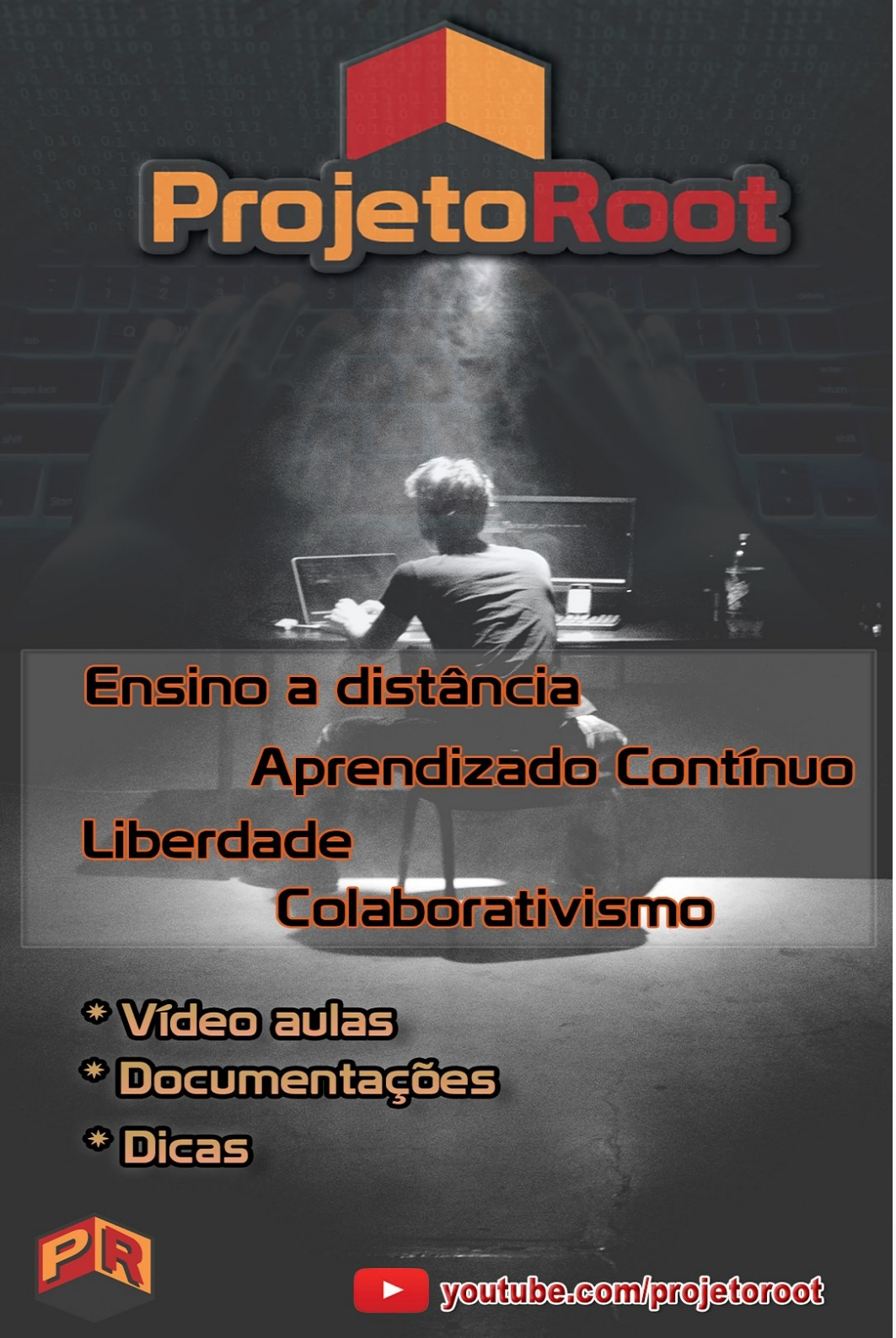


- diegocosta@projetoroot.com.br
- www.projetoroot.com.br
- youtube.com/projetoroot
- facebook.com/projetoroot
- **wiki.projetoroot.com.br**

- Diego Costa

CEO – Projeto Root

- Especialista em Segurança da Informação – Faculdade de Tecnologia SENAC – Porto Alegre - RS
- Tecnólogo em Redes de Computadores – Faculdade de Tecnologia SENAC – Pelotas - RS
- Criador de conteúdos online na área de tecnologia e idealizador do canal no Youtube Projeto Root
- Analista de Segurança da Informação.

Ambientes não monitorados

Monitoramento de Ambientes com OSSEC

- O que são os monitoramentos de ambientes?
- Por que devemos monitorar?
- Qual o impacto que o monitoramento tem na infra?
- Qual o limite deste monitoramento?

OSSEC como alternativa de HIDS

O que é HIDS? Host Intrusion Detection Systems

O que é OSSEC? Open Source HIDS SECurity

Arquiteturas suportadas

i386, X86_64 e ARM (com projetos forks)

Sistemas suportados

Windows, GNU-Linux, Mac

Mas quem criou esse tal de OSSEC?

Daniel B. Cid

https://twitter.com/danielcid

https://www.linkedin.com/in/danielcid/

Lead developer/Founder

OSSEC

jan de 2003 – o momento • 14 anos 11 meses

Lead developer and founder of the open source project OSSEC HIDS (now part of Trend Micro). Description of the project from Wikipedia:

OSSEC is a free, open source host-based intrusion detection system (IDS). It performs log analysis, integrity checking, Windows registry monitoring, rootkit detection, time-based alerting and active response. It provides intrusion detection for most operating systems, including Linux, OpenBSD, FreeBSD, Mac OS X, Solaris and Windows. It has a centralized, cross-platform architecture allowing multiple systems to be easily monitored and managed. It was written by Daniel B. Cid and made public in 2004.

In June 2008 the OSSEC project and all the copyright owned by the project leader, Daniel B. Cid, were acquired by Trend Micro and kept free by them.

Primeiras versões do OSSEC?

Aumentando a segurança do Linux com o OSSEC HIDS

Colaboração: Daniel Cid

Data de Publicação: 24 de Abril de 2006

Essa dica tem o intuito de apresentar o OSSEC HIDS, um sistema open source de detecção de intrusos.

Ele faz analise de logs, checagem de integridade de arquivos, detecção de rootkits, notificação por e-mail e resposta automatica a incidentes (bloqueios no firewall ou no hosts-deny, etc).

Ele já foi testado e roda em Linux, NetBSD, OpenBSD, FreeBSD, Solaris e AIX. Ele é desenvolvido por Brasileiros, mas ultimamente tem recebido apoio de pessoas de todo o mundo.

Uma nova versão acabou de ser lançada e desejo mostrar como instalá-lo bem simplesmente. Essa nova versão pode ser instalada em diferentes linguas (incluindo portugues).

http://www.dicas-l.com.br

Existe apenas OSSEC ?

Wazuh – OpenSource - Fork de OSSEC

(https://wazuh.com/)

AlienVault – Licenciado $$ * Daniel B. Cid (Assessoria Técnica)

(https://www.alienvault.com/products)

TrendMicro – Licenciado $$$ * Daniel B. Cid (Pesquisador)

(https://www.trendmicro.com/en_us/business/products/hybrid-cloud.html)

AlertLogic – Licenciado $$

(https://www.alertlogic.com/solutions/log-correlation-and-analysis/)

Funcionamento

Cliente>Servidor (fluxo)

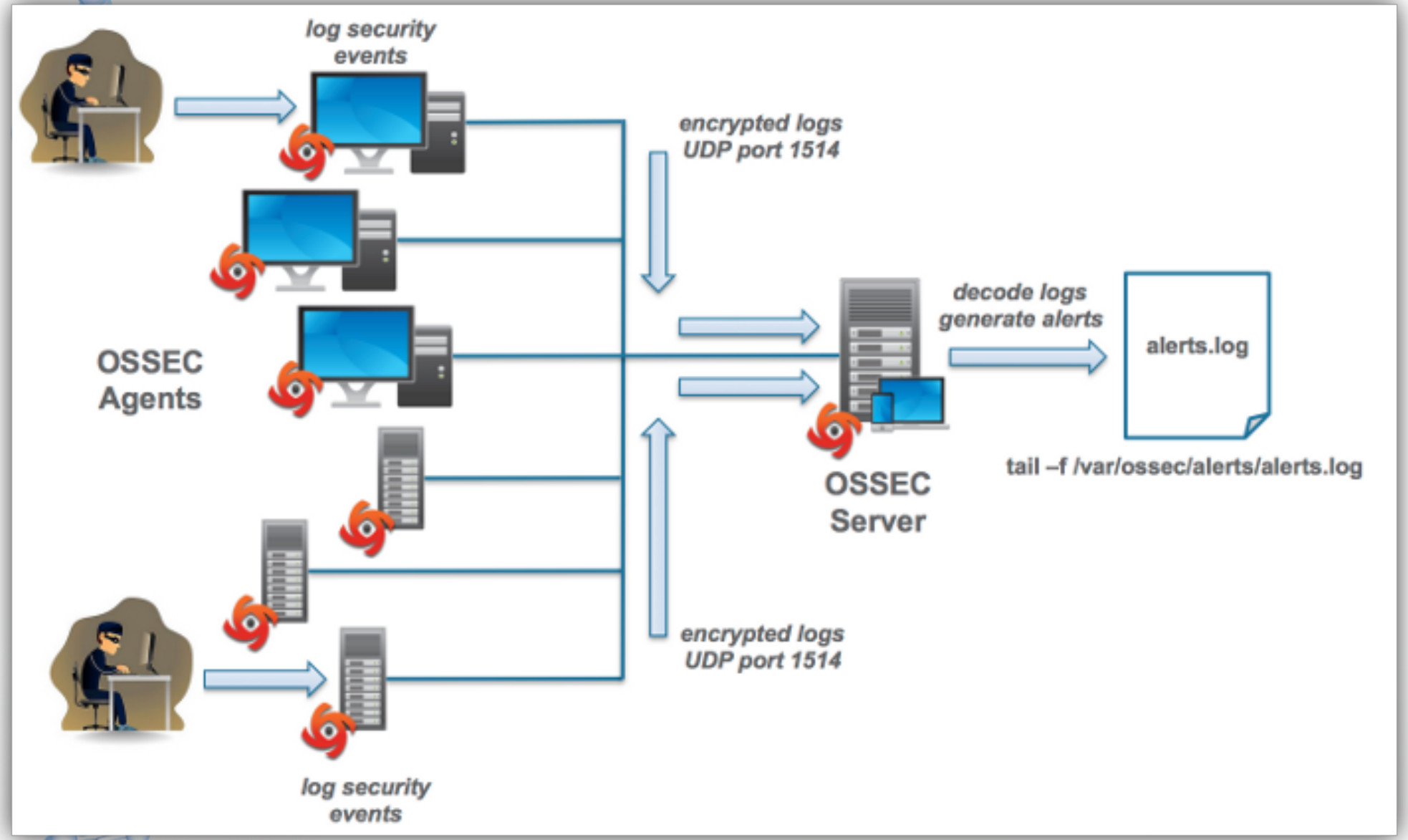
O Agente analisa os logs com base em regras estabelecidas no OSSEC servidor.

O Agente encaminha ao servidor os dados coletados.

Servidor recebe informação de log através da configuração do agente OSSEC (no cliente) e faz a normatização.

Depois de normatizado o servidor toma uma ação (resposta ativa), grava em arquivo de log (pode ser com saída em txt) e/ou envia por e-mail.

Fluxo


log security events
encrypted logs UDP port 1514
OSSEC Agents
decode logs generate alerts
alerts.log
OSSEC Server
tail –f /var/ossec/alerts/alerts.log
encrypted logs UDP port 1514
log security events

O que é coletado?

Log em geral:

Acessos autorizados e não autorizados (ssh,ftp,web,telnet etc…)

Integridade de arquivos (Windows e Linux) * Syscheck

Monitoramento de arquivos ou pastas especificas (/etc/fstab, /home/, c:\Windows, c:\xyz\log.txt) * Syscheck

Instalação ou remoção de softwares (Windows ou Linux) * Syscheck

Registro do Windows * Syscheck

Anomalias no host como Rootkit

Log personalizado (ex: Mikrotik, Roteador XYZ) *Rsyslog

** Resposta Ativa – Bloqueia tentativas de invasões (semelhante ao Fail2Ban)

Como é coletado?

Através de Rules (regras), em formato xml e arquivos de configurações em formato txt e conf, que lidas pelo servidor executam uma série de parametrização, como identificador de processos (id),expressões regulares, descrição de entradas em log, comandos, frequência, entre outras.

No processo de comunicação entre o agente e o servidor existe um processo de compressão (Zlib) e um processo de criptografia (blowfish) em tempo real.

Como OSSEC recebe os Logs

- O log é recebido pelo OSSEC da seguinte forma:

- NOV 19 18:32:04 server1 sshd [1026]: Accept password for root from 192.168.200.1 port 22 ssh2

* Semelhante ao Syslog/Messages

Processo de normatização

- Após recebimento é realizado o Decoding/Normatização

time/date → NOV 19 18:32:04

hostname → server1

program_name → sshd

log → Accept password for root from 192.168.200.1 port 22 ssh2

srcip → 192.168.200.1

user → root

Quando é alertado?

Quando uma entrada de log possuir um match, que é a palavra ou expressão localizada na regra, será lido o valor do nível de criticidade, sendo valores de 0 – 15. Dependendo do nível pré-definido, será tomada a ação, seja apenas guardar a informação em log, alertar por e-mail ou tomar uma ação ativa (ex. Bloqueio no firewall)

00 – Ignorado

15 – Ataque grave

Lista Completa: http://ossec-docs.readthedocs.io/en/latest/manual/rules-decoders/rule-levels.html

Decoder

GNU nano 2.3.1 File: /var/ossec/etc/decoder.xml

```
</decoder>

<decoder name="ssh-closed">
  <parent>sshd</parent>
  <prematch>^Connection closed </prematch>
  <regex offset="after_prematch">^by (\S+)$</regex>
  <order>srcip</order>
</decoder>

<decoder name="ssh-disconnect">
  <parent>sshd</parent>
  <prematch>^Received disconnect </prematch>
  <regex offset="after_prematch">^from (\S+):</regex>
  <order>srcip</order>
</decoder>

<!--XXX
<decoder name="ssh-pam">
  <parent>sshd</parent>
  <prematch>PAM: Module</prematch>
  <regex>for (\S+) from (\S+)$</regex>
  <order>user, srcip</order>
```

XML

```
  GNU nano 2.3.1                File: /var/ossec/rules/vmware_rules.xml

<!-- @(#) $Id: ./etc/rules/vmware_rules.xml, 2011/09/08 dcid Exp $

  -  Official VMWare ESX rules for OSSEC.
  -
  -  Copyright (C) 2009 Trend Micro Inc.
  -  All rights reserved.
  -
  -  This program is a free software; you can redistribute it
  -  and/or modify it under the terms of the GNU General Public
  -  License (version 2) as published by the FSF - Free Software
  -  Foundation.
  -
  -  License details: http://www.ossec.net/en/licensing.html
  -->


<!-- SonicWall Log messages -->
<group name="vmware,">
  <rule id="19100" level="0">
    <decoded_as>vmware</decoded_as>
    <description>VMWare messages grouped.</description>
  </rule>
```

XML

GNU nano 2.3.1 File: /var/ossec/rules/vmware_rules.xml

```
<rule id="19112" level="3">
  <if_sid>19101</if_sid>
  <program_name>vmware-hostd|vmware-authd</program_name>
  <match>Accepted password for|login from</match>
  <description>VMWare ESX user login.</description>
  <group>authentication_success,</group>
</rule>

<rule id="19113" level="3">
  <if_sid>19101</if_sid>
  <program_name>vmware-hostd|vmware-authd</program_name>
  <match>Rejected password for</match>
  <description>VMWare ESX user authentication failure.</description>
  <group>authentication_failed,</group>
</rule>


<!-- Guest OS messages. -->
<rule id="19120" level="8">
  <if_sid>19106</if_sid>
  <match>-> VM_STATE_OFF</match>
  <description>Virtual machine state changed to OFF.</description>
```

- **03 - Sucesso / Eventos autorizados - Incluem tentativas de login bem-sucedidas, eventos permitidos no firewall, etc.**

- **08 - Primeira vez visto - Inclui eventos vistos pela primeira vez , primeira vez que um evento IDS é iniciado ou a primeira vez que um usuário efetuou o login.**

TXT

```
  GNU nano 2.3.1          File: /var/ossec/etc/shared/system_audit_logon.txt

# PermitRootLogin no allowed
# PermitRootLogin indicate if the user root can log in by ssh.
$sshd_file=/etc/ssh/sshd_config;

[SSH Configuration - 1: Root can log in] [any] [1]
f:$sshd_file -> !r:^# && r:PermitRootLogin\.+yes;
f:$sshd_file -> r:^#\s*PermitRootLogin;
```

Conf

```
GNU nano 2.3.1                File: /var/ossec/etc/ossec.conf

<!-- Files to monitor (localfiles) -->

<localfile>
  <log_format>syslog</log_format>
  <location>/var/log/messages</location>
</localfile>

<localfile>
  <log_format>syslog</log_format>
  <location>/var/log/authlog</location>
</localfile>

<localfile>
  <log_format>syslog</log_format>
  <location>/var/log/secure</location>
</localfile>
```

Conf

```
 <log_format>command</log_format>
 <command> yum install </command>
 <frequency>360</frequency>
</localfile>

<localfile>
 <log_format>command</log_format>
 <command> apt-get install </command>
 <frequency>360</frequency>
</localfile>

<localfile>
 <log_format>command</log_format>
 <command> apt-get remove </command>
 <frequency>360</frequency>
</localfile>
```

Estrutura de diretórios

O OSSEC é instalado no diretório /var/ossec/, os principais diretórios são:

/var/ossec/bin/ → Binários do OSSEC

/var/ossec/logs/ → Logs do sistema e de instalação, essencial para Troubleshooting e alertas

/var/ossec/etc/ → Configurações

Daemons

ossec-hids.service

/var/ossec/bin/ossec-analysisd → Analise/normatização
/var/ossec/bin/ossec-syscheckd → Checagem de integridade
/var/ossec/bin/ossec-remoted → Receber registros remotos (logs)
/var/ossec/bin/ossec-logcollector → Leitura de logs
/var/ossec/bin/ossec-agentd → Encaminha logs para o servidor
/var/ossec/bin/ossec-monitord → Monitora os agentes
/var/ossec/bin/ossec-execd → Resposta ativas (bloqueio no fw)
/var/ossec/bin/ossec-maild → E-mail

Gerenciando o OSSEC

Para executar os comandos deve-se estar dentro de /var/ossec/bin/

./ossec-control → inicia, reinicia, para, habilita e desabilita ex. ./ossec-control restart

./agent_control → reinicia com base no ID do cliente (agente) ex. ./agent_control -r 003

./manage_agents → adiciona,remove,lista e extrai keys para agentes ex. ID: 003, Name: Windows_01, IP: 54.215.139.144

Acompanhamento de logs

Para visualizar os logs (Alertas) do ossec, pode-se utilizar o comando tailf ou less no arquivo de alertas como no exemplo:

tailf /var/ossec/logs/alerts/alerts.log

Alertas no shell

```
** Alert 1511129001.174405: mail  - ossec,syscheck,
2017 Nov 19 22:03:21 ip-172-31-5-120->syscheck
Rule: 550 (level 7) -> 'Integrity checksum changed.'
Integrity checksum changed for: '/etc/resolv.conf'
Size changed from '124' to '97'
Old md5sum was: 'a68598e9cf1b5d95d2690843d2189fac'
New md5sum is : '17ab20ec85296d6321284f24d6196301'
Old sha1sum was: '348f968834ad8b2366d20f90c413dfe3b2665bd2'
New sha1sum is : 'c7e726594a726fe6dbadda80005a5f98560793df'
```

Alertas no shell

```
** Alert 1511131472.730834: - windows,win_authentication_failed,
2017 Nov 19 22:44:32 (Windows_01) 54.215.139.144->WinEvtLog
Rule: 18130 (level 5) -> 'Logon Failure - Unknown user or bad password.'
Src IP: 208.94.38.91
User: -
2017 Nov 19 22:44:30 WinEvtLog: Security: AUDIT_FAILURE(4625): Microsoft-Windows-Security-Auditing:
(no user): no domain: EC2AMAZ-JQG91L9: An account failed to log on. Subject:  Security ID:  S-1-0-0
 Account Name:  -  Account Domain:  -  Logon ID:  0x0  Logon Type:   3  Account For Which Logon Fail
ed:  Security ID:  S-1-0-0  Account Name:  administrator  Account Domain:    Failure Information:  F
ailure Reason:  %%2313  Status:   0xc000006d  Sub Status:  0xc000006a  Process Information:  Caller
Process ID: 0x0  Caller Process Name: -  Network Information:  Workstation Name: -  Source Network A
ddress: 208.94.38.91  Source Port:  0  Detailed Authentication Information:  Logon Process:  NtLmSsp
   Authentication Package: NTLM  Transited Services: -  Package Name (NTLM only): -  Key Length:  0
 This event is generated when a logon request fails. It is generated on the computer where access wa
s attempted.
```

Alertas por e-mail

OSSEC Notification - (ISPConfig) 52.53.111.79 - Alert level 7

OSSEC HIDS (19 de Novembro de 2017 12:04)

Para: ossec@projetoroot.com.br

```
OSSEC HIDS Notification.
2017 Nov 19 14:03:40

Received From: (ISPConfig) 52.53.111.79->syscheck
Rule: 553 fired (level 7) -> "File deleted. Unable to retrieve checksum."
Portion of the log(s):

File '/var/www/clients/client1/web1/web/wp-content/updraft/backup_2017-11-18-
1354_Projeto_Root_8357179d98fe-db.gz' was deleted. Unable to retrieve checksum.



 --END OF NOTIFICATION
```

Alertas por e-mail

OSSEC Notification - ip-172-31-5-120 - Alert level 8

OSSEC HIDS (18 de Novembro de 2017 00:30)

Para: ossec@projetoroot.com.br

```
OSSEC HIDS Notification.
2017 Nov 18 02:30:10

Received From: ip-172-31-5-120->/var/log/secure
Rule: 5758 fired (level 8) -> "Maximum authentication attempts exceeded."
Src IP: 103.7.130.114
User: root
Portion of the log(s):

Nov 18 02:30:09 ip-172-31-5-120 sshd[5332]: error: maximum authentication attempts exceeded
for root from 103.7.130.114 port 36710 ssh2 [preauth]



--END OF NOTIFICATION
```

Alertas por e-mail

OSSEC Notification - (Windows_01) 54.215.139.144 - Alert level 10

OSSEC HIDS (19 de Novembro de 2017 20:23)

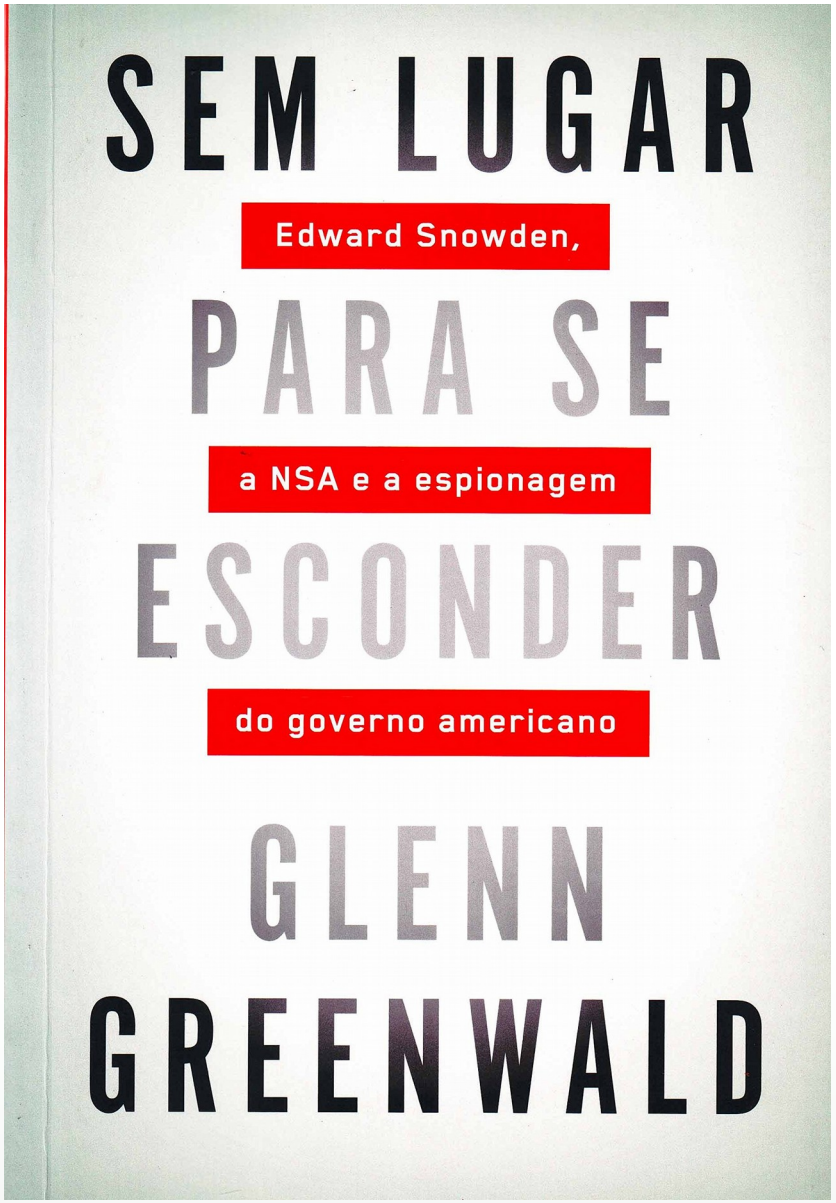
Para: ossec@projetoroot.com.br

```
OSSEC HIDS Notification.
2017 Nov 19 22:22:14

Received From: (Windows_01) 54.215.139.144->WinEvtLog
Rule: 18152 fired (level 10) -> "Multiple Windows Logon Failures."
Src IP: 212.92.120.248
User: -
Portion of the log(s):

2017 Nov 19 22:22:12 WinEvtLog: Security: AUDIT_FAILURE(4625): Microsoft-Windows-Security-
Auditing: (no user): no domain: EC2AMAZ-JQG91L9: An account failed to log on. Subject:
Security ID:  S-1-0-0  Account Name:  -  Account Domain:  -  Logon ID:  0x0  Logon Type:   3
Account For Which Logon Failed:  Security ID:  S-1-0-0  Account Name:  ADMIN  Account Domain:
Failure Information:  Failure Reason:  %%2313  Status:   0xc000006d  Sub Status:  0xc0000064
Process Information:  Caller Process ID: 0x0  Caller Process Name: -  Network Information:
Workstation Name: -  Source Network Address: 212.92.120.248  Source Port:  0  Detailed
Authentication Information:  Logon Process:  NtLmSsp   Authentication Package: NTLM
Transited Services: -  Package Name (NTLM only): -  Key Length:  0  This event is generated
when a logon request fails. It is generated on the computer where access was attempted.
2017 Nov 19 22:22:12 WinEvtLog: Security: AUDIT_FAILURE(4625): Microsoft-Windows-Security-
Auditing: (no user): no domain: EC2AMAZ-JQG91L9: An account failed to log on. Subject:
Security ID:  S-1-0-0  Account Name:  -  Account Domain:  -  Logon ID:  0x0  Logon Type:   3
Account For Which Logon Failed:  Security ID:  S-1-0-0  Account Name:  ADMINISTRATOR  Account
```

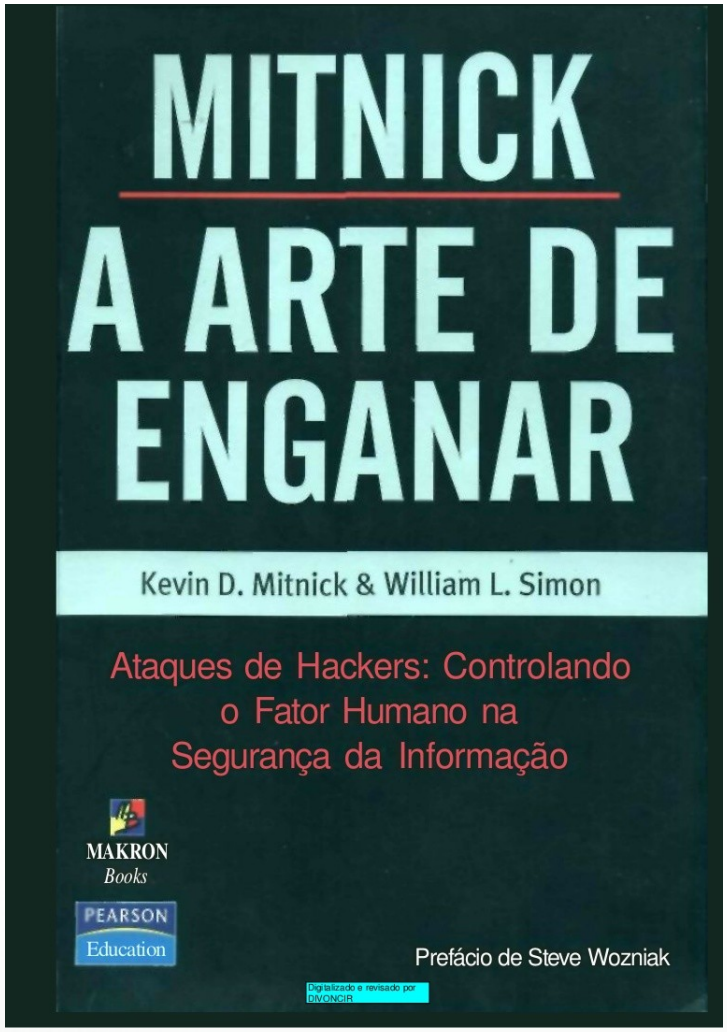
Fontes de pesquisa

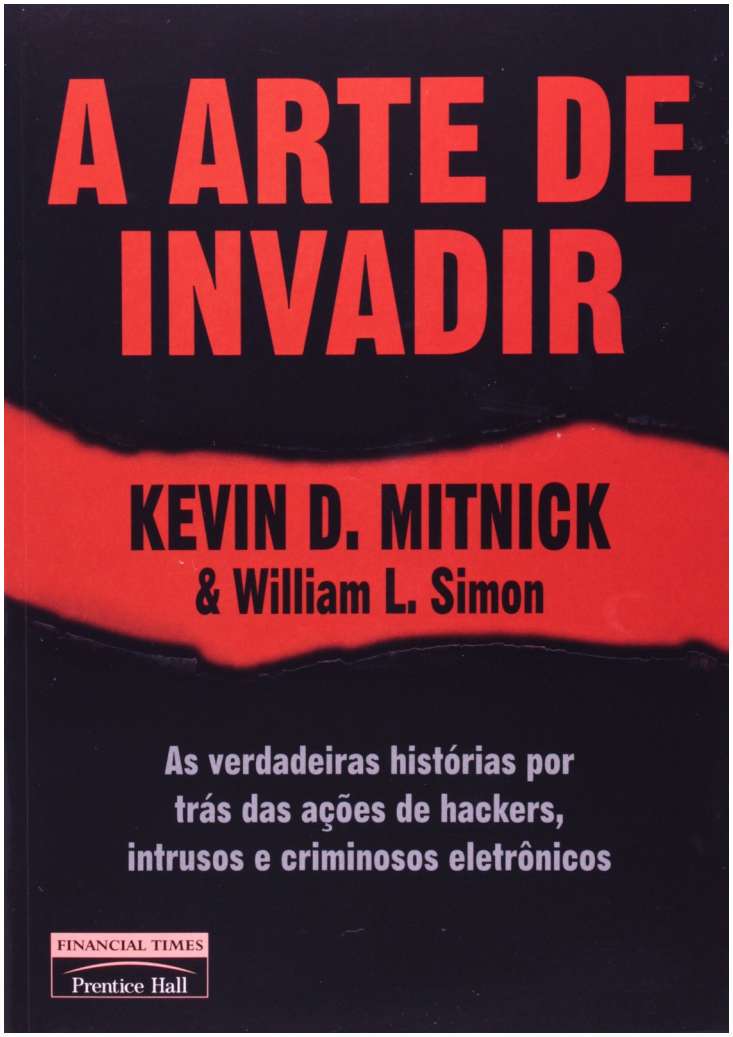
- https://ossec.github.io/ (antigo ossec.net)
- http://ossec-docs.readthedocs.io (documentação e exemplos)
- http://www.dicas-l.com.br (Histórico do ossec)

Indicações - Livros



Indicações - Livros

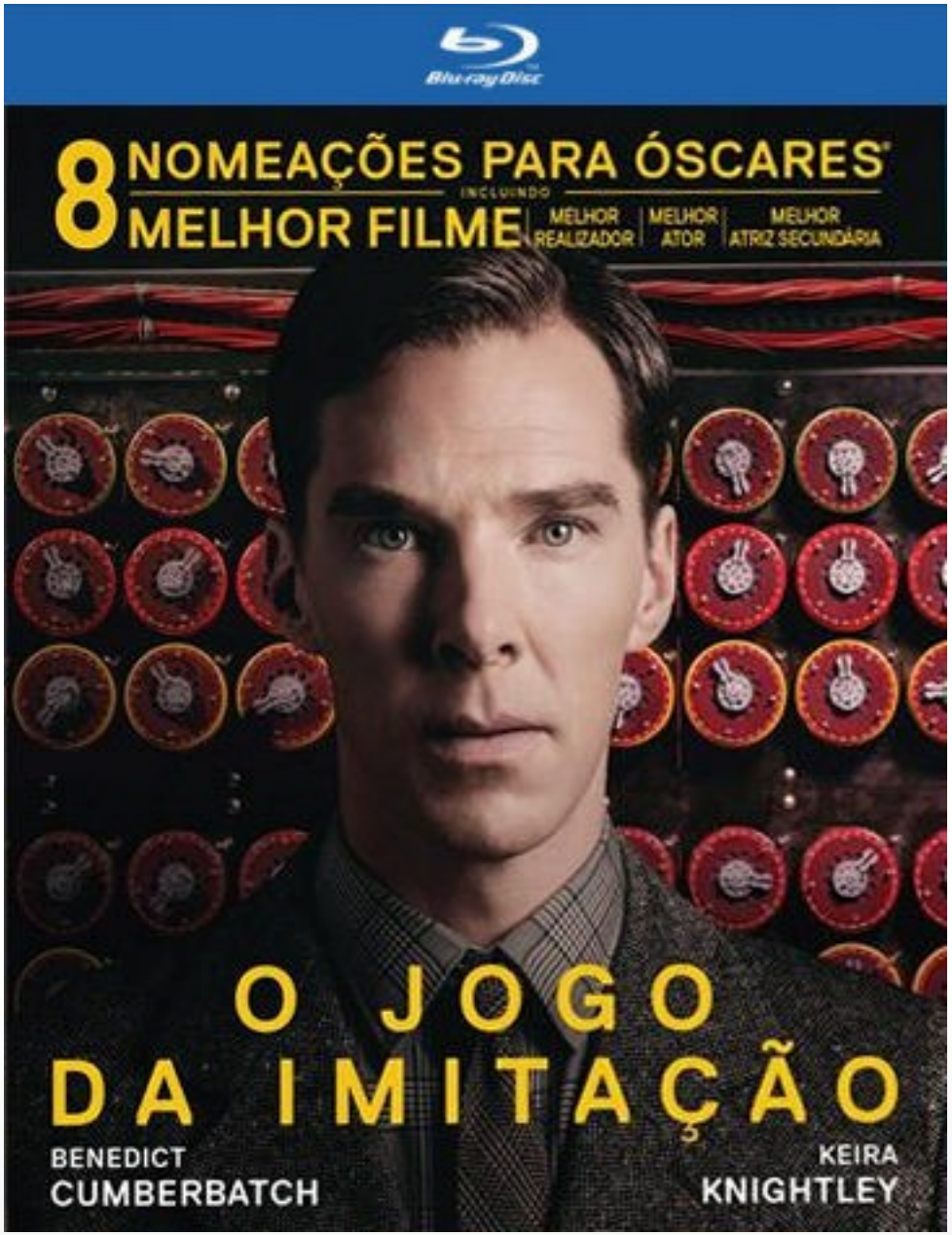




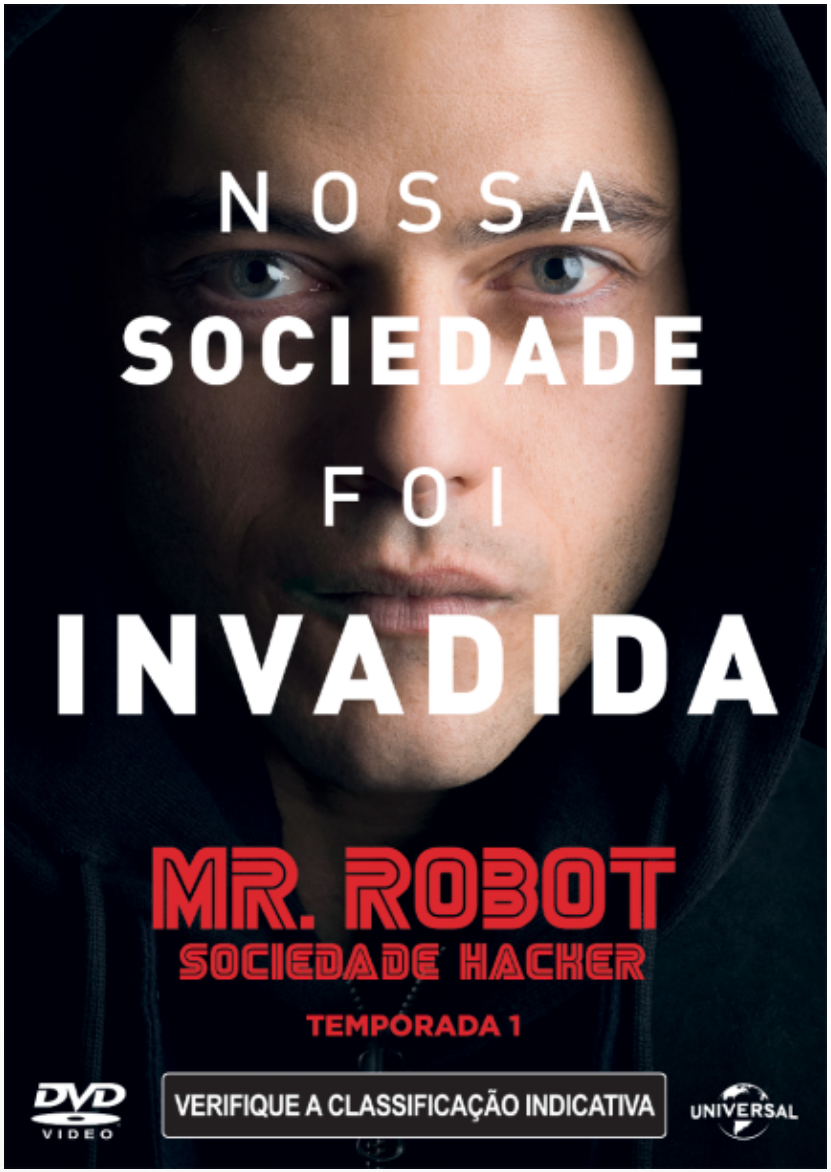
Indicações - PodCast

www.segurancalegal.com

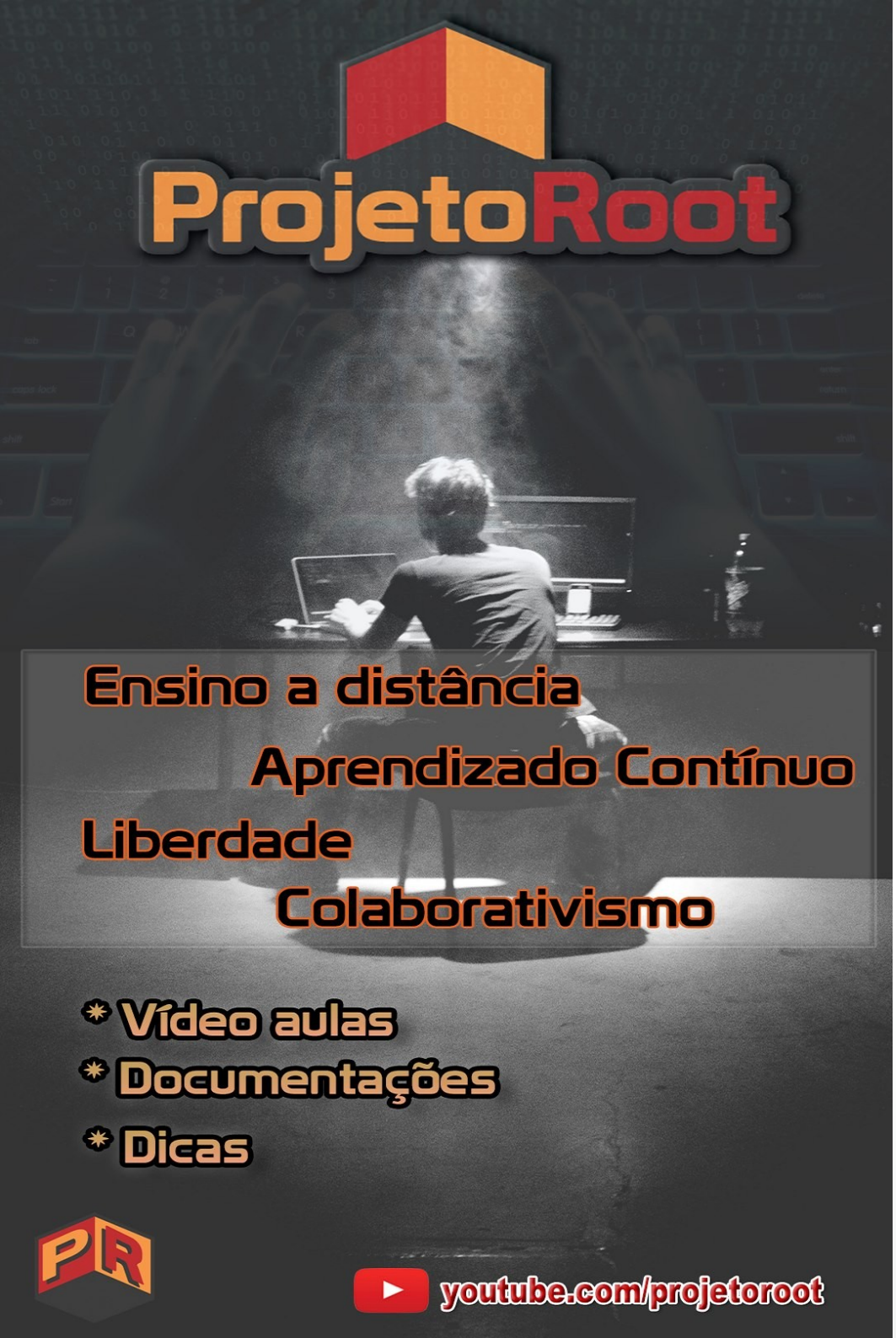
Indicações - Filme



Indicações - Séries



Ossec demo



Perguntas?

- diegocosta@projetoroot.com.br
- www.projetoroot.com.br
- youtube.com/projetoroot
- facebook.com/projetoroot
- **wiki.projetoroot.com.br**

- Diego Costa

CEO – Projeto Root