OSSEC Con 2019 Workshop

Download links

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

Contains the all the examples used here for this workshop:

training/workshop2019/

Under /root/Atomicorp/ on the Hyperqube virtual machines

OSSEC 2019 Workshops

- Active Response
- Threat Intelligence
- Dynamic Decoders

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 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

- lesson01 : 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. Create a test file and restart OSSEC:

```
date >> /mnt/testfile1
/var/ossec/bin/ossec-control restart
```

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: Threat Intelligence

Perform IP address lookups on TI database

Requires:

    at least 1 cdb list (threat4.cdb in this example, these are updated constantly all day!)

    99_threat_intel.xml

Active response? Or not?

OSSEC Workshop: Threat Intelligence

```
cp threat4.cdb /var/ossec/etc/lists/threat
```

Add to the <rules> section at the end in ossec.conf:

```
       <rule_dir pattern=".xml$">etc/rules.d</rule_dir>
        <list>etc/lists/threat/threat4</list>
```

add 99_threat_intel.xml to /var/ossec/etc/rules.d/

OSSEC Workshop: Threat Intelligence

test content is in event.txt, test first with:
/var/ossec/bin/ossec-logtest

```
**Phase 1: Completed pre-decoding.
       full event: '94.103.36.55 - - [19/Mar/2019:11:17:03 +0000] "POST
/wordpress/xmlrpc.php HTTP/1.0" 404 464 "-" "Wget(linux)"'
       hostname: 'c7-64-dev-ossec-community'
       program_name: '(null)'
       log: '94.103.36.55 - - [19/Mar/2019:11:17:03 +0000] "POST
/wordpress/xmlrpc.php HTTP/1.0" 404 464 "-" "Wget(linux)"'
```

OSSEC Workshop: Threat Intelligence

```
**Phase 2: Completed decoding.
       decoder: 'web-accesslog'
       srcip: '94.103.36.55'
       srcuser: '-'
       action: 'POST'
       url: '/wordpress/xmlrpc.php'
       id: '404'
```

OSSEC Workshop: Threat Intelligence

```
**Phase 3: Completed filtering (rules).
       Rule id: '60047'
       Level: '10'
       Description: 'Atomicorp: IP found on Threat
Category 4 Atomicorp RBL - Known Attackers'
**Alert to be generated.
```

OSSEC Workshop: Threat Intelligence

```
<group name="threat_intelligence">
        <rule id="60047" level="10">
                <if_group>web|attack|attacks|iptables|firewall|
sshd</if_group>
                  <list field="srcip"
lookup="address_match_key">etc/lists/threat/threat4</list
>
                  <description>Atomicorp: IP found on Threat
Category 4 Atomicorp RBL - Known
Attackers</description>
        </rule>
</group>
```

OSSEC Workshop: Threat Intelligence

Disable Active Response per rule:

```
<group name="threat_intelligence">
        <rule id="60047" level="10">
              <if_group>web|attack|attacks|iptables|firewall|
sshd</if_group>
               <options>no_ar</options>
                <list field="srcip"
lookup="address_match_key">etc/lists/threat/threat4</list
>
                <description>Atomicorp: IP found on Threat
Category 4 Atomicorp RBL - Known
Attackers</description>
        </rule>
```

OSSEC Workshop: Threat Intelligence

Restart ossec:

```
/var/ossec/bin/ossec-control restart
```

append event.txt to /var/log/messages

```
cat event.txt >> /var/log/messages
```

OSSEC Workshop: Dynamic Decoders

Lesson 01:

Upgrade your system to ossec-hids-3.3.0 (pre-release)

Centos/RHEL/Fedora

```
yum --enablerepo=atomic-testing upgrade ossec-hids
```

Ubuntu 18:

https://updates.atomicorp.com/channels/atomic-testing/ubuntu/

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","","319.667
67857507","141.926534243403","-1","-
```

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":"shimadz
u-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\",\"141.92653424
3403\",\"-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.ab
sorbeddose":"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","shi
madzu.exam.mas":"0.96","shimadzu.exam.sid":"\"\"","shimadzu.exam.sensorsn":"\"180009
59\"","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.ope
rator,shimadzu.exam.dap,shimadzu.exam.absorbeddose,shimadzu.exam.ei,shi
madzu.exam.eit,shimadzu.exam.di,shimadzu.exam.kv,shimadzu.exam.ma,shim
adzu.exam.ms,shimadzu.exam.mas,shimadzu.exam.sid,shimadzu.exam.sensor
sn</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","141.9265342434
03","-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","141.9265342434
03","-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: Dynamic Decoders

Append to /var/log/messages to generate an alert in /var/ossec/logs/alerts/alerts.json and ELK:

```
cat event.txt >> /var/log/messages
```

OSSEC Workshop: Questions?