Recent Changes

Some of the big changes this year

- Moloch 1.0
- Capture stability
- Full IPv6 support
- ES 6 support
- Parliament Alerting
- Packet Search

Moloch 1.0

- Previously field names were terrible, new names are so beautiful
- Unfortunately required a painful reindexing
- Removed all analyzed fields
  - We've gotten feedback this is bad, planning to add back for Moloch 2.0
- ES 5 & ES 6 Support
- Switch to the new Maxmind API and 2 character country codes

Capture

- Many new classifiers: dhcp, dhcpv6, splunk, isakmp, ntp, ...
- OUI lookups
- Can reload oui, geo, rules without restarting
- Can decode many new VPNs
- Suricata plugin
- Autogenerated ES Ids

Capture Stability

- Require gnu99 compiler now
- 1.5/1.6 have numerous stability fixes
- Sanitize
  - New option for clang/gcc
  - Memory, integer overflow, and other checks
  - Runs on every commit now
  - Working on running in lab and production setting
- Cppcheck
  - Static analysis
  - Working to integrate into build system

Suricata Plugin

- Reads eve.json or alerts.json from disk
- Able to enrich moloch sessions since Suricata writes right away, and moloch is delayed
- Not a Suricata UI
- Only works when Moloch can read the files as they are written

Suricata Screenshot

Suricata

Signature	ET POLICY HTTP traffic on port 443 (CONNECT)
Category	Potentially Bad Traffic
Flow Id	1708257947171143
Action	allowed
Gid	1
Severity	0
Signature id	2,013,933

Wise

- Handle multiple WISE servers better
- Support any field
- Splunk data source
- Easier to create views/sources
- Support more than 255 fields

Viewer

- Angular to Vue.js (performance improvements)
- Stats pages for Indices, Tasks, and Shards!
- Packet Search
- Shared Views
- Keyboard shortcuts

DEMO

Upcoming Changes

Building/Releases

- Last year had 4 build systems!
- Currently 3 build systems:
  - Vagrant - Releases
  - Vagrant - Nightly (Will be removed Dec 1st)
  - Screwdriver - builds on commits and pull requests
- Move to screwdriver for all builds
- Use bintray for ppa/repos

Moloch 2.0 - Ideas

- ES 6.x required
- Add field analyzers back
- New visualizations
  - Connections tab rewrite
  - Flow view
- Viewer/Multiviewer merge - Selectable clusters to search
- New Parsers: SIP, IMAP, ...
- Users “rethink” and Parliament
- History of Observed Data Indicators
- Tshark json view

Open source hygiene

- Adding a Contributor License Agreement (CLA) to github commits
- Adding a Code of Conduct to the github project
- Encourage code contributors from outside of Oath
- Goal of adding an external main committer
- Encourage github issues, feature requests, pull requests, wiki additions/revisions


PARLIAMENT


QUESTIONS?