Método para Uso do SIEM como Ferramenta de Inteligência e Automação

Fonte: Amazon

José Lopes
Luiz Batista

8º Fórum Brasileiro de CSIRTs

São Paulo, 10/09/2019

Agenda

1. Histórico
2. Política de SIEM
3. Processamento de Dados
4. Casos de Uso
5. Trabalhos Futuros
6. Conclusão

Histórico

- Empresa auditada por **SOX** para negociar ações na Bolsa de Nova Iorque
- Adquire **SIEM** em 2006 para atendimento de controles SOX
- SIEM usado majoritariamente como banco de dados de ***logs***
- Novo SIEM adquirido em 2017

Histórico

- Novo SIEM adquirido:
  - + robustez
  - + funcionalidades
- Mais cobranças por automação de controles SOX
- Aumento expressivo de origens de log (~50 → ~250)

Fonte: Fine Art America

Política de SIEM

- Objetivo
  Diretrizes e padrões
- Escopo
  Apenas sistemas em produção
- Nomenclatura
- Tempos de Retenção

Política de SIEM

Nomes

Origens de *log*

- unix_honeypot_certbr
- unix_sage_1
- paloalto_panos

Campos de *log*

- cors_honeypot_user
- cors_honeypot_password
- cors_paloalto_rule

Pesquisas

- compliance_sox_dss0501
- monitoring_wsa_realtime
- tshoot_vpn_users_logged

Tempos de Retenção

Curtíssimo prazo --6 meses

- routers, switches
- *netflows*

Curto prazo --18 meses

- firewalls, *proxies*
- IPSs
- antivírus

Médio prazo --30 meses

- NAC

Longo prazo --60 meses

- *domain controllers*

Política de SIEM

Sanitização de *logs* Windows

	Antes	Depois	Redução
Origens de log	92	66	28,26%
Event IDs	1.069	136	87,28%
EPS	3.217	2.157	32,95%

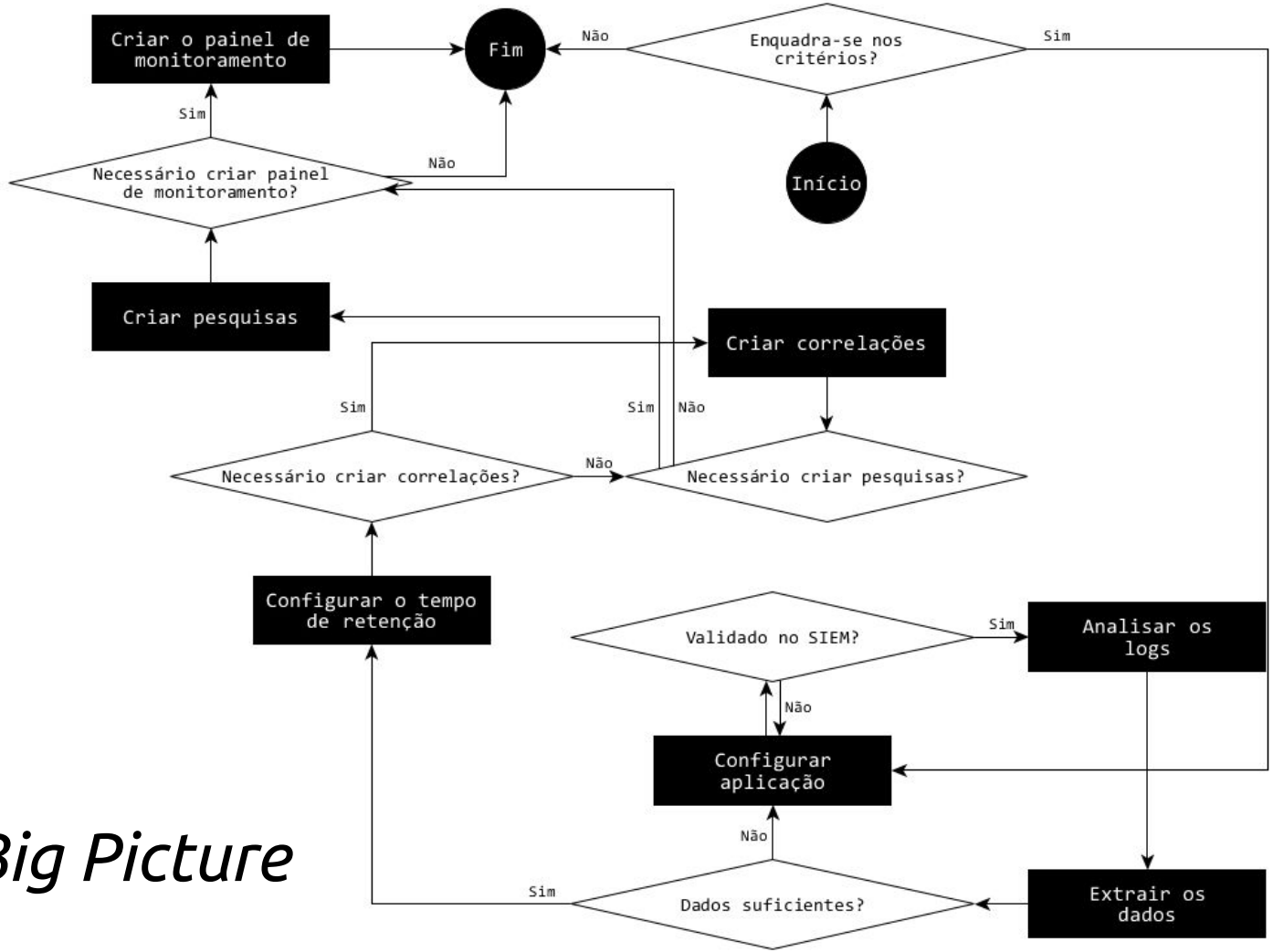
Sanitização de correlações

Total	Ativadas
543	61

Processamento de Dados

1. Configuração básica
   Envio, cadastro, estudo e extração de dados
2. Criação de correlações
   Escrita de regras com dados de uma ou mais origens
3. Criação de pesquisas
   Agrupamento e listagem de dados
4. Criação de monitoramento
   Painéis compostos por dados diversos

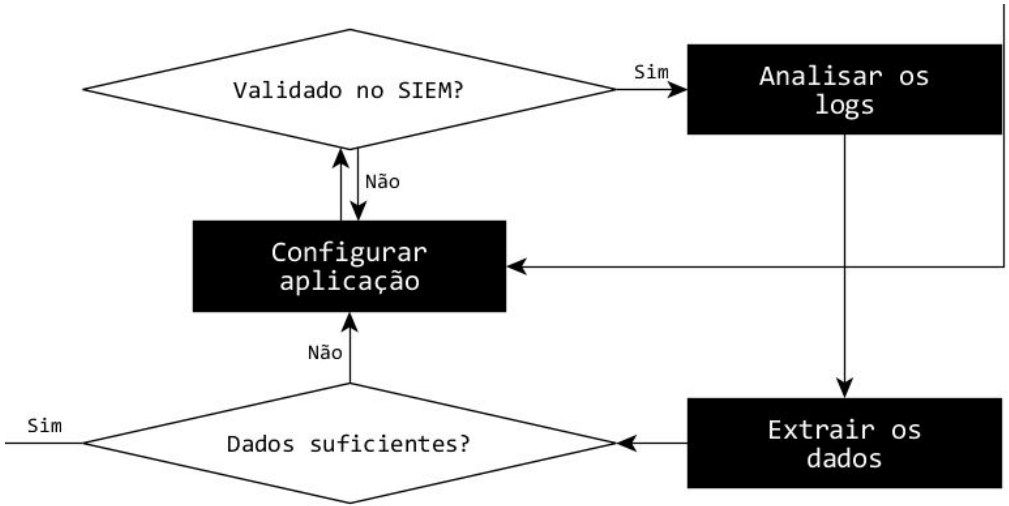
The Big Picture



Processamento de Dados

Configurações básicas

- ***Logs*** não têm padrões definidos, requerendo que o time saiba como extrair os dados
- ***Netflows*** são mais fáceis de configurar, desde que o SIEM tenha suporte



Processamento de Dados

Extrações de dados em *logs*

- Entendimento de padrões usados pelas ferramentas
- Uso extensivo de **expressões regulares** (*regexes*) para extração
- Cuidado com *regexes:* https://blog.cloudflare.com/details-of-the-cloudflare-outage-on-july-2-2019/

```
1 <13>Mar 20 17:47:50 logger[84804]: 2019-03-19 20:29:25 +0000: ftp-honeyd.pl[39832]: IP:
    54.215.xxx.yyy, USER: 'anonymous'
2 <13>Jun 13 00:30:10 logger[90565]: Jun 12 23:53:06 tesla sshd-honeyd[5742]: password auth
    succeeded for 'root' (password 'root') from 141.98.xxx.yyy
3 <13>Jun 13 00:30:08 logger[68364]: 2019-06-12 02:23:24 +0000: pop3-honeyd.pl[18239]: IP:
    193.56.xxx.yyy, USER: 'spammer'
4 <13>Jun 13 00:30:07 logger[9923]: 2019-06-12 23:49:27 +0000: dlink-telnetd.pl[50705]: IP:
    128.201.xxx.yyy, status: login failed, login: "Administrator", password: "admin"
```

Processamento de Dados

Processamento de Dados

Correlações

Nível	Descrição
1	Incidentes são detectados a partir de um tipo de dados.
2	Incidentes são detectados a partir do cruzamento de mais de um tipo de dados, de uma ou mais origens, ou de outras varíaveis, como tempo e limites estabelecidos.
3	Ações são executadas automaticamente em outras ferramentas a partir da detecção de incidentes, sendo esses abertos apenas para conferência humana.

Processamento de Dados

Algoritmo 1: CORRELAÇÃO DE ANTIVÍRUS.

Entrada: *log_source_group*, *av_category*, *av_malware_categories*, *av_action*, *av_malware_actions*
Saída: Incidente registrado

```
1 início
2     se log_source == 'antivirus' então
3         se av_category ∈ av_malware_categories E
            av_action ∈ av_malware_actions então
4             registra incidente;
5         fim
6     fim
7 fim
```

Antes: **350** incidentes por mês
Depois: **107** incidentes por mês
Redução: **69,42%**

Algoritmo 2: CORRELAÇÃO DE DADOS DO HONEYPOT E FIREWALLS.

Entrada: *flow_source*, *log_source_group*, *honeypot_blacklist*, *honeypot_exclusion_list*, $source_ip$
Saída: Incidente registrado

```
1  início
2      se flow_source == 'honeypot' então
3          se source_ip ∉ honeypot_blacklist então
4              honeypot_blacklist ← source_ip
5          fim
6      fim
7      se log_source_group == 'firewalls' então
8          se source_ip ∈ honeypot_blacklist E
             source_ip ∉ honeypot_exclusion_list então
9              registra incidente;
10         fim
11     fim
12 fim
```

Processamento de Dados

Pesquisas

- Usadas para agrupar dados para ajudar na obtenção de informações, seja para monitoramento, seja para resolução de problemas
- Salvar pesquisas para uso futuro ajuda a diminuir o tempo de resposta a incidentes, ao agilizar o acesso a informações

```
1  select dateformat(starttime,'yyyy-MM-dd␣
       HH:mm'),
       "cors_mcafee_updated_hosts_percent"
2  from events
3  where logsourcename(logsourceid) =
       'mcafee_epo_2'
4  order by starttime desc
5  last 30 days
```

```
1  select "cors_honeypot_pass" as pass,
       count(*) as cpass
2  from events
3  where (sourceip = '128.201.xxx.yyy') and
       ("cors_honeypot_user" is not null)
4  group by pass
5  order by cpass desc
6  limit 10
7  last 30 days
```

Processamento de Dados

Monitoramento

- ### Gráficos
  Boa forma de acompanhar o comportamento do ambiente

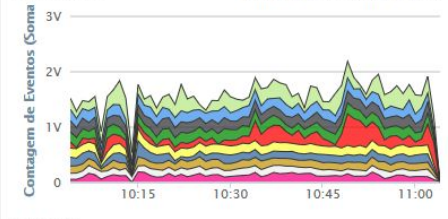
- ### Analista
  Precisa ter habilidade para identificar anomalias

- ### Procedimentos
  Devem estar definidos para ações efetivas

Mostrar Painel: Monitoramento CORS #1 | Novo Painel | Renomear Painel | Excluir Painel | Incluir Item... ▼ | Próxima Atualização: 00:00:45

monitoring_firewall_deny_src (Contagem de Eventos)

Redefinir Zoom 27/06/19 10:04 - 27/06/19 11:04



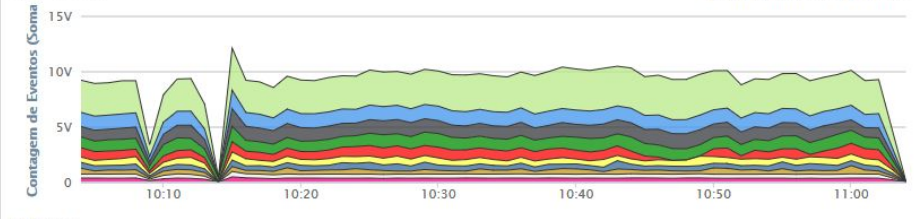
▼ Legenda

83.97. . 192.168. . 177.190. .
10.20. . 10.4. . 192.168. .
192.168. . 192.168. . 177.190. .
192.168. . Restante

Visualizar em Atividade do Log

monitoring_firewall_deny_dst (Contagem de Eventos)

Redefinir Zoom 27/06/19 10:04 - 27/06/19 11:04



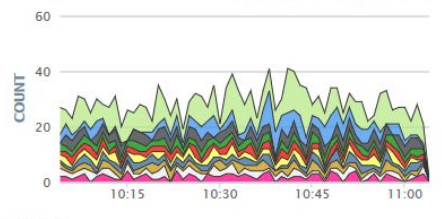
▼ Legenda

172.217. . 192.168. . 172.217. . 8.8. . 23.74. . 192.168. . 192.168. .
192.168. . 192.168. . 194.30. . Restante

Visualizar em Atividade do Log

CORS.CO.02 (COUNT) (série temporal)

Redefinir Zoom 27/06/19 10:04 - 27/06/19 11:04



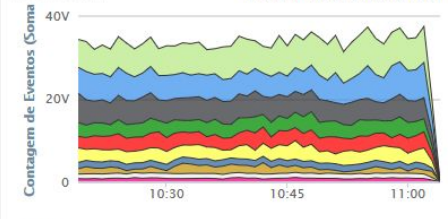
▼ Legenda

185.176. . 185.176. . 77.247. .
102.165. . 216.170. . 83.149. .
176.9. . 159.89. . 5.79. . 179.43. .
Restante

Visualizar em Atividade de Rede

monitoring_firewall_allow_src (Contagem de Eventos)

Redefinir Zoom 27/06/19 10:19 - 27/06/19 11:04



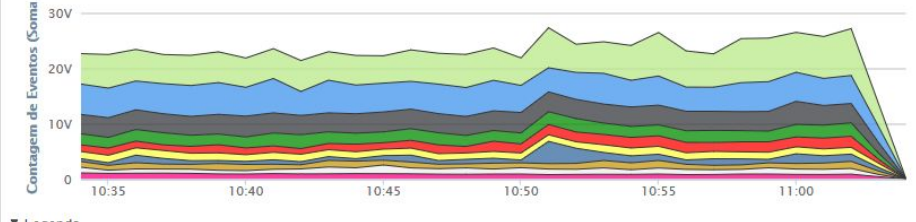
▼ Legenda

10.2. . 192.168. . 192.168. . 10.2. .
10.2. . 10.2. . 10.2. . 10.2. .
10.230. . 10.2. . Restante

Visualizar em Atividade do Log

monitoring_firewall_allow_dst (Contagem de Eventos)

Redefinir Zoom 27/06/19 10:34 - 27/06/19 11:04



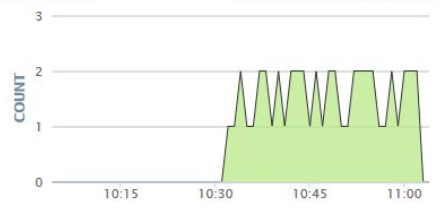
▼ Legenda

10.2. . 10.30. . 192.168. . 192.168. . 208.67. . 128.201. . 10.30. .
10.30. . 128.201. . 192.168. . Restante

Visualizar em Atividade do Log

monitoring_firepower_top_block (COUNT) (série temporal)

Redefinir Zoom 27/06/19 10:04 - 27/06/19 11:04



▼ Legenda

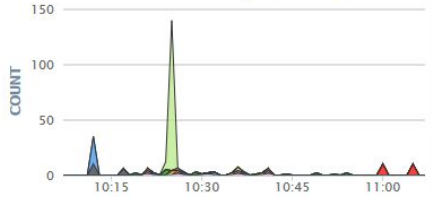
192.168. .

Visualizar em Atividade do Log

Mostrar Painel: Monitoramento CORS #2 | Novo Painel | Renomear Painel | Excluir Painel | Incluir Item... ▼ | Próxima Atualização: 00:00:40

monitoring_mcafee_threat_host (COUNT) (série temporal)

Redefinir Zoom 27/06/19 10:07 - 27/06/19 11:07



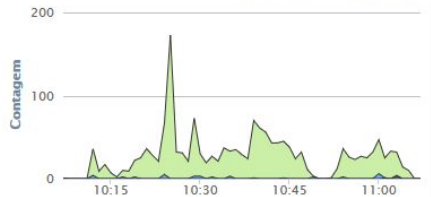
▼ Legenda

NOTP NOTP MICP
MICP MICP MICP
MICP MICP MICP
micp Restante

Visualizar em Atividade do Log

monitoring_mcafee_top_threat (Contagem) (série temporal)

Redefinir Zoom 27/06/19 10:07 - 27/06/19 11:07

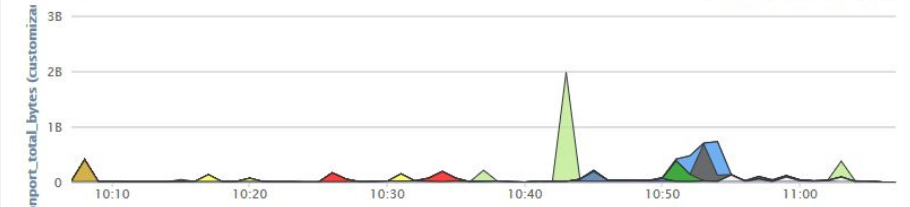


▼ Legenda

Visualizar em Atividade do Log

monitoring_wsa_top_access (cors_ironport_total_bytes)

Redefinir Zoom 27/06/19 10:07 - 27/06/19 11:07



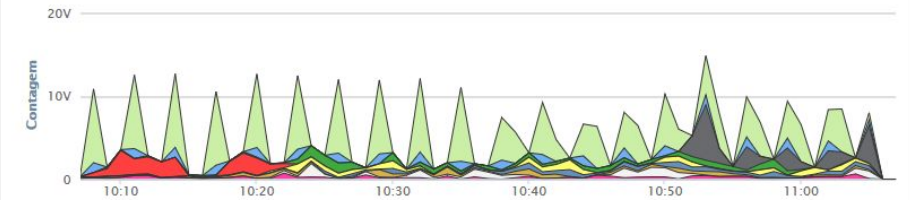
▼ Legenda

N/D:10.20. . c053 :10.20. . N/D:10.40. . N/D:10.20.10.214 N/D:10.20. . c050 :10.20. .
N/D:10.20. . N/D:172.18. . c057 :10.20. . e20 :10.20. . Restante

Visualizar em Atividade do Log

monitoring_wsa_top_block (Contagem) (série temporal)

Redefinir Zoom 27/06/19 10:07 - 27/06/19 11:07



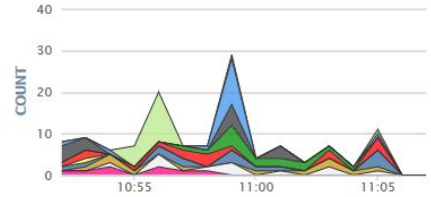
▼ Legenda

e22 :10.20. . e21 :10.2. . c053 :10.12. . N/D:10.20. . e20 :10.20. . N/D:10.40. .
N/D:10.40. . N/D:10.40. . N/D:10.4. . N/D:10.40. . Restante

Visualizar em Atividade do Log

monitoring_esa_top_helo (COUNT) (série temporal)

Redefinir Zoom 27/06/19 10:52 - 27/06/19 11:07



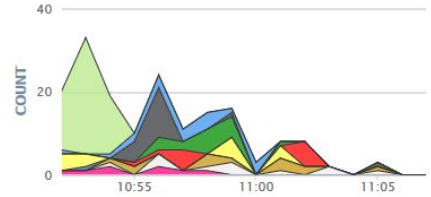
▼ Legenda

.acessabrasil.com.br mail.remo.com.br
.ons.org.br .app.etouches.com
.outbound.protection.outlook.com
.smiles.com.br

Visualizar em Atividade do Log

monitoring_esa_top_from (COUNT) (série temporal)

Redefinir Zoom 27/06/19 10:52 - 27/06/19 11:07



▼ Legenda

@encel.com.br
@d-view.uhmailsrvc6.com @mkt.anefac.com.br
@mbaconstrutora.com.br
@bounces.santander.com.br @ons.org.br

Visualizar em Atividade do Log

Casos de Uso

Honeypot

Netflows --IPFIX

Logs de acessos: syslog, *users*, *passwords*, URLs

```
<13>Jul 31 00:30:07 logger[26308]: Jul 30 19:27:49 tesla sshd-honeyd[64166]: password auth succeeded for 'root' (password 'root') from 141.98.xxx.yyy
```

https://gist.github.com/forkd/81b90d86b30e2730df241c90cc323837

Fonte: Piming

Casos de Uso

Honeypot

- Uso de *netflow* para monitoramento de acessos
- Processamento de *logs* para análise de dados
- Exemplos: nomes de usuário, senhas e URLs recebidas pelos *listeners* do honeypot em 30 dias

Usernames

Username	#
root	68.249
admin	15.456
guest	2.289
shell	1.737
enable	1.542
supervisor	1.451
default	845
support	817
administrator	759
Administrator	750

Passwords

Password	#
root	31.522
1234	2.937
admin	2.254
password	2.245
system	2.215
12345	2.190
	1.583
123456	1.504
54321	1.491
aquario	1.482

Casos de Uso

Honeypot

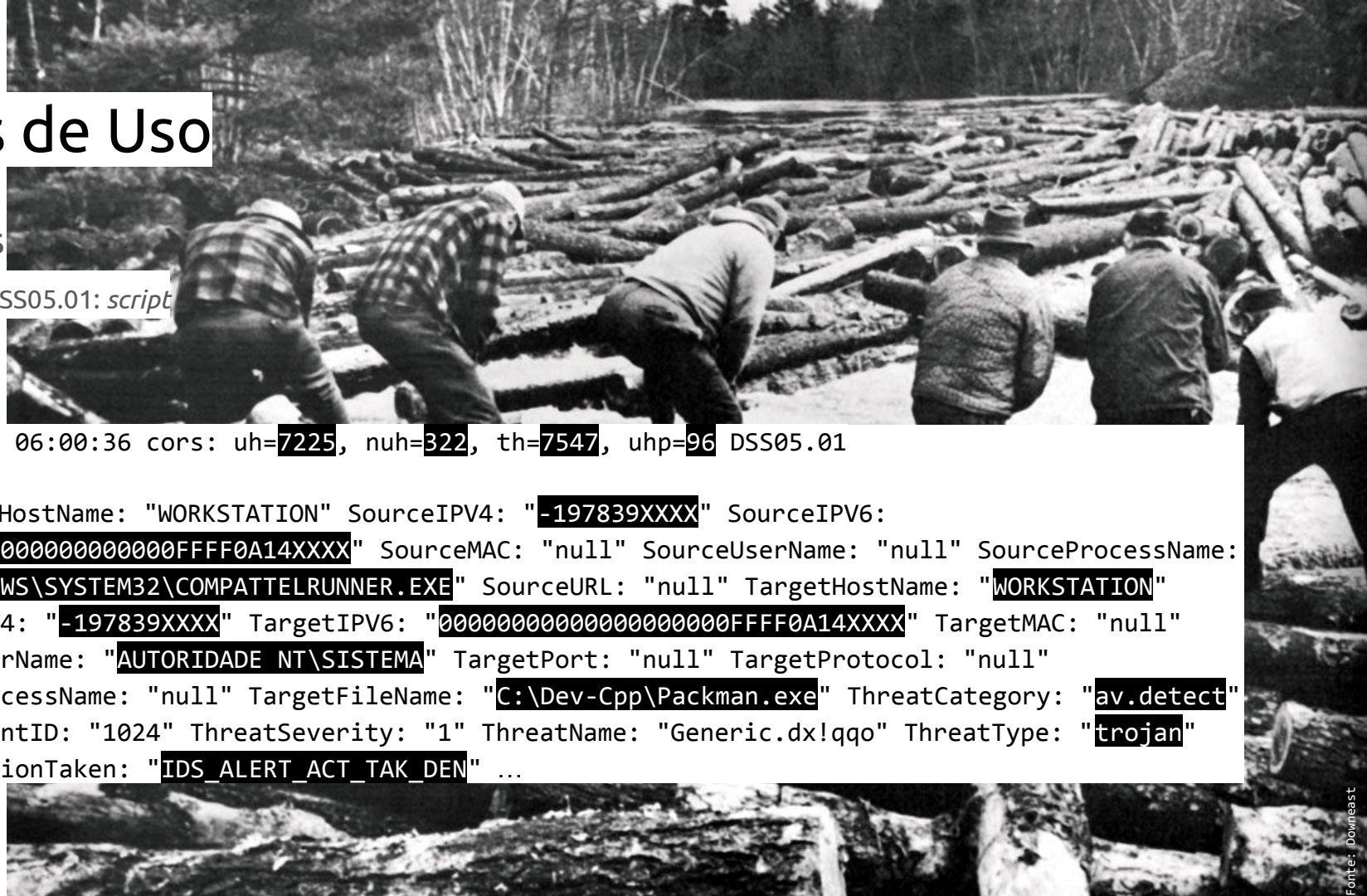
URLs	
URL	#
http://23.254.138.248:80/8mips8	2.056
http://198.12.97.68:80/bins/UnHAnaAW.mips	944
http://209.141.46.124:80/bins/mips	593
http://68.183.233.217:80/bins/hoho.mips	563
http://51.79.54.106:80/bins/hoho.mips	526
http://142.11.211.114:80/8mips8	508
http://178.128.92.133:80/bins/hoho.mips	454
http://137.74.154.197:80/bins/Ruthless1337.mips	431
http://142.11.240.29:80/bins/kowai.mips	351
http://209.141.46.124:80/bins/wolf.mips	285

https://www.sans.org/reading-room/whitepapers/malicious/analyzing-backdoor-bot-mips-platform-35902 → MIPS

Casos de Uso

Antivírus

SOX DSS05.01: *script*



```
<5>Jul 30 06:00:36 cors: uh=7225, nuh=322, th=7547, uhp=96 DSS05.01

… SourceHostName: "WORKSTATION" SourceIPV4: "-197839XXXX" SourceIPV6:
"0000000000000000000FFFF0A14XXXX" SourceMAC: "null" SourceUserName: "null" SourceProcessName:
"C:\WINDOWS\SYSTEM32\COMPATTELRUNNER.EXE" SourceURL: "null" TargetHostName: "WORKSTATION"
TargetIPV4: "-197839XXXX" TargetIPV6: "0000000000000000000FFFF0A14XXXX" TargetMAC: "null"
TargetUserName: "AUTORIDADE NT\SISTEMA" TargetPort: "null" TargetProtocol: "null"
TargetProcessName: "null" TargetFileName: "C:\Dev-Cpp\Packman.exe" ThreatCategory: "av.detect"
ThreatEventID: "1024" ThreatSeverity: "1" ThreatName: "Generic.dx!qqo" ThreatType: "trojan"
ThreatActionTaken: "IDS_ALERT_ACT_TAK_DEN" …
```

Fonte: Downeast

Casos de Uso

IPS

- Automatização do controle SOX DSS05.07.5_IPS
  Atualização de regras/vacinas
- Envio de logs de bloqueios para posterior correlação
- Problemas com suporte do fabricante

https://medium.com/@forkd/cr%C3%B4nicas-da-opera%C3%A7%C3%A3o-1-a24a9d0a41ad

Fonte: Twitter

<046>2019-08-19T18:41:08Z SFIMS %FTD-6-430001: SrcIP: 10.20.xxx.yyy, DstIP: 10.2.xxx.yyy, SrcPort: 63650, DstPort: 8080, Protocol: tcp, Priority: 1, GID: 1, SID: 27710, Revision: 2, Message: MALWARE-CNC User-Agent known malicious user-agent string IExplore, Classification: A Network Trojan was Detected, User: No Authentication Required, WebApplication: Google, Client: Web browser, ApplicationProtocol: HTTP, ACPolicy: ACP_DC, NAPPolicy: DC_NETWORK, InlineResult: Blocked

Casos de Uso

Proxies

- Usuários
- Auditoria
- URLs e códigos de resposta
- Consumo de banda

```
<38>Jul 31 10:16:37 SERVER.cemig.ad.corp W3C_Syslog: Info: 10.40.xxx.yyy "USER@CEMIG"
https://hangouts.google.com:443/webchat/u/0/host-js 216.58.202.142 1329 "Chat and Instant
Messaging" "Chat and Instant Messaging" TCP_DENIED_SSL/403
BLOCK_WEBCAT_12-Internet_Cemig-DefaultGroup-NONE-NONE-NONE-NONE-NONE "CORP_INTERNET" "Google+"
"Google+ Hangouts/Chat"
```

Fonte: Blogspot

Casos de Uso

Firewalls

- Permissões e bloqueios
- Aplicações de regras
- Auditoria em geral

Missão-crítica

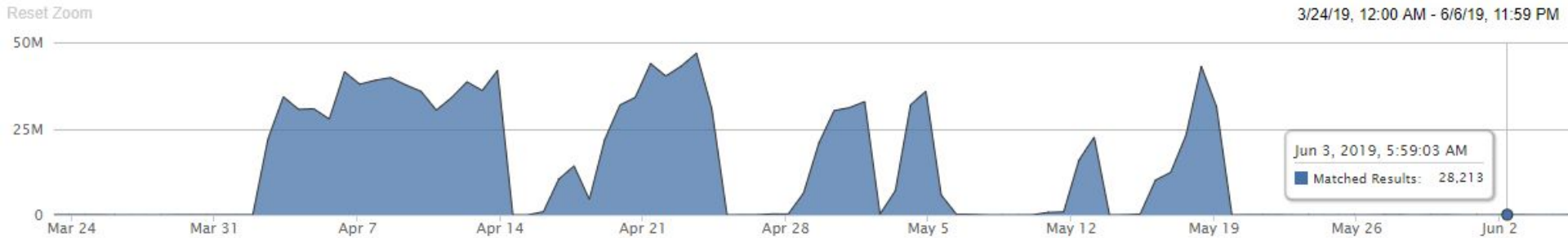
- Regras mais restritivas para operação
- Controle de acessos
- *Commits*

Fonte: Coin Status

Casos de Uso

Firewalls

- Análise de vulnerabilidade
- Falha em aplicação crítica



<14>Aug 13 09:39:48 FW-CEMIG-CORP-01 1,2019/08/13 09:39:48,001701009830,SYSTEM,general,0,2019/08/13 09:39:48,,general,,0,0,general,informational,User jose.lopes logged in via Web from 10.2.xxx.yyy using https,17023830,0x8000000000000000,0,0,0,0,,FW-CEMIG-CORP-01

<14>Aug 13 10:50:42 FW-CEMIG-CORP-01 Path: 2019/08/13 10:50:42 Type:CONFIG Action_type:commit Device:FW-CEMIG-CORP-01 User:pwi_adm\jose.lopes IP_src:10.2.xxx.yyy Client:Web Time:2019/08/13 10:50:42 [Before: After:]

Casos de Uso

Força bruta

- Sistemas de monitoramento mal configurados tentando autenticar em servidores

```
<38>Aug  3 19:19:43 Message forwarded from 10.2.xxx.yyy:
sshd[44368054]: input_userauth_request: invalid user solarusr
[preauth]
```

Fonte: Square Space

5.682 tentativas

Fonte: Chris Slane

Trabalhos Futuros

- Integrações
  Corsair <https://github.com/forkd/corsair>
  SOAR

- Aumentar e melhorar o trabalho com *netflows*

- Melhorar as telas de monitoramento
  Graphite/Graphana

- Aprimorar o ambiente de SIEM

Fonte: Wikimedia

Conclusão

- Mais visão sobre a rede implica em mais atividades proativas
- Cruzamento de dados entre *logs* e *netflows* tende a prover visão privilegiada do ambiente
- É preciso ter critério para tratar os dados recebidos, para realmente gerar informações relevantes

Fonte: Chris Slane

Cyber Security Incident Response Team

abuse@cemig.com.br

José Lopes de Oliveira Júnior

joselopes@cemig.com.br

/jlopesjr

Baixe o artigo

https://www.researchgate.net/publication/334466530_Metodo_para_Uso_do_SIEM_como_Ferramenta_de_Inteligencia_e_Automacao

"Se vi mais longe, foi por estar sobre ombros de gigantes."

– Sir Isaac Newton (1643-1727)