

Intrusion Detection

with

AIDE



FOSS ASIA 2016 - Singapore

</Michael art Rebultan>

MIT | CEH | ECSA

WELCOME !!!

The logo for Fossasia, featuring the word "foss" in a bold, red, sans-serif font on the top line, and the word "asia" in a similar bold, red, sans-serif font on the bottom line. The letters are closely spaced and have a slightly rounded, modern feel. The entire logo is centered within a white rectangular area.

**foss
asia**



FOSSASIA2016

</AGENDA>

- Integrity check w/ AIDE on Linux



FOSSASIA2016

</OBJECTIVE>

- One of the first safety measures that any sysadmin may want to implement in their production servers is a mechanism to detect file tampering - not only the content of files, but also their attributes.



</SCOPE>

- Install, Set-up, Configure and POC



FOSSASIA2016

</AIDE is NOT>

- NIDS
- Anti-Malware
- Real-Time Detection



</KICKSTART>

- `yum install -y aide`
- `cd /var/lib/aide`
- `mv aide.db.new.gz aide.db.gz`
- `aide -check`
- `aide -update`
- Automate with Cron
- Tweak the configuration
- POC – (*Recoded Demo*)



FOSSASIA2016

</My 2¢>

- Do not assume anything
- Trust no-one
- Nothing is secure
- Security is a trade-off with usability
- Paranoia is your friend

XIE XIE NI !!!

**foss
asia**

<http://mrebultan.simplesite.com/>