OSSEC Con 2020

Leadership

Dan Cid (Founder)

- Sucuri / Godaddy

Scott Shinn (Current Project Lead) : OSSEC Foundation

- Joined in 2006
- Project Leader in 2014
- CTO Atomicorp

Dan Parriot : OSSEC Foundation

- Joined in 2006
- Reluctant Developer

Domink Lisiak: Community

- Joined in 2016
- FreeBSD lead

OSSEC

"For me, OSSEC is a project that sits at the intersection of maturity + impact"

 @kwm

Project At a Glance

- First released in 2005 by Daniel Cid
- Started in 2003
- Its short for Open Source Security
- Acquired by Third Brigade in 2008, and Trend Microsystems in 2009
- Millions of installs, on every continent

- Supports:




any many more

What is OSSEC

LIDS – Log Intrusion Detection System

FIM – File Integrity Monitor

Audit – Compliance (PCI-DSS, GDPR, NIST-800-53, etc)

Malware Detection

Active Response & Self Healing

Supported Projects

OSSEC Foundation

- 503c Non-Profit managing the OSSEC project
- Conference
- Support for security researchers, developers, and organizations
- Open Source Software certification, Approved Product Lists, code audit (this deserves it's own slide!)
- Support open source and commercial with domain experts
- Coordinate with other 503c, Sponsors and Grant programs

OSSEC Foundation Plans in 2020-2021

- Shamelessly accept your tax deductible donations!
- Continue our work with grant programs sponsoring information security researchers (TAP, and others)
- Dedicated community developer(s) and internships
- Expand our educational initiative with UVA and other universities
- Support other open source security projects
- Expand our commercial/community/government partnerships
- More training sessions

What's New in OSSEC

What's New in OSSEC

- Current release 3.6.0
- Hundreds of community developers (no commit is too small!)
- Post-Graduate researchers joining the community
- IBM Power Z-Series Redhat PPC and AIX
- ARM CPU support for Centos/Redhat, and Ubuntu
- Security Audit by Daniel McCarney
- Multi-line log analysis update (multiline_indented) by Boris Lukashev
- PCRE2 IDS engine updates (@jubois) completed

What's New in OSSEC

- Dept of Defense Enterprise DevSecOps (DSOP)
- Azure Marketplace
- Google Marketplace
- IBM / Redhat Container marketplace

OSSEC New Architectures: ARM64

- Yui Naruse (@nurse) of Treasure Data Inc. (www.treasuredata.com)
- AWS Graviton Processor (A1, etc)
- Builds available for Redhat/Centos 8 and Ubuntu 18
- Build automation using the aarch64 module for KVM
- Planning phase for Android on ELO touch point of sale systems

OSSEC New Architectures: IBM i-Series

- Virtual environments for builds, and testing
- Power 8 and Power 9 architectures
- AIX
- Redhat 7 and 8 PowerPC
- Ubuntu 16 and 18
- IBM IOS5

But… we cannot automate pipelines….

OSSEC on Github

Source:

https://github.com/ossec/ossec-hids/

Documentation:

https://github.com/ossec/ossec-docs/

New Repos and Distros

- Amazon / Amazon LTS
- CentOS / RHEL / Clones 6/7/8
- Debian 8/9/10
- Kali
- Mint
- Ubuntu 14/16/18
- Windows
- Architectures: x86_64, aarch64, ppc

Docker Repos

https://hub.docker.com/r/atomicorp/ossec-docker/

Docker pull atomicorp/ossec-docker

docker run -d -p 1514:1514/udp -p 1515:1515/tcp -v ossec-data:/var/ossec/data --name ossec-server atomicorp/ossec-docker

OSSEC Con 2020: Day 2

Provided by Hyperqube.io, a virtual OSSEC environment accessible via web browser.
Will continue to be available until July 8

- Session 1: New to OSSEC, how to build/compile ossec servers, agents, and windows.
- Session 2: Installation automation on windows/linux and clouds
- Session 3: Centralized management, Compliance testing, Active Response, and Realtime FIM

OSSEC 2020

- Open to individuals and organizations
- We’re on Slack! ossec.slack.com
- Not just for coders! Tech writer? Student? Researcher?

Questions?

Scott Shinn (@atomicrocketturtle)
scott@ossec.net

OSSEC Con 2020 Workshop

Download links

git clone https://github.com/Atomicorp/training

Contains the all the examples used here for this workshop:

/root/src/training/workshop2020/

Under /root/src/training/ on the Hyperqube virtual machines

OSSEC 2020 Workshops

- New to OSSEC: compile and installation
- Installation automation with Active Directory
- Advanced Topics: Troubleshooting, Rootcheck, AR, and more

OSSEC 2020 Workshops

- New to OSSEC: compile and installation
- Installation automation with Active Directory
- Advanced Topics: Troubleshooting, Rootcheck, AR, and more

OSSEC Workshop: Brought by Hyperqube.io

Hyperqube is a network design studio

- Build entire networks
- Fully interactive systems
- Cloned for each user
- Only requires a web browser (Chrome or Firefox!)

OSSEC Workshop 1 : Installation

- Server builds, and common issue troubleshooting
- Agent builds, and saving settings for binary installation
- Windows builds and getting around outside of install.sh

OSSEC Workshop 1: Build a Server

- Server builds, and common issue troubleshooting
- You will need:
  - Centos 7
  - Development Tools
  - Basic linux navigation

Open Hyperqube Environment:

OSSEC: Installation

Login: hyperqube / Hyperqube1!

OSSEC Workshop 1: Building the Server

- Dependencies (Redhat/Centos)
  - pcre2-devel
  - libevent-devel
  - openssl-devel
- install.sh, and what it does/does not do

  ./install.sh

  /var/ossec/bin/ossec-control start

OSSEC Workshop 1: Server Components

- ossec-analysisd : IDS analysis (rules/decoders)
- ossec-remoted : Listener for agent traffic
- ossec-syscheckd : FIM daemon
- ossec-logcollectord : Log collector daemon
- ossec-execd : Active Response daemon
- ossec-monitord : Logrotation, cleanup, and reporting daemon
- ossec-maild : Mail User Agent daemon
- ossec-dbd : Database Connector daemon
- ossec-authd: Agent registration daemon

OSSEC Workshop 1: Server Components

Troubleshooting:

Startup logs here:
/var/ossec/log/ossec.log

Typos? Invalid configs? run this:
/var/ossec/bin/ossec-analysisd -t

OSSEC Workshop 1: Building the windows agent

- Dependencies: Docker
- Windows binaries are built from linux

```
cd /root/src
docker run -it -v /root/src:/root/src ossec-windows-builder /bin/bash
cd /root/src/ossec-hids-3.6.0/src/
make clean
make TARGET=winagent external PCRE2_SYSTEM=no
make TARGET=winagent PCRE2_SYSTEM=no
```

output: win32/ossec-agent.exe

OSSEC Workshop 1: Advanced Settings

- We’re still in src/ !
- No install.sh here!

make help

make TARGET=server

make clean

make TARGET=server DATABASE=mysql MAXAGENTS=8192

OSSEC Workshop 1: Advanced Settings

- Putting this together with install.sh

```
cd src/ && make clean
cd ..
DATABASE=mysql MAXAGENTS=8192 ./install.sh
```

OSSEC Workshop 1: Repeatable Agent Builds

- Dependencies (Redhat/Centos)
- install.sh tips and tricks for repeatable builds

cd src/ && make clean
cp etc/preloaded-vars.conf.example etc/preloaded-vars.conf
edit etc/preloaded-vars.conf and set:
    USER_BINARYINSTALL=”y”
cd src/ && make TARGET=agent
copy this directory to target
./install.sh

OSSEC Workshop 1: Breaking it!

- Common Build Problems

rpm -e pcre2-devel
cd /root/src/ossec-hids-3.6.0/src
make clean
make TARGET=server

fatal error: pcre2.h: No such file or directory

OSSEC Workshop 1: Breaking it!

Finding the file with yum (note: we are offline!)

yum provides */pcre2.h

normally: yum install pcre2-devel
but we're offline!
rpm -Uvh /root/src/dependencies/pcre2-devel*rpm

make TARGET=server

OSSEC Workshop 1: Questions

Scott Shinn (@atomicrocketturtle)
scott@ossec.net

OSSEC Workshop 2: Installation Automation

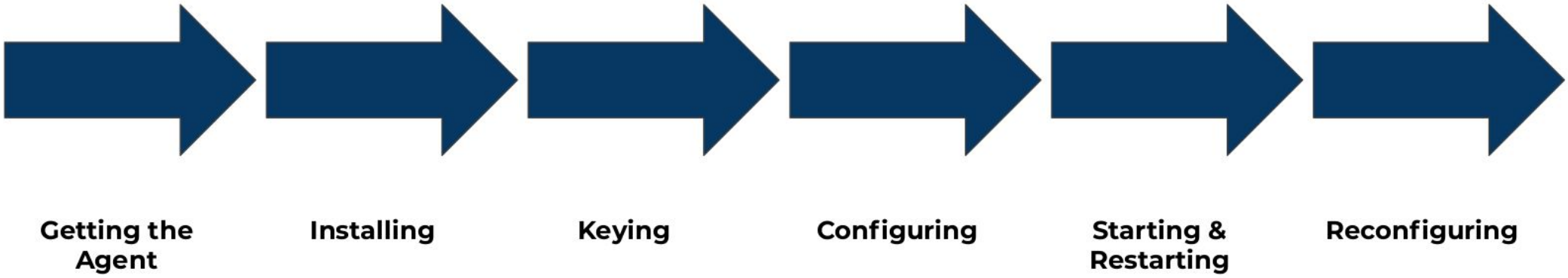
- Windows using Active Directory, Powershell, and reboots
- You will need:
  - Active Directory server (win2016)
  - Windows 10 agent
  - Powershell
  - OSSEC Server
  - Webserver

Open Hyperqube environment:

OSSEC 1

OSSEC Workshop 2: Installation Automation

Challenges in Automating OSSEC Deployment



OSSEC Workshop 2: Installation Automation

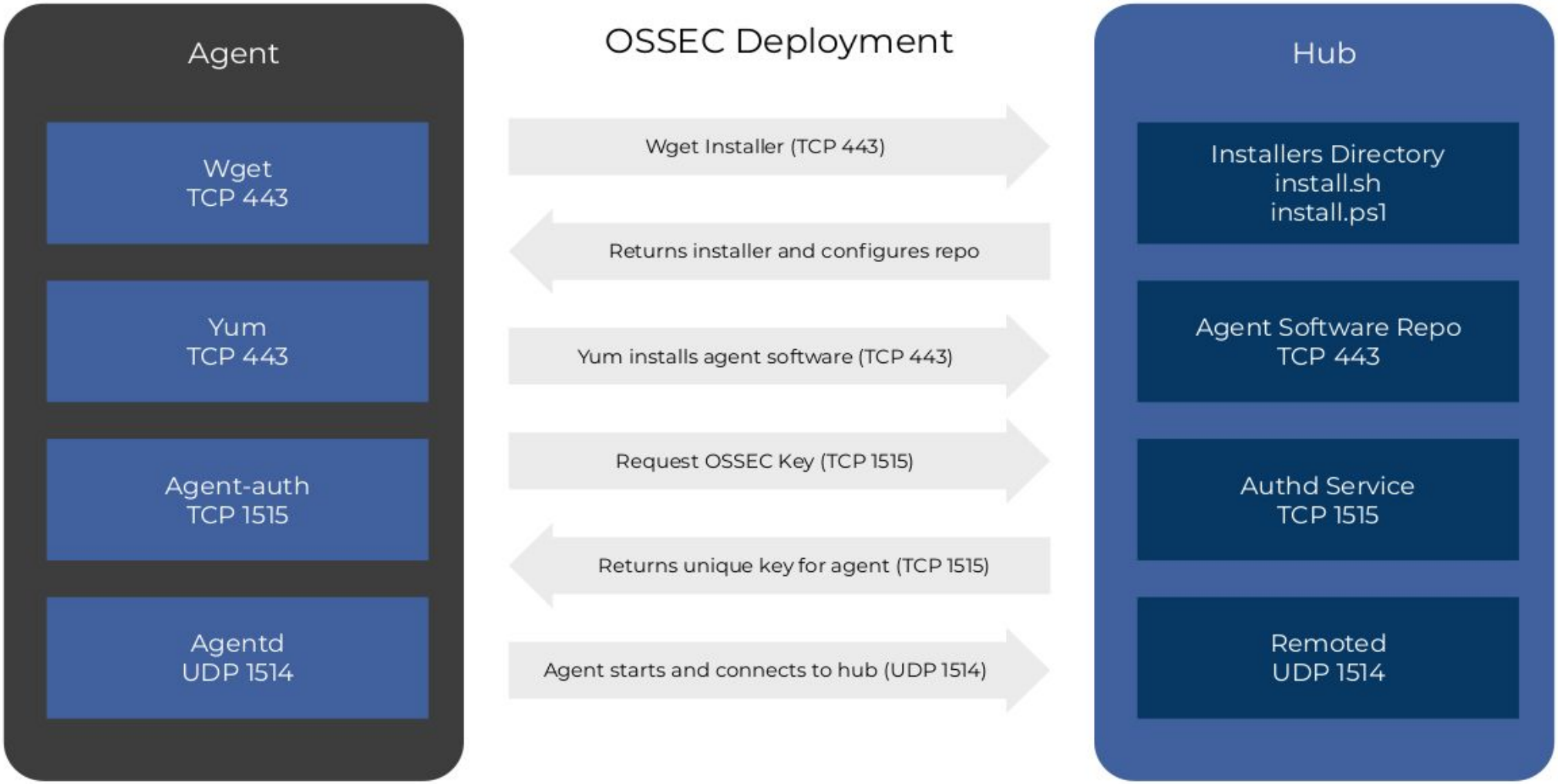
Automating OSSEC Deployment

The manual way you are used to:

Log into server
run manage_agents on the server,
copy key
Log into agent
run manage_agent on the agent
paste key
Repeat until done

Difficult at Scale and
in Dynamic Environments

OSSEC Workshop 2: Installation Automation



OSSEC Workshop 2: Using a GPO

- This installs when the Windows 10 system reboots
- Active Directory GPO configures the system to
  - Copy the powershell installer to the system from share
  - Run the installer as SYSTEM
  - Pass variables to the powershell script for the server IP
- Gotchas:
  - Package signing can break installs over shares
  - Firewalls can break registration
  - Permissions!

OSSEC Workshop 2: Using a GPO

- Example uses powershell, this is probably overkill
- This can be used for
  - new installs
  - upgrades
  - re-keying

OSSEC Workshop 2: Using a GPO Workflow

- Installs and configures the agent on a host reboot
- Runs 1 time
- copies installer.ps1 from C:\networkShared to the system
- Agent runs installer.ps1 locally as SYSTEM user**
- Downloads software to C:\ossec-agent-latest.exe
- Installs application
- Registers the agent with the hub server
- Configures ossec.conf and starts the agent on the host

**you can change this to a domain admin, etc

OSSEC Workshop 2: Using a GPO Step 1

Server manager select Tools

Group Policy Management

Select domain: atomicorp.local

Right click on the domain, create GPO and Link it here

name this: install1

Right click on install1 and select Edit

OSSEC Workshop 2: Using a GPO Step 1

Select Computer Configuration

- Preferences
  - Windows Settings
    - Files

Select New->Files

- set the Action to Create
  - set path to source file : \\Ad-server\sysvol\atomicorp.local\installer.ps1
  - set path to destination on host: C:\installer.ps1
- click OK

OSSEC Workshop 2: Using a GPO Step 2

Select Computer Configuration

Preferences

Control Panel Settings

Scheduled Tasks

Right click and select New->Immediate Scheduled Task (At least windows 7)

Enter name: install-agent

Enter description: OSSEC agent

Select when running task use the following user account: SYSTEM

OSSEC Workshop 2: Using a GPO Step 2 cont.

Select run whether user is logged on or not

Select Run with highest privileges

Select configure for Windows 7, windows server 2008R2

OSSEC Workshop 2: Using a GPO Step 3

Select action tab, and click New
Enter in program/Script: powershell.exe
Enter in Add arguments:

-executionpolicy bypass -file C:\installer.ps1 -ossec_exe http://192.168.1.102/ossec-agent-latest.exe -server_ip 192.168.1.102

Click OK, select the Common tab, and check Apply once and do not reapply. Click OK

OSSEC Workshop 2: Using a GPO Step 4

Log in to the OSSEC server, and run:
tail -f /var/log/httpd/*

Log in to the Windows 10 system, and reboot.

You should see the windows 10 system request the ossec package, and in a few minutes complete the installation

OSSEC Workshop 2: Troubleshooting

Can the new agent read the share drive?

check the win10 system if it copied C:\install1.ps1

Did the GPO run?

from the win10 system, run: gpresult /r

Did the agent register?

from the ossec server, run /var/ossec/bin/agent_control -l

OSSEC Workshop 2: Reset Windows 10

(Optional) To repeat the previous scenario

Log in to windows 10 as: Hyperqube / Hyperqube1!
Add / Remove Programs, Remove ossec hids 3.6.0
(as administrator) Remove C:\installer.ps1
(as administrator) Remove C:\ossec-agent.exe

Change your GPO to run again on boot

OSSEC Workshop 2: Questions

Scott Shinn (@atomicrocketturtle)
scott@ossec.net

OSSEC Workshop 2: Bonus Round Cloud-Init

The Problem:

- Dynamic scaling on Amazon (Google, Azure, etc)
- OSSEC agent keys have to be unique

Solution:

- Cloud-init

OSSEC Workshop 2: Bonus Round Cloud-Init

Launched in 2008: https://cloud-init.io

Supports more than 20 public cloud providers

Openstack, LXD, KVM, etc

Adds an “init” type API to the operating system for:

- first-boot: First time the system has ever booted
- per-boot: Every time the system boots
- per-instance: First time a cloned (dynamic scaling) instance boots

OSSEC Workshop 2: Bonus Round Cloud-Init

Launched in 2008: https://cloud-init.io

Supports more than 20 public cloud providers

Openstack, LXD, KVM, etc

Adds an “init” type API to the operating system for:

- per-once: First time the system has ever booted
- per-boot: Every time the system boots
- per-instance: First time a cloned (dynamic scaling) instance boots

Available for: Ubuntu, Debian, Redhat, Centos, *BSD, and more

OSSEC Workshop 2: Bonus Round Cloud-Init

Our action is simple, just rekey the agent:

/var/ossec/bin/agent_auth -m 10.10.10.10

But we need to do this immediately without requiring a human or external devops action.

OSSEC Workshop 2: Bonus Round Cloud-Init

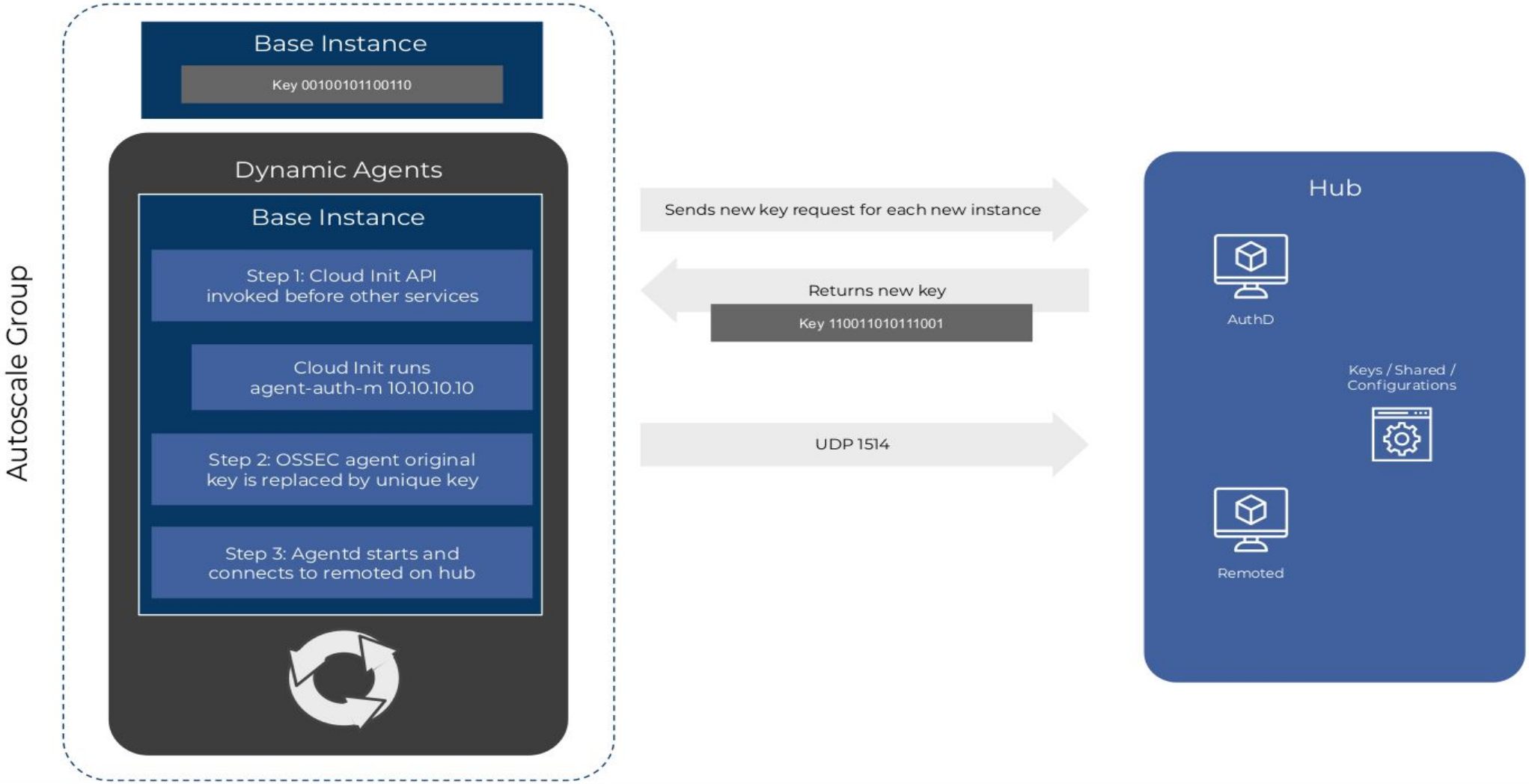
What about rc.local?

It would work, however it rc.local happens after the regular ossec-agent daemon starts

It could result in creating even more keys, given that the rc.local is set at the master instance level.

We need something smarter

OSSEC Workshop 2: Bonus Round Cloud-Init



OSSEC Workshop 2: Bonus Round Cloud-Init

It’s this easy:

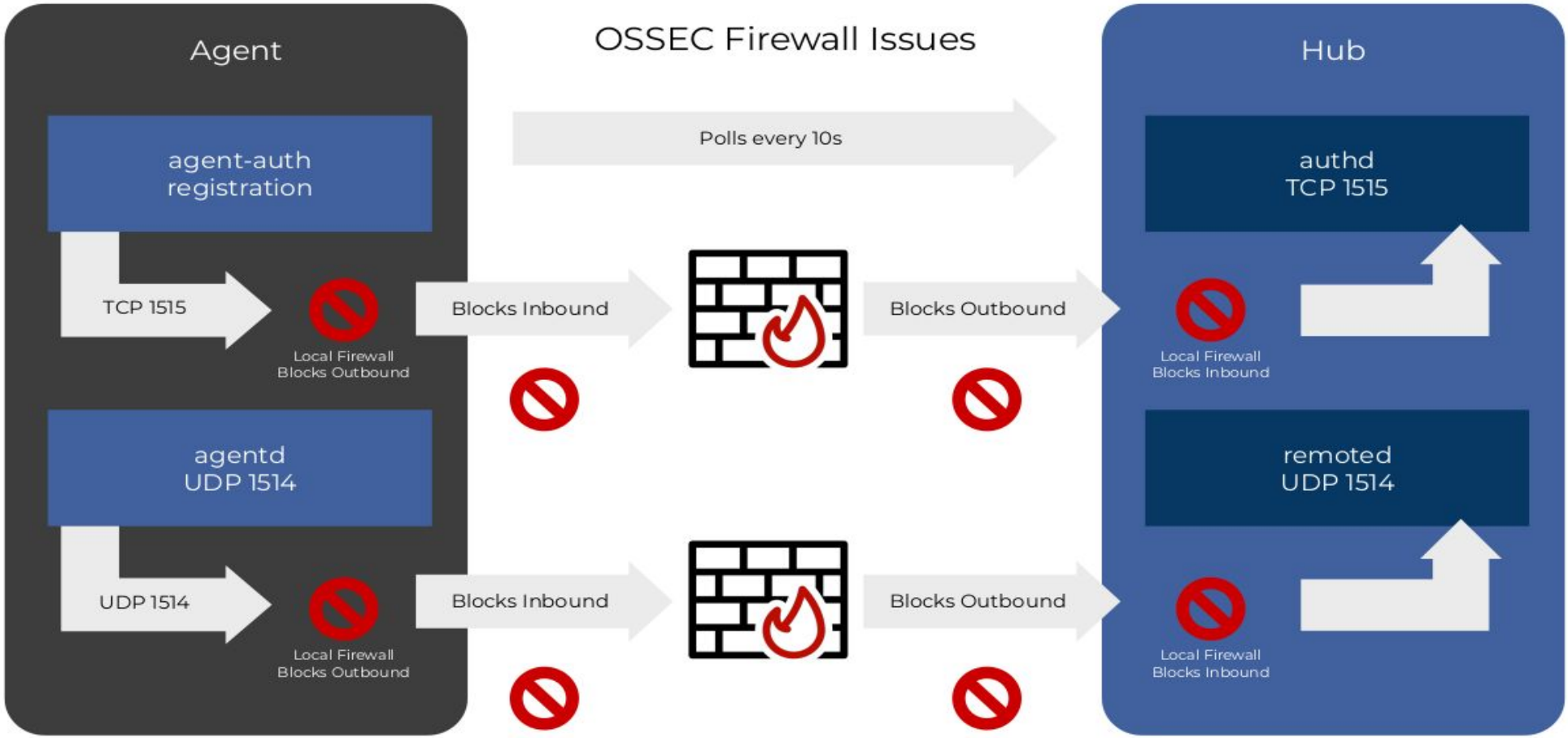
cat /var/lib/cloud/scripts/per-instance/ossec-agent.sh

```
#!/bin/sh
/var/ossec/bin/agent-auth -m 10.10.10.10
```

OSSEC Workshop 3: Advanced Topics

- Network Troubleshooting
- Central Management with shared/
- Rootcheck: Malware detection, Compliance Testing, Application discovery
- Malware / FIM whitelisting (filename)

OSSEC Workshop 3: Network Troubleshooting



OSSEC Workshop 3: Network troubleshooting

Scenario 1, agent_control reports “Never Connected”

This indicates the TCP Port 1515 (authd) registration completed successfully, but the agent communication is blocked

Check the agent to ensure the server ip is correct and the agent is started

Use a sniffer on the Server to watch for UDP 1514 traffic from the host: tshark -i eth0 port 1514

No traffic means a firewall is blocking UDP 1514 at some point

OSSEC Workshop 3: Network troubleshooting

Scenario 2, agent_control reports “Disconnected”

This indicates the UDP Port 1514 had worked in the past, but the agent communication is blocked

Run: /var/ossec/bin/agent_control -i <ID> to see when the agent last checked in successfully

Is the agent running?

Is the Server IP correct?

Is a firewall blocking UDP 1514?

Is its key good?

OSSEC Workshop 3: Network troubleshooting

agent_control cheatsheet

“Never Connected” - This means agent registered (TCP 1515) but has never connected over remoted (UDP 1514)
“Disconnected” - Agent registered (TCP 1515) and had previously connected over remoted (UDP 1514) but is no longer online
“Active” - Everything is fine!
“Pending” - a transitional state, the agent is in the process of connecting. This is only an issue if it takes a long period of time

OSSEC Workshop: Active Response

- Block source addresses (srcip)
- Disable Accounts (username)
- Malware / FIM whitelisting (filename)
- Self-healing (pin to a rule)
- Reporting (JIRA, slack, etc)
- PaaS API (cloudflare, aws, etc)
- IFTTT
- Amazon Echo / Google Home
- etc!

OSSEC Workshop: Active Response

- ossec-execd runs active response (ossec-agent on windows)
  - Commands live in: /var/ossec/active-response/bin/
  - This daemon forks! Beware! Job control is up to you!
  - Context:
    - srcip
    - username
    - filename
    - or no context at all

OSSEC Workshop: Active Response

- Can run on:
  - where the attack happened
  - a specific system
  - every system
- Configured from the server, but the action has to be on the agent (except… repeated_offenders...)
- ARs can be in any language (Powershell, bash, python, go, etc)
- Timed, Repeat offenders, or no timer
- Active response can be configured in TWO places
  - /var/ossec/etc/ossec.conf or in a rule

OSSEC Workshop: Active Response Values

- Action (add or delete)
- Username (ex: testguy)
- IP address (ex: 1.2.3.4)
- Alert ID (ex: 1552939106.13039)
- Rule ID (ex: 553)
- Agent (ex: (testagent1.atomicorp.com))
- Location (ex: 10.10.10.10->syscheck)
- Filename (ex: /mnt/test1)

OSSEC Workshop: Active Response

- In a ossec.conf

```
<command>
   <name>syscheck-api</name>
   <executable>syscheck-api</executable>
   <expect>filename</expect>
</command>

<active-response>
   <command>syscheck-api</command>
   <location>server</location>
   <level>5</level>
   <rules_group>syscheck</rules_group>
</active-response>
```

OSSEC Workshop: Active Response

- In a rule:
  - <action> to declare the name of the script
  - <status> to pass the add or delete value

```
<rule id="601" level="3">
   <if_sid>600</if_sid>
   <action>firewall-drop.sh</action>
   <status>add</status>
   <description>Host Blocked by firewall-drop.sh Active Response</description>
 <group>active_response,</group>
 </rule>
```

OSSEC Workshop: Active Response Utils

- List: /var/ossec/bin/agent_control -L
  Response name: test-all0, command: test-all.sh
  Note: 0 indicates the timer, if set. Not set in this example

- Run manually (I use this for testing) Example:

  /var/ossec/bin/agent_control -b 1.2.3.4 -f test-all0 -u 000

OSSEC Workshop: Active Response Utils

Debugging Tip: syscheck wont start generating events until rootcheck finishes its job. Rootcheck can take a while, so turn it off for development

Debugging Tip: Not clear if syscheck is running? Tail ossec.log and look for “Ending syscheck scan”. After this, perform your tests

OSSEC Workshop: Active Response FILENAME

- Simulation and Testing configuration
- Syscheck can take a long time to run, for this workshop we will set the following to speed things up:
  - <directories realtime="yes" check_all="yes" report_changes="yes">/mnt</directories>
  - disable rootcheck
  - internal_options.conf
    - syscheck.sleep=1
    - syscheck.sleep_after=150

OSSEC Workshop: Active Response FILENAME

```
cd /root/src/workshop2020/lab03/active-response
/var/ossec/bin/ossec-control stop
cp ossec.conf /var/ossec/etc/
cp internal_options.conf /var/ossec/etc/
cp syscheck-api.sh /var/ossec/active-response/bin/
/var/ossec/bin/ossec-control start
```

OSSEC Workshop: Active Response FILENAME

- perform actions against FIM events
- active response configuration key values:
  - <expect>filename</expect>
  - <rules_group>syscheck</rules_group>

This example only logs the script being run. Restart OSSEC and Create a test file:

date >> /mnt/testfile1

OSSEC Workshop: Active Response FILENAME

- Update /mnt/testfile1:

  date >> /mnt/testfile1

Generates 552 event, and logs:

Tue Mar 10 09:04:59 EDT 2019

/var/ossec/active-response/bin/syscheck_all.sh add - -

1553000699.9105 552 field6(syscheck) Filename: (/mnt/hosts)

field8() field9() field10(add0)

OSSEC Workshop: Dynamic Decoders

- Dynamic fields are declared in the decoder
- Output is formatted in /var/ossec/logs/alerts/alerts.json

Example input from a Shimadzu mobile radiographic imager:

"1/1/2014","01:26:48","78-XR-14-000045","Rad","CHEST AP X-WISE","CHEST","L\F","AP","deleom","","","","","","","0.031","","319.66767857507","141.926534243403","-1","-10000","90","160","6","0.96","","18000959"

OSSEC Workshop: Dynamic Decoders

```
cd /root/src/training/workshop2020/lab03/dynamic-decoders/
cp *conf /var/ossec/etc/
cp decoder.xml /var/ossec/etc/
/var/ossec/bin/ossec-control restart
```

OSSEC Workshop: Dynamic Decoders

JSON output:

{"rule":{"level":7,"comment":"Shimadzu Exam Log","sidid":91000,"firedtimes":1,"groups":["shimadzu"]},"id":"1553009395.27394","TimeStamp":1553009395000,"decoder":"shimadzu-exam-log1","decoder_parent":"shimadzu-exam-log1","location":"/var/log/messages","full_log":"\"1/1/2014\",\"01:26:48\",\"78-XR-14-000045\",\"Rad\",\"CHEST AP X-WISE\",\"CHEST\",\"L\\F\",\"AP\",\"deleom\",\"\",\"\",\"\",\"\",\"\",\"\",\"\",\"0.031\",\"\",\"319.66767857507\",\"141.926534243403\",\"-1\",\"-10000\",\"90\",\"160\",\"6\",\"0.96\",\"\",\"18000959\"","hostname":"c7-64-dev-ossec-community","shimadzu.exam.protocol":"Rad","shimadzu.exam.bodypart":"CHEST AP X-WISE","shimadzu.exam.operator":"deleom","shimadzu.exam.dap":"\"\"","shimadzu.exam.absorbeddose":"0.031","shimadzu.exam.ei":"141.926534243403","shimadzu.exam.eit":"-1","shimadzu.exam.di":"-10000","shimadzu.exam.kv":"90","shimadzu.exam.ma":"160","shimadzu.exam.ms":"6","shimadzu.exam.mas":"0.96","shimadzu.exam.sid":"\"\"","shimadzu.exam.sensorsn":"\"18000959\"","decoder":{"parent":"shimadzu-exam-log1","name":"shimadzu-exam-log1"},"hostname":"c7-64-dev-ossec-community","timestamp":"2019 Mar 19 11:29:55","location":"/var/log/messages"}

OSSEC Workshop: Dynamic Decoders

```
<decoder name="shimadzu-exam-log2">
    <parent>shimadzu-exam-log1</parent>

<regex>^\S+,\S+,\S+,"(\S+)","(\.+)",\S+,\S+,\S+,"(\S+)",\S+,\S+,\S+,\S+,(\S+),"(\S+)",\S+,\S+,"(\S+)
","(\S+)","(\S+)","(\S+)","(\S+)","(\S+)","(\S+)",(\S+),(\.+)</regex>

<order>shimadzu.exam.protocol,shimadzu.exam.bodypart,shimadzu.exam.operator,shimadzu.
exam.dap,shimadzu.exam.absorbeddose,shimadzu.exam.ei,shimadzu.exam.eit,shimadzu.exam
.di,shimadzu.exam.kv,shimadzu.exam.ma,shimadzu.exam.ms,shimadzu.exam.mas,shimadzu.e
xam.sid,shimadzu.exam.sensorsn</order>
</decoder>
```

OSSEC Workshop: Dynamic Decoders

Lesson 01:

append 99-shimadzu-exam-decoder.xml to /var/ossec/etc/decoder.xml

add to ossec.conf:

<rule_dir pattern=".xml$">etc/rules.d</rule_dir>

copy 99_custom_shimadzu_rules.xml to /var/ossec/etc/rules.d/

check analysisd.decoder_order_size= value in internal_options.conf

OSSEC Workshop: Dynamic Decoders

Paste the contents of event.txt into /var/ossec/bin/ossec-logtest:

```
**Phase 1: Completed pre-decoding.
    full event: '"1/1/2014","01:26:48","78-XR-14-000045","Rad","CHEST AP
X-WISE","CHEST","L\F","AP","deleom","","","","","","","0.031","","319.66767857507","141.926534
243403","-1","-10000","90","160","6","0.96","","18000959"'
    hostname: 'c7-64-dev-ossec-community'
    program_name: '(null)'
    log: '"1/1/2014","01:26:48","78-XR-14-000045","Rad","CHEST AP
X-WISE","CHEST","L\F","AP","deleom","","","","","","","0.031","","319.66767857507","141.926534
243403","-1","-10000","90","160","6","0.96","","18000959"'
```

OSSEC Workshop: Dynamic Decoders

```
**Phase 2: Completed decoding.
    decoder: 'shimadzu-exam-log1'
    shimadzu.exam.protocol: 'Rad'
    shimadzu.exam.bodypart: 'CHEST AP      X-WISE'
    shimadzu.exam.operator: 'deleom'
    shimadzu.exam.dap: '""'
    shimadzu.exam.absorbeddose: '0.031'
    shimadzu.exam.ei: '141.926534243403'
    shimadzu.exam.eit: '-1'
    shimadzu.exam.di: '-10000'
    shimadzu.exam.kv: '90'
    shimadzu.exam.ma: '160'
    shimadzu.exam.ms: '6'
    shimadzu.exam.mas: '0.96'
    shimadzu.exam.sid: '""'
    shimadzu.exam.sensorsn: '"18000959"'
```

OSSEC Workshop: Dynamic Decoders

**Phase 3: Completed filtering (rules).
    Rule id: '91000'
    Level: '7'
    Description: 'Shimadzu Exam Log'
**Alert to be generated.

OSSEC Workshop: Rootcheck Lab

restore ossec.conf to re-enable rootcheck

cp /var/ossec/etc/ossec.conf.org /var/ossec/etc/ossec.conf
/var/ossec/bin/ossec-control restart

OSSEC Workshop: Rootcheck

What to know:

rootcheck scans the filesystem.

No really. Rootcheck. Scans. The. Filesystem.

Syscheck (FIM) will not report events until rootcheck has finished starting

Centrally managed from /var/ossec/etc/shared/

OSSEC Workshop: Rootcheck Capabilities

Capabilities

- Can look at the content of a file/registry
- Tests for processes
- Examine directories

Compliance: cis_rhel7_linux_rcl.txt

Malware: rootkit_files.txt, rootkit_trojans.txt

Application Inventory: win_applications_rcl.txxt

OSSEC Workshop: Rootcheck Compliance

edit /var/ossec/etc/shared/cis_rhel7_linux_rcl.txt

File example, detect partitions, 1.1.1

This reads /etc/fstab, and looks for a string

f:/etc/fstab <- FOR this file

!r:/tmp <- regular expression for this value.

This test fails (!) if /tmp is not detected in /etc/fstab

OSSEC Workshop: Rootcheck Compliance

Process lookup example:

Goto 3.2, remove X Windows
f:/usr/lib/systemd/system/default.target
  r:Graphical (looking for the string)

OR
p:gdm-x-session; <- this is looking for the running process

Both conditions will flag this event

OSSEC Workshop: Rootcheck Compliance

Gotchas and Advanced Usage

edit /var/ossec/etc/shared/system_audit_rcl.txt

$web_dirs=/var/www,/var/htdocs

d:$web_dirs -> ^.ssh

the above will crawl every directory tree declared in web_dirs looking for the directory ".ssh". This IOC detection can be IO intensive depending on the size or type of directory. Realtime FIM is an alternative

OSSEC Workshop: Rootcheck Malware detction

Simple:
d:$web_dirs -> ^.htaccess -> r:RewriteCond \S+HTTP_REFERERS
\S+google;

rootkit_trojans, this is performing a binary search
ls !bash|^/bin/sh

Registries, win_malware_rcl.txt
r:HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\
Run -> userinit -> r:ntos.exe

OSSEC Workshop: Rootcheck Application Inventory

win_applications_rcl.txt

[Remote Access - gotomypc]
f:\Program Files\Citrix\GoToMyPC\g2comm.exe
r:HKLM\software\microsoft\windows\currentversion\run ->
gotomypc;
p:r:g2svc.exe

OSSEC Workshop: Rootcheck a new compliance test

Open one of the CIS benchmark PDF's from your desktop: Ubuntu

Save yourself some time, copy the debian benchmark to:
cis_ubuntu18_linux_L1_rcl.txt

OSSEC Workshop: Questions?