



OSSEC 3.0 Preview

OSSEC CON 2018

Scott Shinn – OSSEC Project Manager





WHAT'S NEW WITH OSSEC 3.0

A Preview of the Latest Release





What's New in OSSEC 3.0

- New linux distribution, snapshot and docker repo support
- GeoIP in Rules
- Provisioning Automation in Windows and Linux
- SQLite support in FIM
- IPv6 Support, and TCP transport for Agent Communications
- Slack and Pagerduty Notification
- Much much more!



The Big Changelog

- OSSEC changelog (3.0.0) <scott@atomicorp.com>
- Release Maintainers
 - Dan Parriott
 - Scott R. Shinn (Atomicorp, Inc.)
- Whats New
 - Click [here](#) to see the full changelog



OSSEC on Github

- Source:
 - <https://github.com/ossec/ossec-hids/>
- Documentation:
 - <https://github.com/ossec/ossec-docs/>



New Repos and Distros

- Binary packaging for master (snapshots!)
- Amazon / Amazon LTS
- CentOS / RHEL / Clones 6/7
- Debian 8/9
- Kali
- Mint
- Ubuntu 14/16/18
- Windows



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`



GeoIP Rules

- Uses the MaxMind GeoLite database (www.maxmind.com)
- Updated twice daily (update often!)
- Adds the rule tag modifies:
 - `<srcgeoip>XX</srcgeoip>`
 - `<dstgeoip>XX</dstgeoip>`
 - `<different_srcgeoip />`



GeoIP Rules Example

```
<rule id="5749" level="6" frequency="1" timeframe="28800">
```

```
  <if_matched_sid>5715</if_matched_sid>
```

```
  <same_user />
```

```
  <different_srcgeoip />
```

```
  <description>Multiple successful logins from same user from different countries.</description>
```

```
  <group>behaviour_anomaly,</group>
```

```
</rule>
```

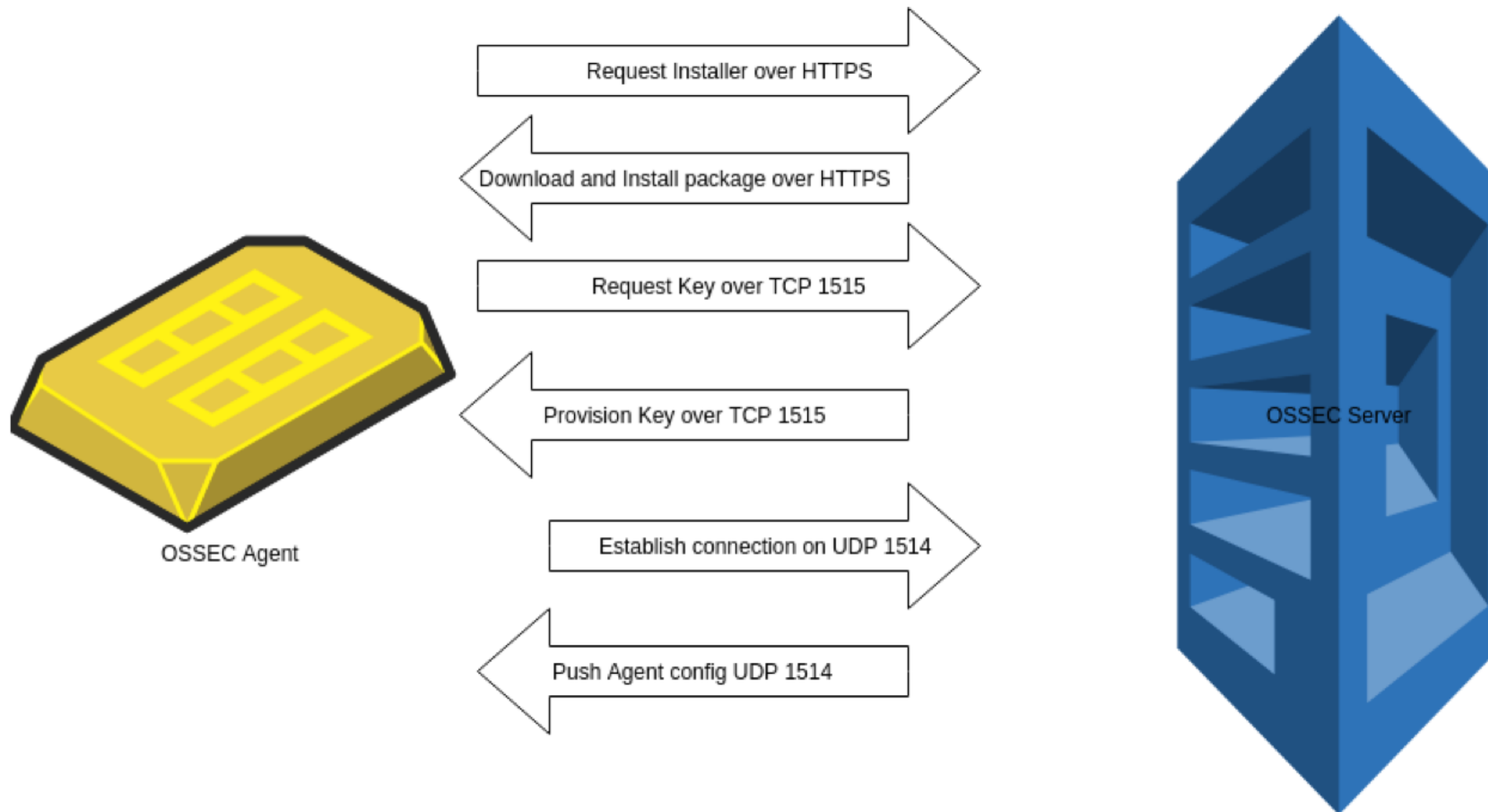


Provisioning Automation

Yum / Apt + agent-auth = one click installs
(windows too!)



Provisioning Automation





JSON Output / Elasticsearch



ELASTIC
SEARCH



Logstash

Kibana



JSON Output Example

```
{
  "rule": {
    "level": 3,
    "comment": "System Audit event.",
    "sidid": 516,
    "group": "ossec,rootcheck, "
  },
  "id": "1522850038.10150",
  "TimeStamp": 1522850038000,
  "decoder": "rootcheck",
  "location": "rootcheck",
  "full_log": "System Audit: CIS - RHEL7 - 6.2.9 - SSH Configuration - Empty passwords permitted {CIS: 6.2.9 RHEL7} {PCI_DSS: 4.1}. File: /etc/ssh/sshd_config. Reference: https://benchmarks.cisecurity.org/tools2/linux/CIS_Red_Hat_Enterprise_Linux_7_Benchmark_v1.1.0.pdf.",
  "hostname": "ossec-01"
}
```



OSSEC

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

Twitter@kwm



OSSEC GOVERNANCE

The Open-Source Project at a Glance





Project at a Glance

- First Released in 2005 by Daniel Cid
- Started in 2003
- Its short for Open Source Security and even we do not agree on how to pronounce it.
- Acquired by Third Brigade in 2008, and Trend Microsystems in 2009
- Supports Windows, Linux, OSX, Solaris, Aix, and many many more
- Millions of installs, on every continent



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





Leadership

- Dan Cid (Founder)
 - Sucuri / Godaddy
- Jeremy Rossi (Previous Project Lead)
 - Bloomberg
- Scott Shinn (Current Project Lead)
 - Joined in 2006
 - Project Leader in 2014
 - CTO Atomicorp



Governance Goals

- Transition project to a non-profit entity
- Certification for FIPS-140-2
- Open Source Software certification, and Approved Product Lists
- Industry support with domain experts like Virgil, Elasticsearch, Amazon, and Slack



Learn More About OSSEC

- [OSSEC GitHub Site](#)
- [OSSEC Download Page](#)
- [The OSSEC community on Slack](#)
- [Subscribe to monthly OSSEC newsletter](#)
- [Follow the OSSEC Project on Twitter](#)

