Arkimeet 2023

WELCOME!

Welcome!

Pick up a shirt during any break

Refreshments are in the coolers

Happy Hour is here, 5pm-7pm

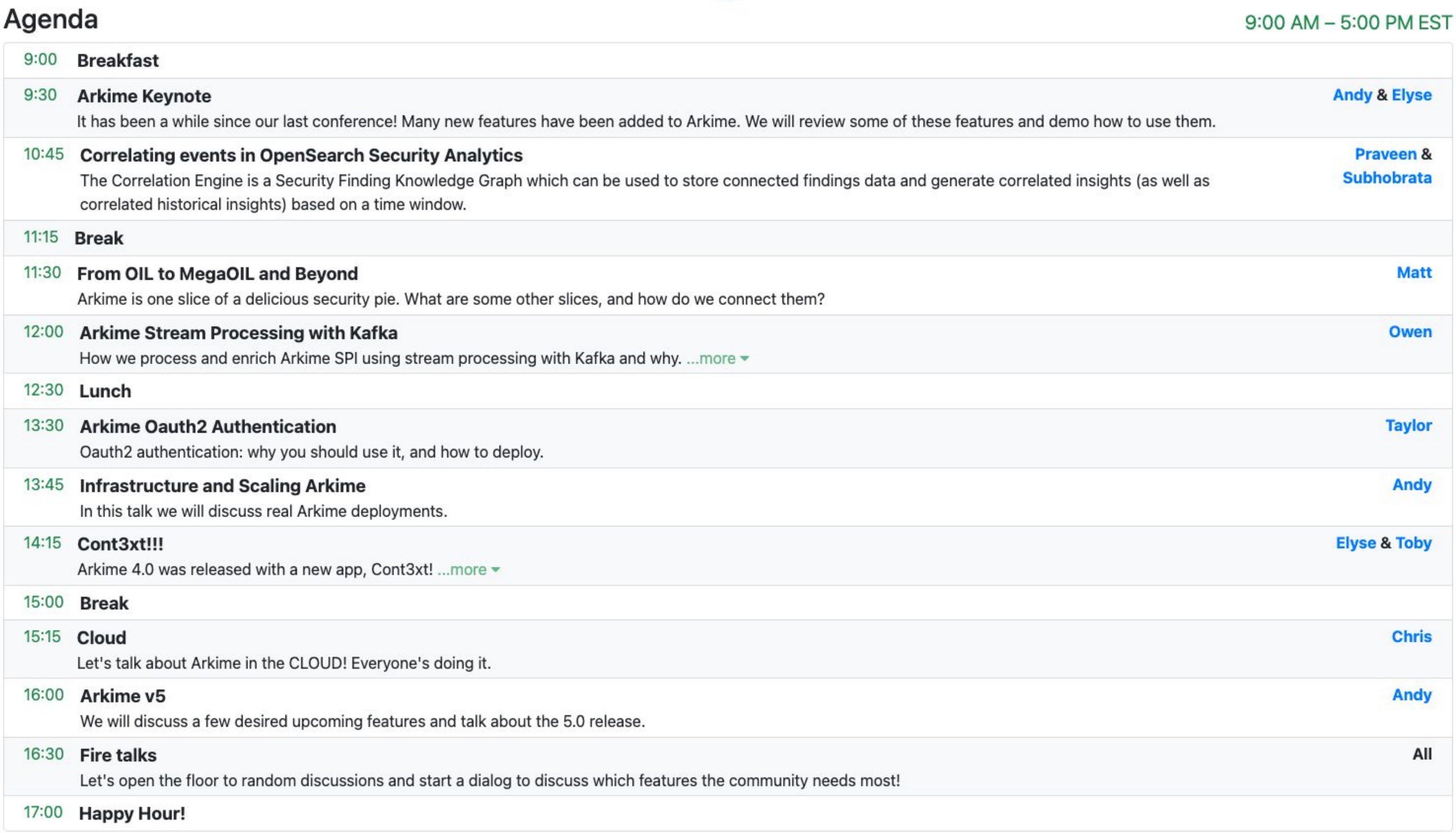
MEET US!

Andy Wick
Arkime Creator

Elyse Rinne
Software Engineer
& UI Expert

Chris Helma
Software Engineer
& Cloud Expert

Toby Salusky
Software Development
Intern



Agenda

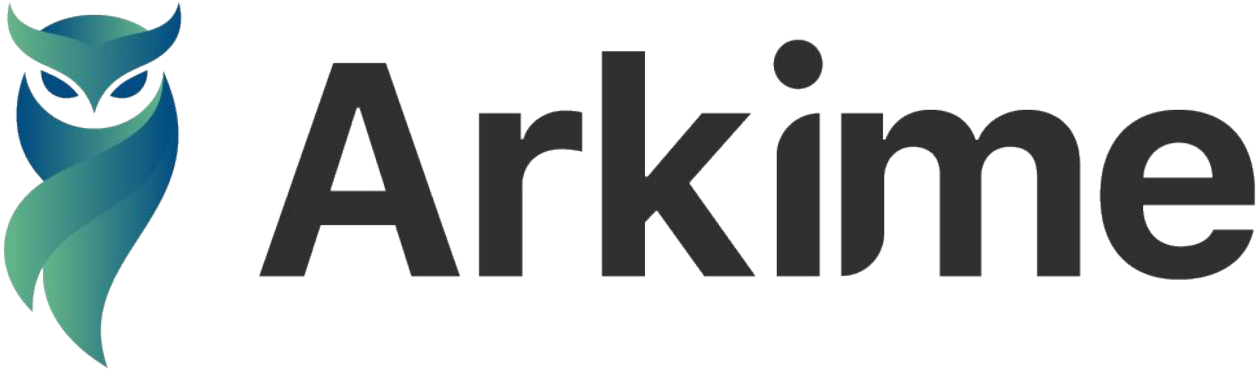
9:00 AM – 5:00 PM EST

9:00	**Breakfast**	
9:30	**Arkime Keynote** It has been a while since our last conference! Many new features have been added to Arkime. We will review some of these features and demo how to use them.	Andy & Elyse
10:45	**Correlating events in OpenSearch Security Analytics** The Correlation Engine is a Security Finding Knowledge Graph which can be used to store connected findings data and generate correlated insights (as well as correlated historical insights) based on a time window.	Praveen & Subhobrata
11:15	**Break**	
11:30	**From OIL to MegaOIL and Beyond** Arkime is one slice of a delicious security pie. What are some other slices, and how do we connect them?	Matt
12:00	**Arkime Stream Processing with Kafka** How we process and enrich Arkime SPI using stream processing with Kafka and why. ...more ▾	Owen
12:30	**Lunch**	
13:30	**Arkime Oauth2 Authentication** Oauth2 authentication: why you should use it, and how to deploy.	Taylor
13:45	**Infrastructure and Scaling Arkime** In this talk we will discuss real Arkime deployments.	Andy
14:15	**Cont3xt!!!** Arkime 4.0 was released with a new app, Cont3xt! ...more ▾	Elyse & Toby
15:00	**Break**	
15:15	**Cloud** Let's talk about Arkime in the CLOUD! Everyone's doing it.	Chris
16:00	**Arkime v5** We will discuss a few desired upcoming features and talk about the 5.0 release.	Andy
16:30	**Fire talks** Let's open the floor to random discussions and start a dialog to discuss which features the community needs most!	All
17:00	**Happy Hour!**	

slido

Pick the correct answer

ⓘ Start presenting to display the poll results on this slide.



New Name - New Logo

Approachability & Inclusivity

Merlin's Owl, Archimedes - smart, grouchy, and sarcastic

OpenSearch Elasticsearch

Continue to support both

We will say one, but usually mean either

We hope to support both

(ex. ILM & ISM)

Yahoo runs large ES clusters

Run tests against both

slido

How long ago was the last Conference?

ⓘ Start presenting to display the poll results on this slide.

We've been busy!

github.com/arkime/arkime/blob/main/CHANGELOG

MolochON - Oct 1, 2019

v2.0.1

commit **#3,182**

Arkimeet - May 23, 2023

v4.3.1

commit **#5,305**

API Documentation

arkime.com/apiv3
arkime.com/wiseapi
arkime.com/commonapi

JSDoc standard

Easy to build and update

Arkime.com Web Site

github.com/arkime/arkimeweb

Uses Github Pages

Improved download page

New Galleries of Rules & WISE config

Please contribute!!!

slido

How many releases since last conference?

ⓘ Start presenting to display the poll results on this slide.

Roles

arkime.com/roles

New with v4

Permissions & sharing

superAdmin/usersAdmin are special

*User & *Admin role for each tool

More to come

Index Prefix

arkime.com/settings#prefix

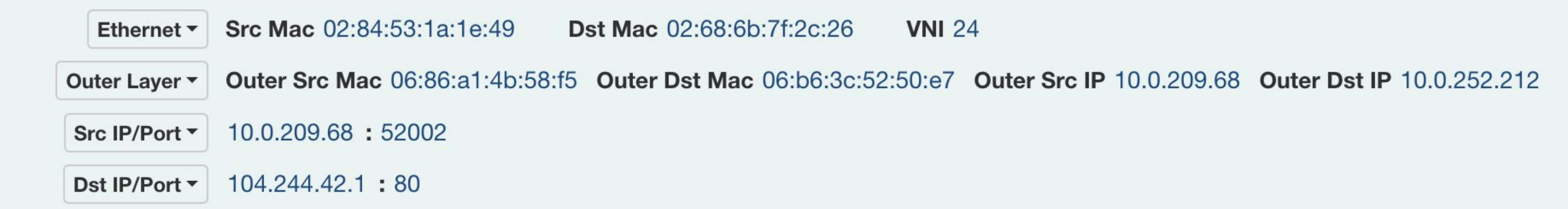
Since v3 new clusters now prefix all indices with arkime_

Can still have Multi-tenant with prefix and usersPrefix settings

Protocol Refactoring

Challenged at MolochON 2019 to support more that just TCP/UDP

- arp, bgp, igmp, isis, lldp, ospf, pim, …
- TCP/UDP are now just parsers
- Standardized layering
  - easy to add new encapsulating protocols
- Track outer IP/MAC information



Ethernet ▾ Src Mac 02:84:53:1a:1e:49 Dst Mac 02:68:6b:7f:2c:26 VNI 24

Outer Layer ▾ Outer Src Mac 06:86:a1:4b:58:f5 Outer Dst Mac 06:b6:3c:52:50:e7 Outer Src IP 10.0.209.68 Outer Dst IP 10.0.252.212

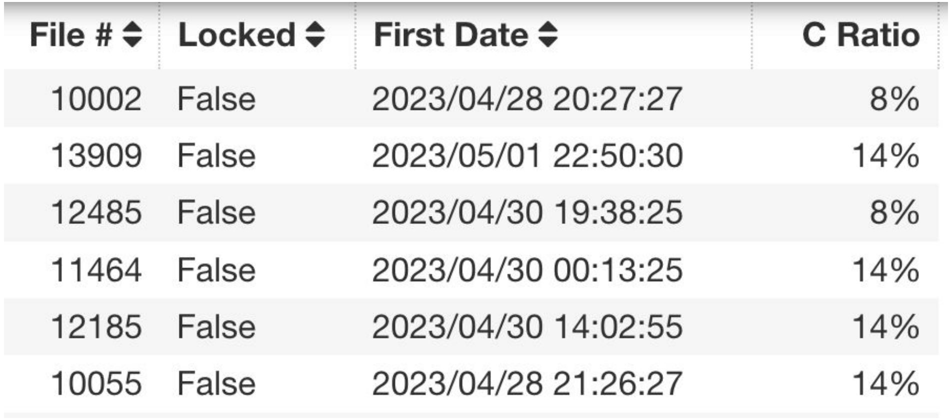
Src IP/Port ▾ 10.0.209.68 : 52002

Dst IP/Port ▾ 104.244.42.1 : 80

Compression

Reducing PCAP storage size is important

- 5 - 25% savings - Andy was wrong
- Support both gzip (4.x default), zstd
  - simpleCompression=gzip
- Compresses in seekable blocks
  - simpleCompressionBlockSize=32000
- Shorten packet headers 16 vs 6 bytes
  - simpleShortHeader=true



File #	Locked	First Date	C Ratio
10002	False	2023/04/28 20:27:27	8%
13909	False	2023/05/01 22:50:30	14%
12485	False	2023/04/30 19:38:25	8%
11464	False	2023/04/30 00:13:25	14%
12185	False	2023/04/30 14:02:55	14%
10055	False	2023/04/28 21:26:27	14%

S3 for PCAP Storage

- Improving since v0.12
- Contributions from community members
- Supports gzip & zstd compression
- New file for each packetThread since v4.3
  - for high volume
- New auth methods supported
  - IMDSv2
  - environment variables

Performance

Do more with less

- afpacket (tpacketv3) rewrite (v4.0.0)
  - Fix packet out of order
  - Lower CPU usage, 25% or more
- Packet deduplication (v2.7.1)
  - enablePacketDedup=true
  - Over dedupSeconds Arkime with drop duplicate packets before processing
  - Saves less PCAP and less packet processing

Capture Improvements

Better build process

HTTP/2

HTTP/3

GQUIC

Authentication Refactor

- Support more than just Digest & Header
    - OIDC to the rescue!!!
- Authentication for all tools in one place
- Fully embrace the nodejs Passport method for authentication
    - And actually understand it
- Can turn off authentication for sensors
- Control where Arkime trusts authentication from using userAuthIps

ES Proxy

Security Proxy:

- Protect OpenSearch/Elasticsearch from a compromised Arkime sensor
- Use it between sensors and OpenSearch/Elasticsearch, but not for Central/Multi viewers
- Enforces rules on which APIs and documents can be used by each sensor

T-ing proxy:

- Send a copy of sessions to two OpenSearch/Elasticsearch clusters
- Use when moving clusters

Viewer Improvements

Automate CyberChef

Refactor into JS classes

Many new stats

Sharing

Nodejs v16

NEW ARKIME FEATURES DEMO

Questions?

slido

What of the following is NOT a private ip?

ⓘ Start presenting to display the poll results on this slide.

Parliament

arkime.com/parliament

Arkime Cluster Dashboard

Links to Clusters

Cluster Health

View Issues

Get Alerts

PARLIAMENT DEMO

WISE

With Intelligence See Everything
arkime.com/wise

Framework for integrating feeds

UI!

Stats

Refactor using JS Classes

Threatstream non copy mode

Shared config

WISE DEMO

Testing & Verification

3 test suites: API, UI, PCAP

- Runs on every commit
- Uses sanitized builds

Fuzzing with -fsanitize=fuzzer

Bug Bounty & Live Hacking Events

Static Tools: cppcheck, eslint

Github code scanning

- formerly lgtm.com

Yahoo Bug Bounty

arkime.com/security

HackerOne since 2018

Intigriti since 2022

Bug Bounty

- AOL/Yahoo! have sponsored Arkime bug bounty program since 2018
- Arkime included in 2 Live Hacking Events
  - 2019/11/19 - HackerOne - Los Angeles, USA
  - 2022/08/17 - Intigriti - Antwerp, Belgium
- Paid hackers over **$90,000**
- Findings
  - ESProxy bypass
  - Filename sanitization
  - Log escaping
  - Capture parsing infinite recursion
  - Capture Hash Table DOS

Cont3xt

arkime.com/cont3xt

Aggregate Threat Intelligence

New to v4

Demo at 14:15

slido

What is Andy's favorite color

ⓘ Start presenting to display the poll results on this slide.

How you can help

github.com/arkime/arkime/blob/main/CONTRIBUTING.md

Add/improve documentation

Submit bugs

Request features

Submit pull requests

Talk to the community on Slack

Office hours

slido

Audience Q&A Session

ⓘ Start presenting to display the audience questions on this slide.