aptible

shared-us-west-1

Enclave Intrusion Detection Report

2017-11-06 to 2017-11-12

Preamble

Aptible Enclave is a container orchestration platform that enables users to deploy containerized workloads onto dedicated isolated networks. Each isolated network and its associated cloud infrastructure is called an Enclave stack.

Enclave stacks contain a number of AWS EC2 instances (virtual machines), on which Enclave customers deploy their apps and databases in Docker containers. The Enclave security team is responsible for the integrity of these instances, and provides this report on a periodic basis as evidence of its activity.

Scope

This particular report is a consolidated view of host-level intrusion-detection (HIDS) activity on the **shared-us-west-1** stack over the **2017-11-06 to 2017-11-12** reporting period.

As such, it exhaustively covers HIDS activity relevant to the apps and databases deployed on the **shared-us-west-1** stack during this timeframe.

Status

This report was generated on **2017-11-13** for the **2017-11-06 to 2017-11-12** reporting period. It was signed-off on by **Frank Macreery** <**frank@aptible.com**>, **CTO**.

This means that, as of **2017-11-13**, all the events listed in this report have been reviewed by the Enclave security team and remediated if applicable.

Methodology

Aptible Enclave collects HIDS events using OSSEC, a leading open-source intrusion detection system.

The events generated by OSSEC are ingested in Aptible's security reporting platform, to be processed in one of the following ways:

- Automated Review
- Bulk Review
- Manual Review

Once processed, these events are included in this report.

If an intrusion is suspected or detected, the Enclave security team activates its incident response process to assess, contain, and eradicate the threat, and notifies affected customers, if any.

Aptible's incident response program has been developed in alignment with ISO 27001 standards. A copy of Aptible's ISO 27001 certification is available on the Aptible website.

The diagram on the next page describes this process visually.

Process Diagram

Review Processes

This section explains the review processes used by the Enclave security team for intrusion detection.

Automated Review

Enclave's security reporting platform automatically reviews a certain number of events generated by OSSEC.

Here are some examples of automated review:

- Purely informational events such as events indicating that OSSEC performed a periodic integrity check. These are automatically reviewed because their sole purpose is to let them appear in the final report you are looking at now.
- Acceptable security events. For example, an automated script running as root using `sudo`: using `sudo` is technically a relevant security event, but if the user already has root privileges, it cannot result in privilege escalation, so that event is automatically approved.

Bulk Review

Enclave's security reporting platform integrates with a number of other systems that members of the Aptible operations and security teams interact with. Information from these other systems is collected by Aptible's security reporting platform to determine whether the events generated by OSSEC can be approved without further review.

Here are some notable examples of bulk-reviewed events:

- When a successful SSH login occurs on an Enclave instance, Enclave's monitoring determines whether the SSH login can be tied to an authorized Aptible operations team member, and if so prompts them via Slack to confirm that they did trigger this login (if no authorized team member can be found, or the team member takes too long to respond, an alert is immediately escalated to the Aptible security team). When a login is approved this way, corresponding IDS events will be automatically approved and flagged as bulk review.
- When a member of the Aptible operations team deploys updated software via AWS OpsWorks to Enclave hosts, corresponding file integrity alerts are

automatically approved in Aptible's security reporting platform, and flagged as bulk reviews.

Manual Review

When a security event is neither reviewed automatically nor in bulk, it is escalated to the Aptible security team for manual review, which is performed on a regular basis in conformance with Aptible's ISO 27001-certified policies and procedures.

Some examples of manually-reviewed events include:

- Malware detection events. Malware detection is often racy and generates a number of false positives, which need to be manually reviewed by Aptible.
- Configuration changes that were not otherwise bulk-reviewed. For example, changes that result from nightly automated security updates.

List of Security Events

This seciton lists the Security Events monitored by Enclave as of the generation of this report:

CIS benchmark non-conformance

This event is generated when Enclave's monitoring detects an instance that does not conform to the CIS Controls Enclave is currently targeting.

These events are often triggered on older instances that are not yet configured to follow Enclave's latest security best practices.

The underlying conformance is remediated by replacing or reconfiguring the instance, and is prioritized by the Aptible security team depending on the severity of the non-conformance.

File integrity change

This event is generated when Enclave's monitoring detects a change to a monitored file.

These events are often the result of package updates, deployments, or the activity of Enclave operations team members, and are reviewed accordingly.

Other informational event

This event is generated when Enclave's monitoring detects an otherwise un-categorized informational event.

These events are often auto-reviewed due to their informational nature, and they're used by the Enclave security team for high-level reporting.

Other low-severity event

This event is generated when Enclave's monitoring detects an otherwise un-categorized low-severity event.

These events tend to provide a very low signal-to-noise ratio, so they're often reviewed automatically, periodically reviewed in aggregate by the Enclave security team.

Periodic rootkit check

Enclave performs a periodic scan for resident rootkits and other malware. This event is generated every time the scan was performed.

If potential infection is detected, a rootkit check event alert will be generated.

Periodic system integrity check

Enclave performs a periodic system integrity check to scan for new files in monitored system directories as well as deleted files. This event is generated every time the scan was performed.

Among others, this scan covers /etc, /bin, /sbin, /boot, /usr/bin, /usr/sbin.

Note that Enclave also monitors changes to files under these directories in real-time. If they change, a file integrity alert will be generated.

Privilege escalation (e.g. sudo, su)

This event is generated when Enclave's monitoring detects that a user escalated their privileges on a host, using tools such as sudo or su.

This activity is often the result of automated maintenance scripts or the activity of Enclave operations team members, and is reviewed accordingly.

Rootkit check event

This event is generated when Enclave's monitoring detects potential rootkit or malware infection.

Due to the inherently racy nature of most rootkit scanning techniques, these events are often false positives, but they are all investigated by Enclave's security team.

SSH login

This event is generated when Enclave's monitoring detects host-level access via SSH.

Whenever they log in to a host, Enclave operations team members are prompted to confirm that the activity is legitimate, so these events are often reviewed in bulk.

Uncategorized event

This event is generated for uncategorized events generated by Enclave's monitoring. These events are often reviewed directly by the Enclave security team.

User or group modification

This event is generated when Enclave's monitoring detects that a user or group was changed on the system.

This is usually the result of the activity of Enclave operations team members.

Instances

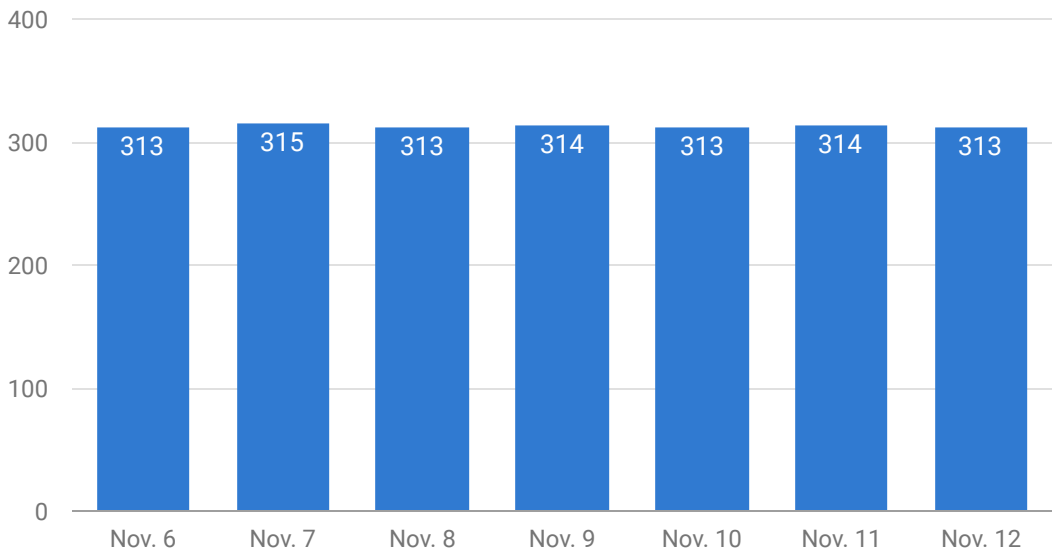
Below is a list of all the instances that were present on the **shared-us-west-1** stack during the reporting period, on which customer Docker containers may be deployed.

The report includes one section for each instance, which contains a histogram depicting the number of events collected during each day in the reporting period, and a table breaking down the number of events by category and how they were reviewed.

1. i-044d53173fee02692
2. i-07ee971b810531107
3. i-0bc7e5432366237d5
4. i-3cd71f88
5. i-837ac540

Instance Report: i-044d53173fee02692

Events by day

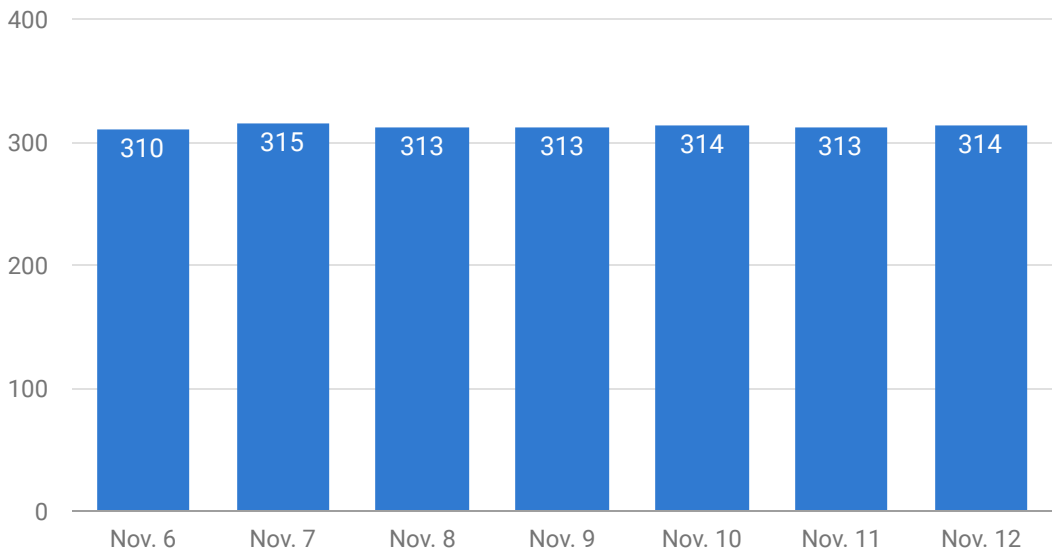


Events by category

EVENT	SEVERITY	TOTAL COUNT	AUTOMATED REVIEW	BULK REVIEW	MANUAL REVIEW	PENDING REVIEW
Privilege escalation (e.g. sudo, su)	MEDIUM	1344	1344	0	0	0
File integrity change	LOW	1	0	1	0	0
Other informational event	INFORMATIONAL	672	672	0	0	0
Periodic system integrity check	INFORMATIONAL	164	164	0	0	0
Periodic rootkit check	INFORMATIONAL	14	14	0	0	0
Total		**2195**	**2194**	**1**	**0**	**0**

Instance Report: i-07ee971b810531107

Events by day

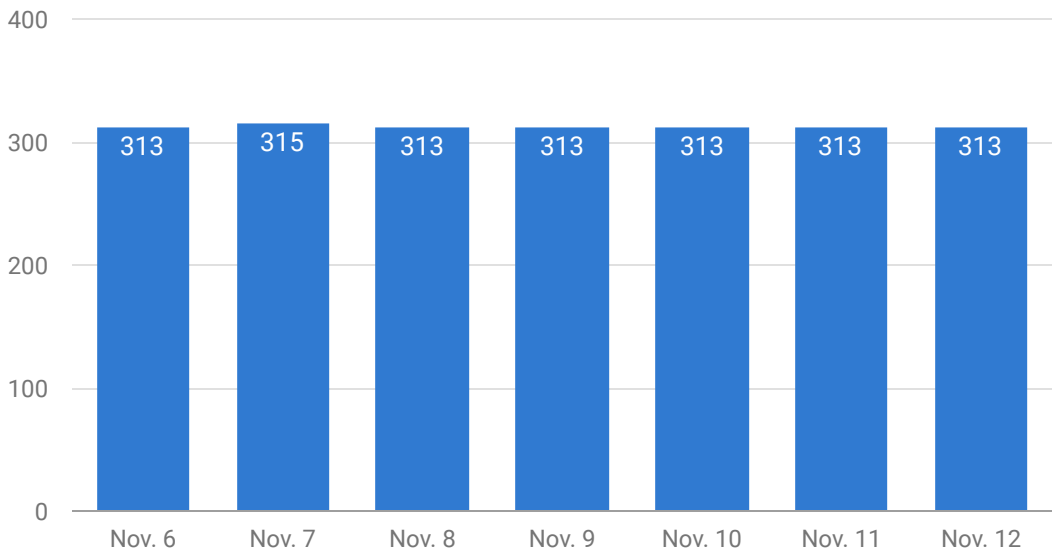


Events by category

EVENT	SEVERITY	TOTAL COUNT	AUTOMATED REVIEW	BULK REVIEW	MANUAL REVIEW	PENDING REVIEW
Privilege escalation (e.g. sudo, su)	MEDIUM	1342	1342	0	0	0
File integrity change	LOW	1	0	1	0	0
Other informational event	INFORMATIONAL	671	671	0	0	0
Periodic system integrity check	INFORMATIONAL	164	164	0	0	0
Periodic rootkit check	INFORMATIONAL	14	14	0	0	0
Total		**2192**	**2191**	**1**	**0**	**0**

Instance Report: i-0bc7e5432366237d5

Events by day

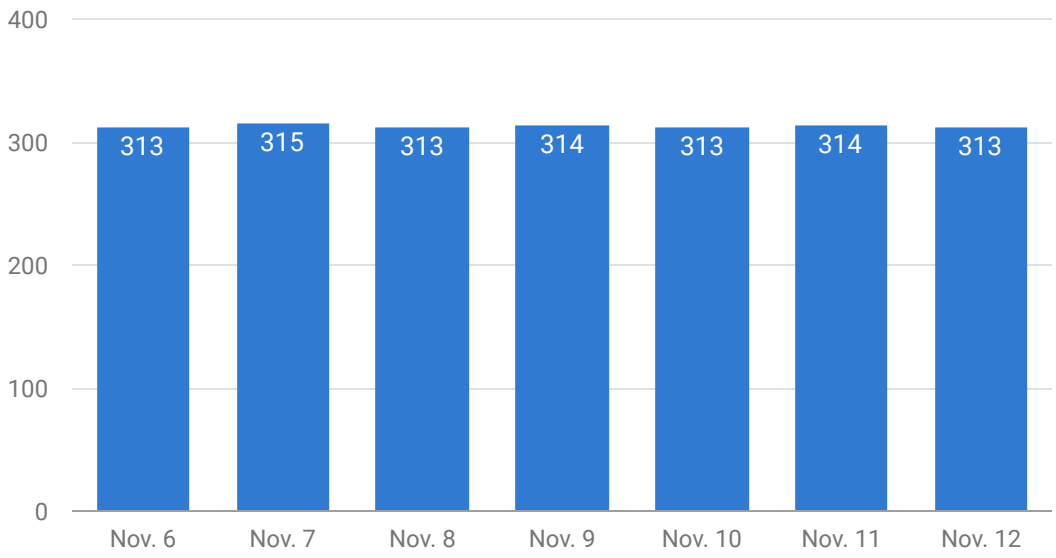


Events by category

EVENT	SEVERITY	TOTAL COUNT	AUTOMATED REVIEW	BULK REVIEW	MANUAL REVIEW	PENDING REVIEW
Privilege escalation (e.g. sudo, su)	MEDIUM	1344	1344	0	0	0
File integrity change	LOW	1	0	1	0	0
Other informational event	INFORMATIONAL	672	672	0	0	0
Periodic system integrity check	INFORMATIONAL	162	162	0	0	0
Periodic rootkit check	INFORMATIONAL	14	14	0	0	0
Total		**2193**	**2192**	**1**	**0**	**0**

Instance Report: i-3cd71f88

Events by day

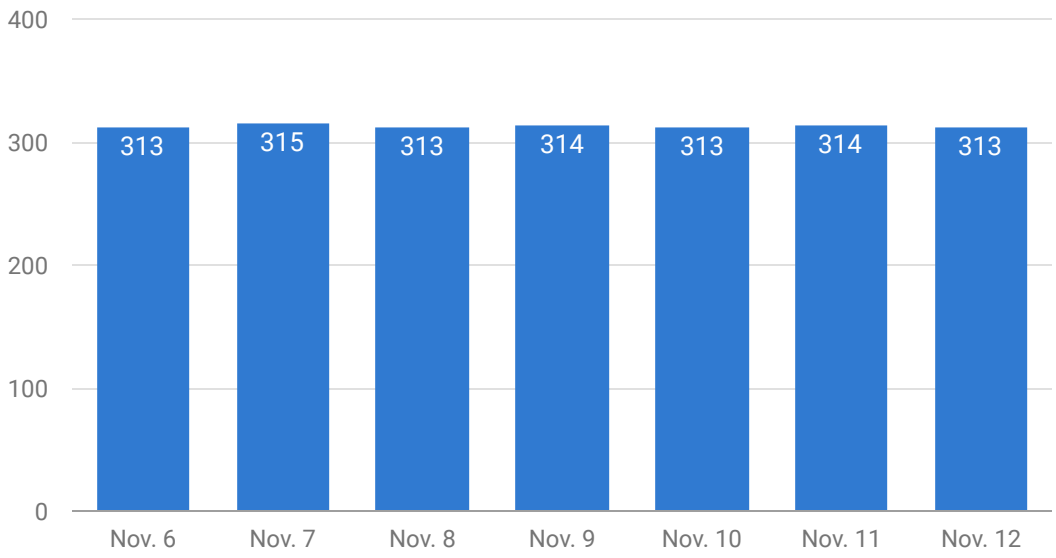


Events by category

EVENT	SEVERITY	TOTAL COUNT	AUTOMATED REVIEW	BULK REVIEW	MANUAL REVIEW	PENDING REVIEW
Privilege escalation (e.g. sudo, su)	MEDIUM	1344	1344	0	0	0
File integrity change	LOW	1	0	1	0	0
Other informational event	INFORMATIONAL	672	672	0	0	0
Periodic system integrity check	INFORMATIONAL	164	164	0	0	0
Periodic rootkit check	INFORMATIONAL	14	14	0	0	0
Total		**2195**	**2194**	**1**	**0**	**0**

Instance Report: i-837ac540

Events by day



Events by category

EVENT	SEVERITY	TOTAL COUNT	AUTOMATED REVIEW	BULK REVIEW	MANUAL REVIEW	PENDING REVIEW
Privilege escalation (e.g. sudo, su)	MEDIUM	1344	1344	0	0	0
File integrity change	LOW	1	0	1	0	0
Other informational event	INFORMATIONAL	672	672	0	0	0
Periodic system integrity check	INFORMATIONAL	164	164	0	0	0
Periodic rootkit check	INFORMATIONAL	14	14	0	0	0
Total		**2195**	**2194**	**1**	**0**	**0**