Roadmap Update

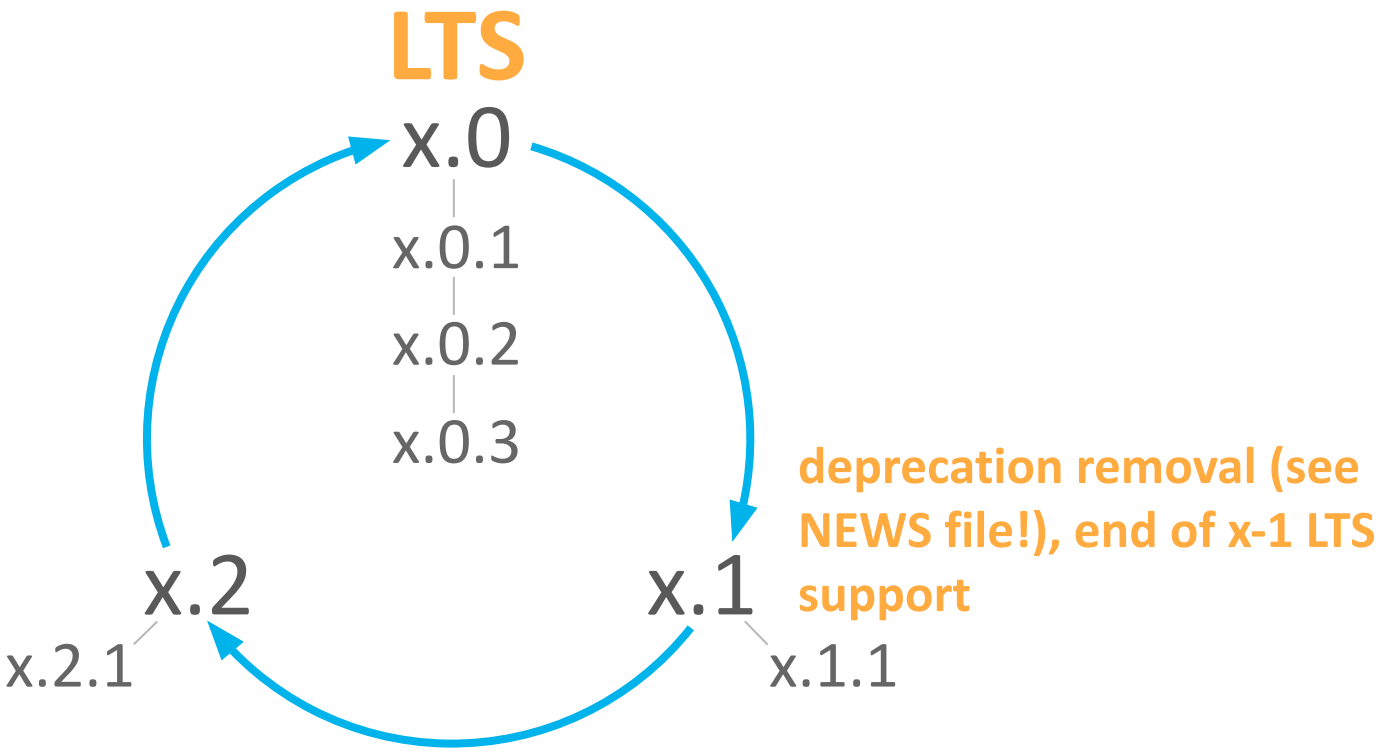
February 2025

Christian Kreibich

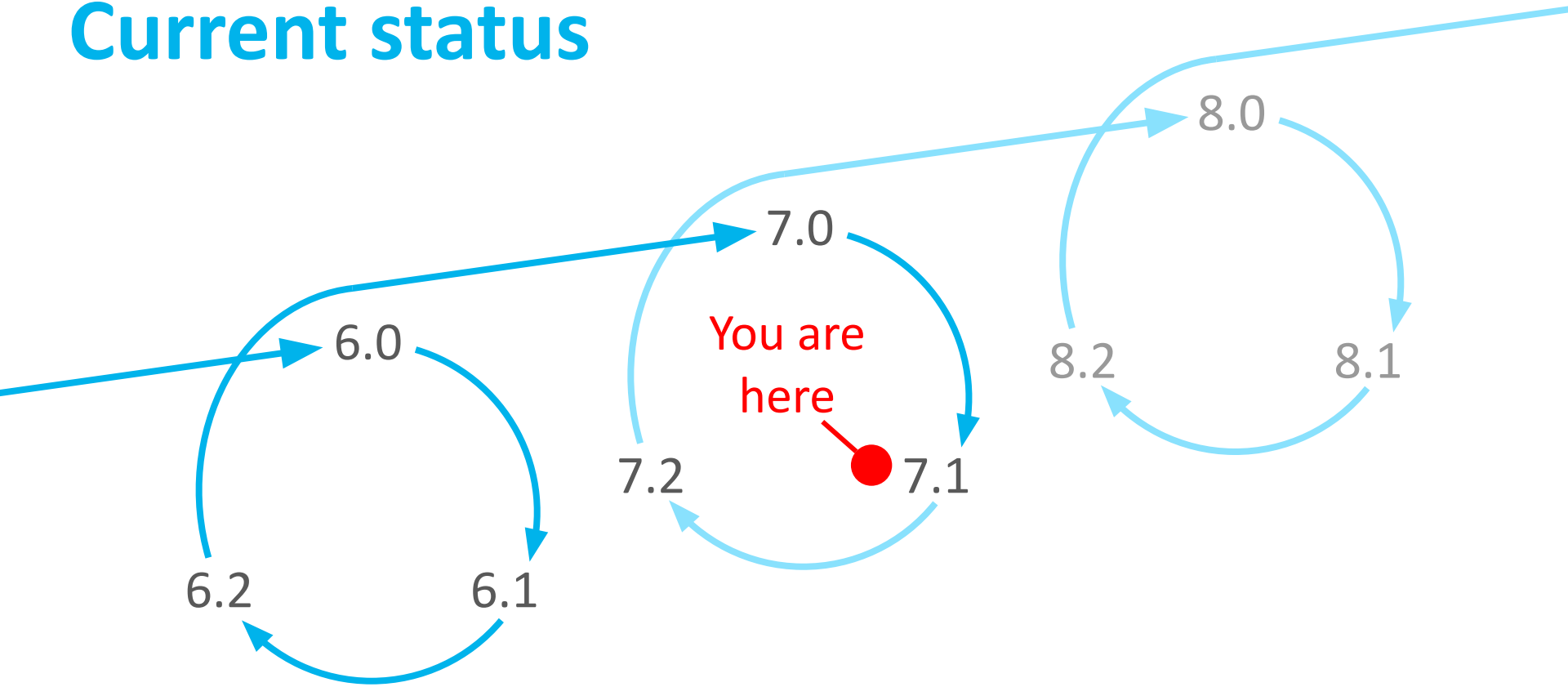
christian@zeek.org

Release cadence

Three feature releases per year



Current status



https://github.com/zeek/zeek/wiki/Release-Cadence

Zeek 6 in context

Zeek 6.0 recap (July ‘23)

- JavaScript support
- JSON ingestion
- Packet analyzer improvements
  - LLC, SNAP, Novell 802.3 support, including from VLAN analyzer
  - GRE -> Aruba handoff
  - Proper tunnel handling in 802.11
  - Start of broader Spicy adoption
- Full multi-logger text-logging support
- Event metadata support
- Native Community ID support
- Spicy troubleshooting support and proper integration (no more Spicy plugin)
- Out-of-the-box support for private address ranges
- Telemetry framework expansion and tunability

Themes:
Infrastructure
Usability

Zeek 6.1 recap (Oct ’23)

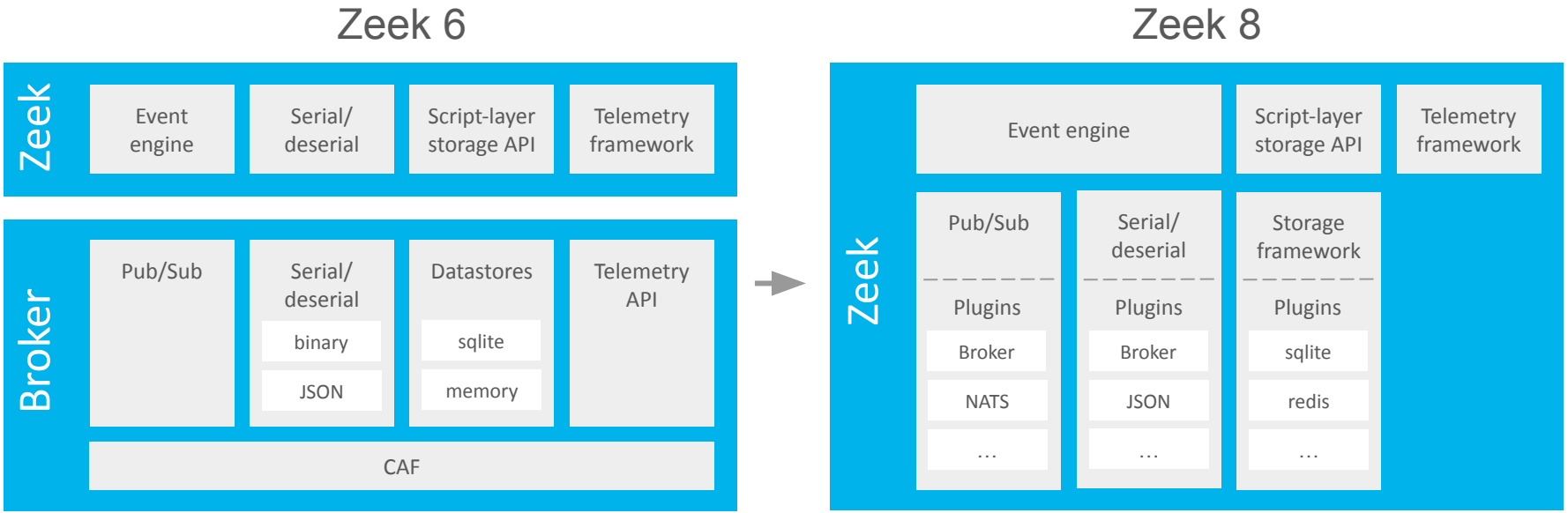
- LDAP and QUIC analyzers (both using Spicy)
- Modbus analyzer expansion
- DLT_PPP packet analyzer
- Language improvements
  - `assert()`, `&default_insert`, set/vector casts, namespacing
- JSON ingestion improvements (normalization callbacks)

Themes:
Infrastructure
Usability
Performance

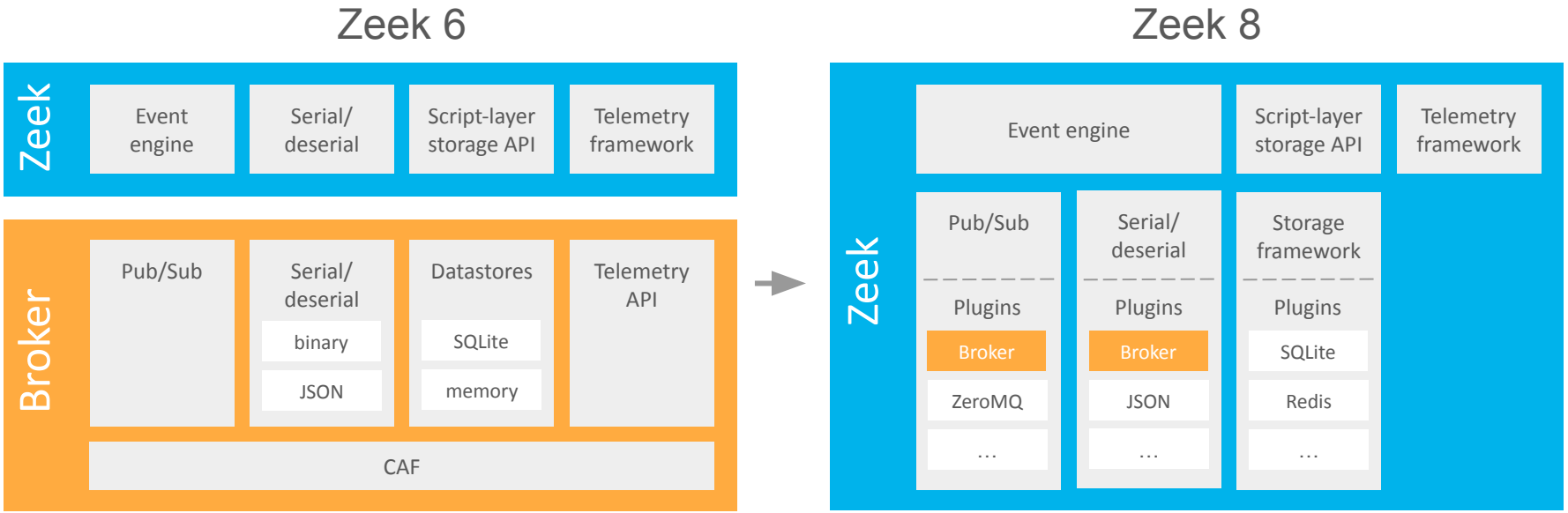
Behind the scenes:

- Broker revamp begins
  - Separation of telemetry and storage functionality into Zeek proper
  - Refocusing on pub/sub to prepare for off-the-shelf comparisons
- CI-driven performance analysis (“zeek-benchmarker”)
  - Macro/micro benchmarks for a range of scenarios

Zeek 6 -> Zeek 8 architectural revamp



Zeek 6 -> Zeek 8 architectural revamp



Zeek 6.2 (March ‘24)

- SMTP BDAT support
- GRE-over-UDP support
- HTTP protocol upgrade support & WebSocket analysis
  - BinPAC and Spicy implementation
- QUIC analyzer improvements
- Efficient support for matching strings on `table[pattern]`
- Delayed log writes
- “X” in the conn history indicates exceeded thresholds
- `Intel::seen_policy` hook to intercept `Intel::seen behavior`

Behind the scenes:

- Broker revamp continues
  - Hurdles in the C++ OpenTelemetry code

Themes:
Infrastructure
Usability

Zeek 7 and beyond

Zeek 7.0 (Aug ‘24)

- New Telemetry framework
  - Based on Prometheus and service discovery
  - No longer dependent on Broker
- Spicy 1.11
  - Compiler speedups
  - Improved correctness and error reporting
  - Better resynchronization
- ZAM, the Zeek Abstract Machine, officially supported
- Lots of performance improvements
- Language features: `delete` on tables/sets/vectors, helper BiFs

Themes:
Infrastructure
Usability
Performance

Behind the scenes:

- Storage framework development begins

Zeek 7.1 (Jan ‘25)

- Packet analyzer improvements
  - New Postgres analyzer
  - LDAP, MySQL, DNS hardening and expansion
- First round of pluggable backend work landed
  - Experimental ZeroMQ backend
- Controllable Broker buffer sizing & backpressure
- Expanded operational metrics in telemetry
- IP protocol logging in conn.log
- Spicy 1.12: conditional unit fields, improved error handling, faster compilation

Themes:
Infrastructure
Usability

Behind the scenes:

- Storage framework development continues, lots of sync/async iteration

Zeek 7.2 roadmap (~April ‘25)

- New storage framework lands
  - SQLite & Redis backends, NATs prototype, all pluggable
- Expanded cluster backend infrastructure
  - New WebSocket support
  - Additional refactoring of Broker
- DPD analyzer detachment/logging improvements
  - Configurable updates to analyzer.log, log analyzer history
  - conn.log service confirmation/violation logging
  - dpd.log deprecation
- Add log schema tooling
- zkg usability improvements — UX, bundles, tidiness

Themes:
Infrastructure
Usability

Zeek 8 roadmap (~Aug ‘25)

- New frameworks & infrastructure mature
- Bugfix / maintenance release
- Documentation push
- Resume cluster management improvements 🤞

Themes:
Infrastructure
Usability

There's a lot more — check our release notes for new, changed, deprecated, and removed functionality, and follow our blog for release updates.

Also, a huge thank you to our contributors! 🙏

Thanks!

Documentation

https://docs.zeek.org

Community links

https://zeek.org/community

Github project

https://github.com/zeek

Project wiki

https://github.com/zeek/zeek/wiki