoriamente.

A prova de conceito demonstrou que a arquitetura proposta possibilita a aceleração de identificação de ameaças e possíveis incidentes antes que os mesmos sejam amplamente reportados pela comunidade, contribuindo para antecipação de ações de segurança e inteligência de ameaças cibernéticas.

Todos os sistemas utilizados na prova de conceito são *OpenSource*, adotando formatos de protocolos padronizados pela comunidade de Inteligência de Ameaças. Estas características facilitam seu emprego e flexibilizam sua utilização, deixando clara a aplicabilidade da arquitetura proposta. Assim, a metodologia pode ser adotada amplamente pelas organizações sendo adaptativa a ferramentas e soluções já instaladas. Além disso, observa-se a importância de uma TISP compartilhando informações com várias bases de dados.

Como trabalhos futuros pode-se considerar as questões relativas à integração com outros tipos de sensores, bem como em outras Plataformas de Compartilhamento de Inteligência de Ameaças - TISPs.

AGRADECIMENTOS

Os autores agradecem o apoio da ABIN TED 08/2019.

REFERÊNCIAS

Abdullahi, M. *et al.* (2022) “Detecting Cybersecurity Attacks in Internet of Things Using Artificial Intelligence Methods: A Systematic Literature Review”, *Electronics (Switzerland)*, 11(2), p. 1–28. doi: 10.3390/electronics11020198.

Albasheer, H. *et al.* (2022) “Cyber-Attack Prediction Based on Network Intrusion Detection Systems for Alert Correlation Techniques: A Survey”, *Sensors*, 22(4), p. 1494. doi: 10.3390/S22041494.

Alcantara, L. *et al.* (2021) “Syrius: Synthesis of Rules for Intrusion Detectors”, *IEEE Transactions on Reliability*, p. 1–12. doi: 10.1109/TR.2021.3061297.

Botacin, M., Ceschin, F. e Grégio, A. (2021) “Corvus: Uma solução Sandbox e de Threat Intelligence para Identificação e Análise de Malware”, *Anais Estendidos do XXI Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais*, p. 50–57. doi: 10.5753/SBSEG_ESTENDIDO.2021.17339.

Burger, E. W. *et al.* (2014) “Taxonomy Model for Cyber Threat Intelligence Information Exchange Technologies”. doi: 10.1145/2663876.2663883.

Cheswick, W. R. e Bellovin, S. M. (1994) *Firewalls and Internet security : repelling the wily hacker*. Addison-Wesley. Available at: https://archive.org/details/firewallsinterne00ches (Acessado: 7 de abril de 2021).

Company, N. (2010) *IP Address Tools, Network Tools, DNS Tools | IPVoid*. Available at: https://www.ipvoid.com/ (Acessado: 19 de março de 2022).

Date Time Format Info. Universal Sortable Date Time Pattern (sem data) *GitHub*. Available at: http://shorturl.at/gKX27 (Acessado: 23 de abril de 2022).

Elmellas, J. (2016) “Knowledge is power: the evolution of threat intelligence”, *Computer Fraud and Security*, 2016(7), p. 5–9. doi: 10.1016/S1361-3723(16)30051-3.

Hoepers, C., Steding-Jessen, K. e Montes, A. (2003) “Honeynets Applied to the CSIRT Scenario”, in *FIRST*, p. 9. Available at: http://www.honeynet.org/alliance/ (Acessado: 17 de maio de 2022).

Kim, E. *et al.* (2018) “Cytime: Cyber threat intelligence management framework for automatically generating security rules”, *ACM International Conference Proceeding Series*, Part F1377. doi: 10.1145/3226052.3226056.

Koloveas, P. *et al.* (2021) “inTIME: A Machine Learning-Based Framework for Gathering and Leveraging Web Data to Cyber-Threat Intelligence”, *Electronics*, 10(7), p. 818. doi: 10.3390/electronics10070818.

Kristiansen, L. M. *et al.* (2020) “CTI-Twitter: Gathering Cyber Threat Intelligence from Twitter using Integrated Supervised and Unsupervised Learning”, *Proceedings - 2020 IEEE International Conference on Big Data, Big Data 2020*, p. 2299–2308. doi: 10.1109/BigData50022.2020.9378393.

Marchio, J. (2014) “Analytic Tradecraft and the Intelligence Community: Enduring Value, Intermittent Emphasis”, *Intelligence and National Security*, 29(2), p. 159–183. doi: 10.1080/02684527.2012.746415.

Masip-Bruin, X. *et al.* (2021) “Cybersecurity in ict supply chains: Key challenges and a relevant architecture”, *Sensors*, 21(18). doi: 10.3390/S21186057.

de Melo e Silva, A. *et al.* (2020) “A methodology to evaluate standards and platforms within cyber threat intelligence”, *Future Internet*, 12(6), p. 1–23. doi: 10.3390/fi12060108.

Mironeanu, C. *et al.* (2021) “Experimental cyber attack detection framework”, *Electronics (Switzerland)*, 10(14). doi: 10.3390/ELECTRONICS10141682.

Nam, K. e Kim, K. (2018) “A Study on SDN security enhancement using open source IDS/IPS Suricata”, *9th International Conference on Information and Communication Technology Convergence: ICT Convergence Powered by Smart Intelligence, ICTC 2018*, p. 1124–1126. doi: 10.1109/ICTC.2018.8539455.

OISF (2020) “Suricata | Open Source IDS / IPS / NSM engine”. Open Information Security Foundation. Available at: https://suricata-ids.org/ (Acessado: 7 de abril de 2021).

Panwar, A. *et al.* (2017) *iGen: Toward Automatic Generation and Analysis of Indicators of Compromise (IOCs) using Convolutional Neural Network*. Arizona State University. Available at: https://hdl.handle.net/2286/R.I.44216.

Sander, T. e Hailpern, J. (2015) “UX Aspects of Threat Information Sharing Platforms”, in *Proceedings of the 2nd ACM Workshop on Information Sharing and Collaborative Security*. New York, NY, USA: ACM, p. 51–59. doi: 10.1145/2808128.2808136.

Schlette, D. *et al.* (2021) “Measuring and visualizing cyber threat intelligence quality”, *International Journal of Information Security*, 20, p. 21–38. doi: 10.1007/s10207-020-00490-y.

Schreiber, J., Meehan, M. e Langston, R. (2020) *2021 Open Source IDS Tools: Suricata vs Snort vs Bro (Zeek) | AT&T Cybersecurity*, *AT&T Business Blog*. Available at: http://shorturl.at/NTY48 (Acessado: 21 de abril de 2022).

Siebert, E. (2020) *Indicadores de ataque versus indicadores de comprometimento*, *Network*. Austin, Texas. Available at: http://shorturl.at/hlQV6.

Sousa, C. E. de, Gondim, J. J. C. e Albuquerque, R. de O. (2021) *ENRICHER:ferramenta de enriquecimento de dados integrada à plataforma MISP*. Universidade de Brasília.

Sworna, Z. T., Islam, C. e Babar, M. A. (2022) “APIRO: A Framework for Automated Security Tools API Recommendation”, p. 41. Available at: https://arxiv.org/abs/2201.07959v1.

Zhou, Y. *et al.* (2022) “CTI View: APT Threat Intelligence Analysis System”, *Security and Communication Networks*, 2022. doi: 10.1155/2022/9875199.