The State of Zeek

February 2025

Christian Kreibich
christian@zeek.org

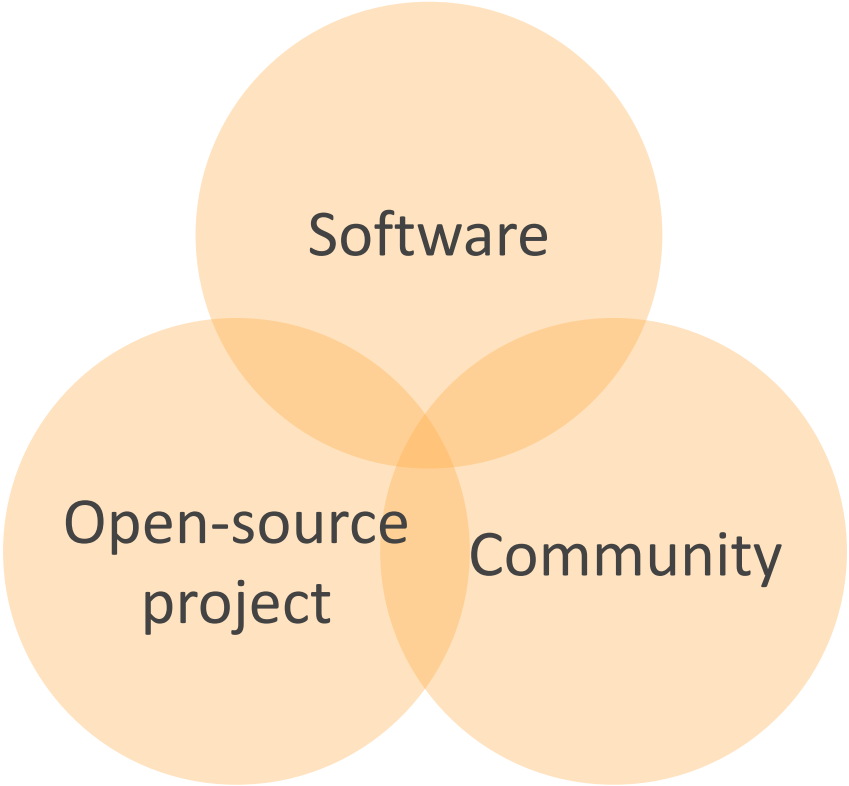
Hi, I’m Christian

Zeek project tech lead

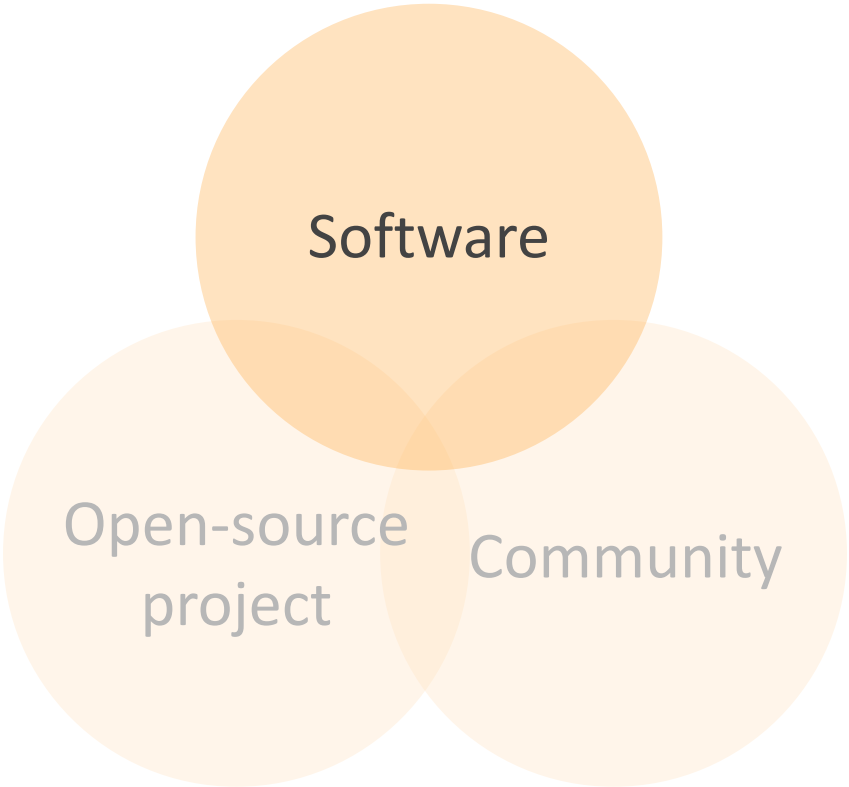
Recovering academic

I work at Corelight

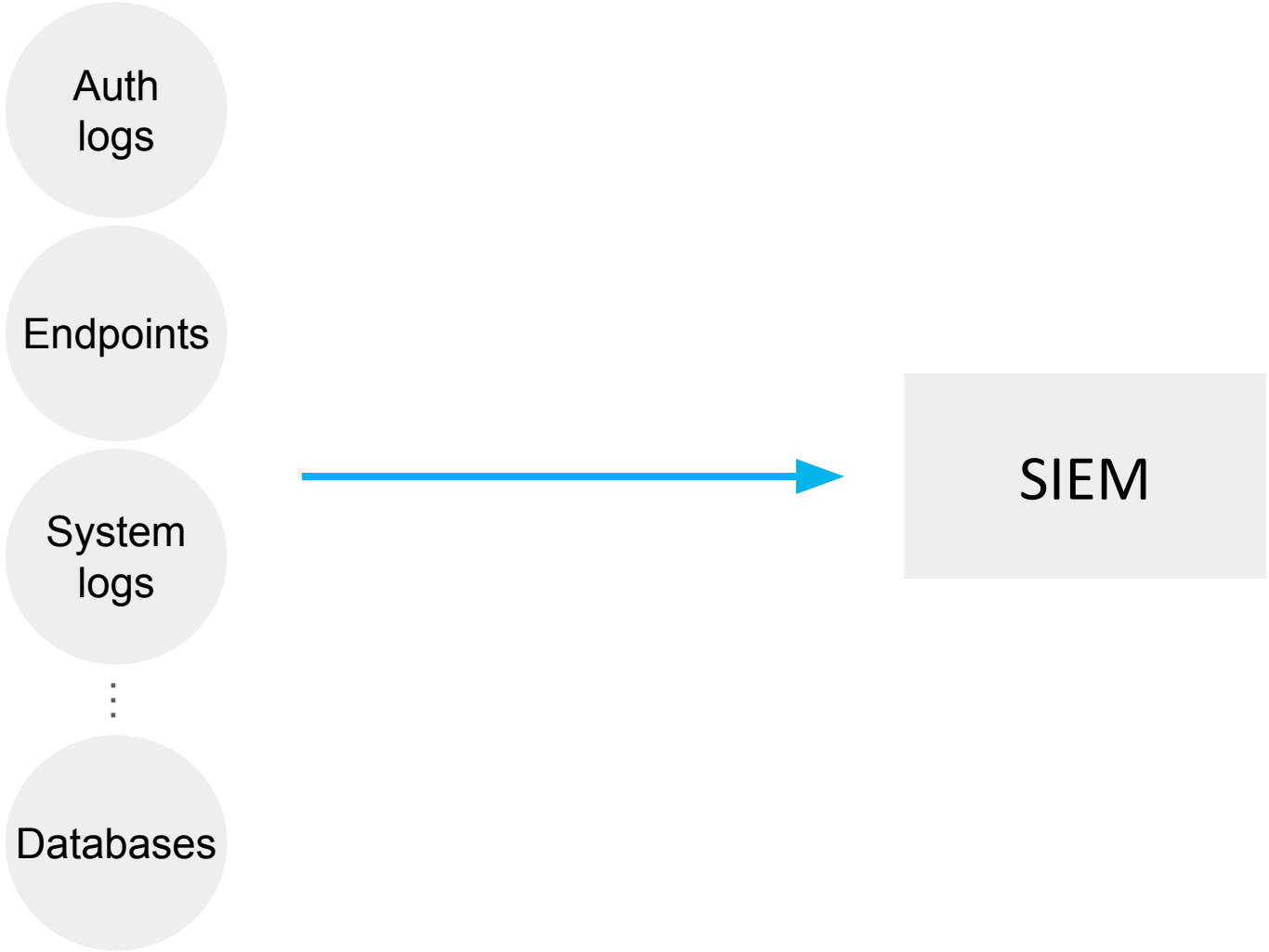
Zeek is many things …

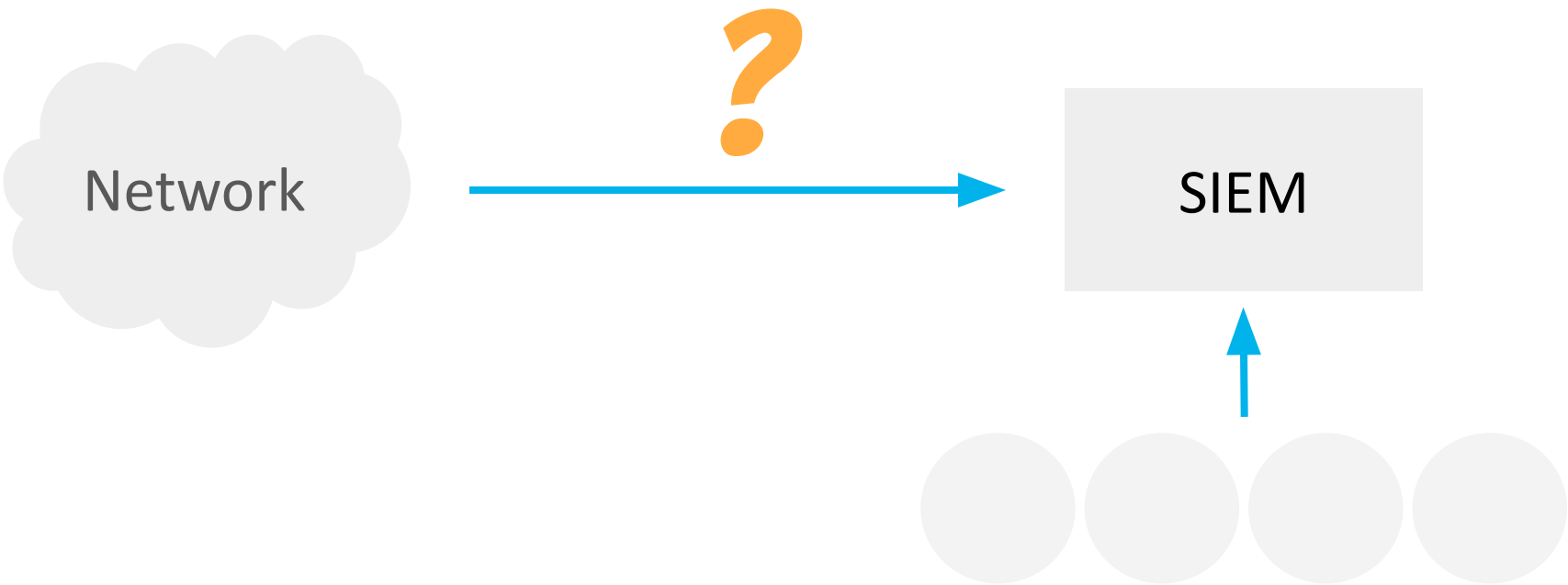


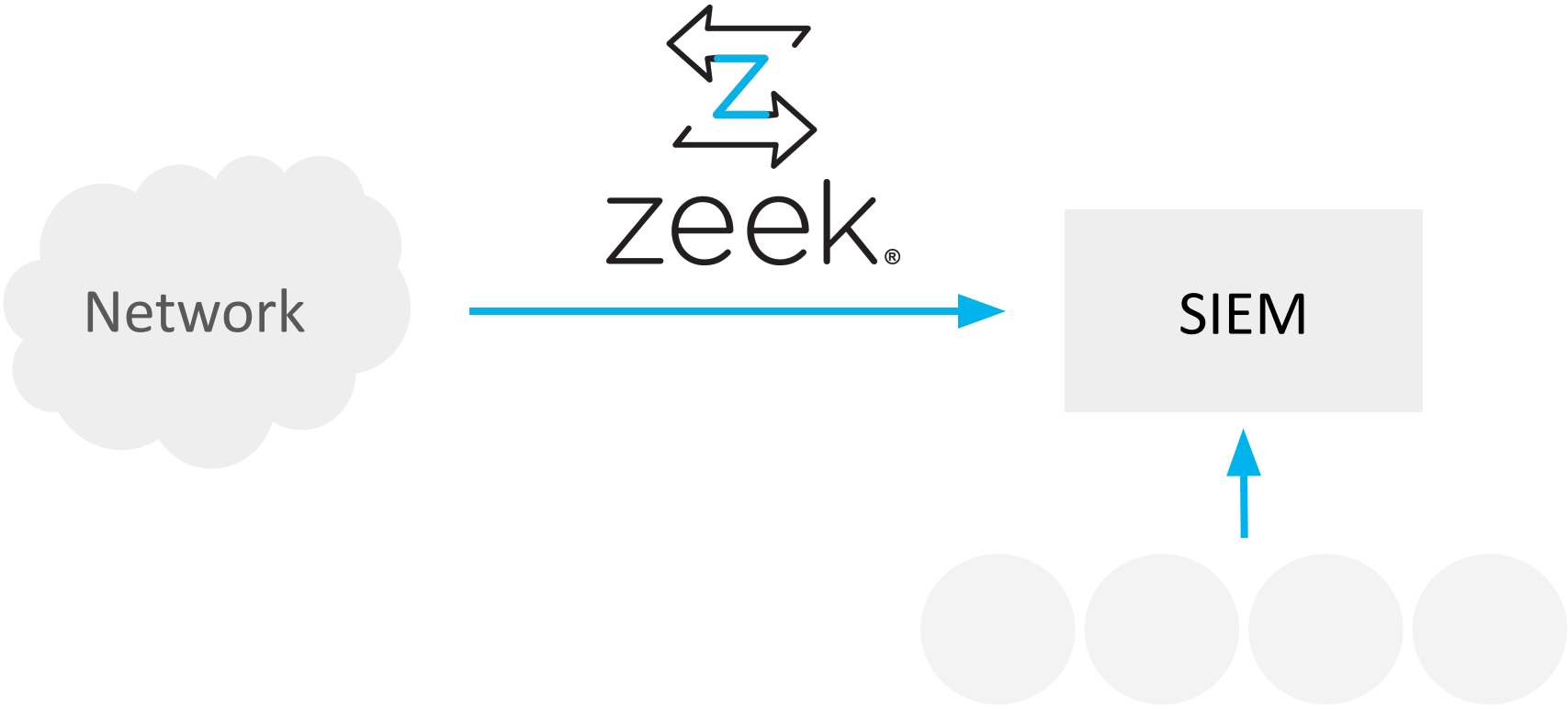
... I'll largely focus on our code.



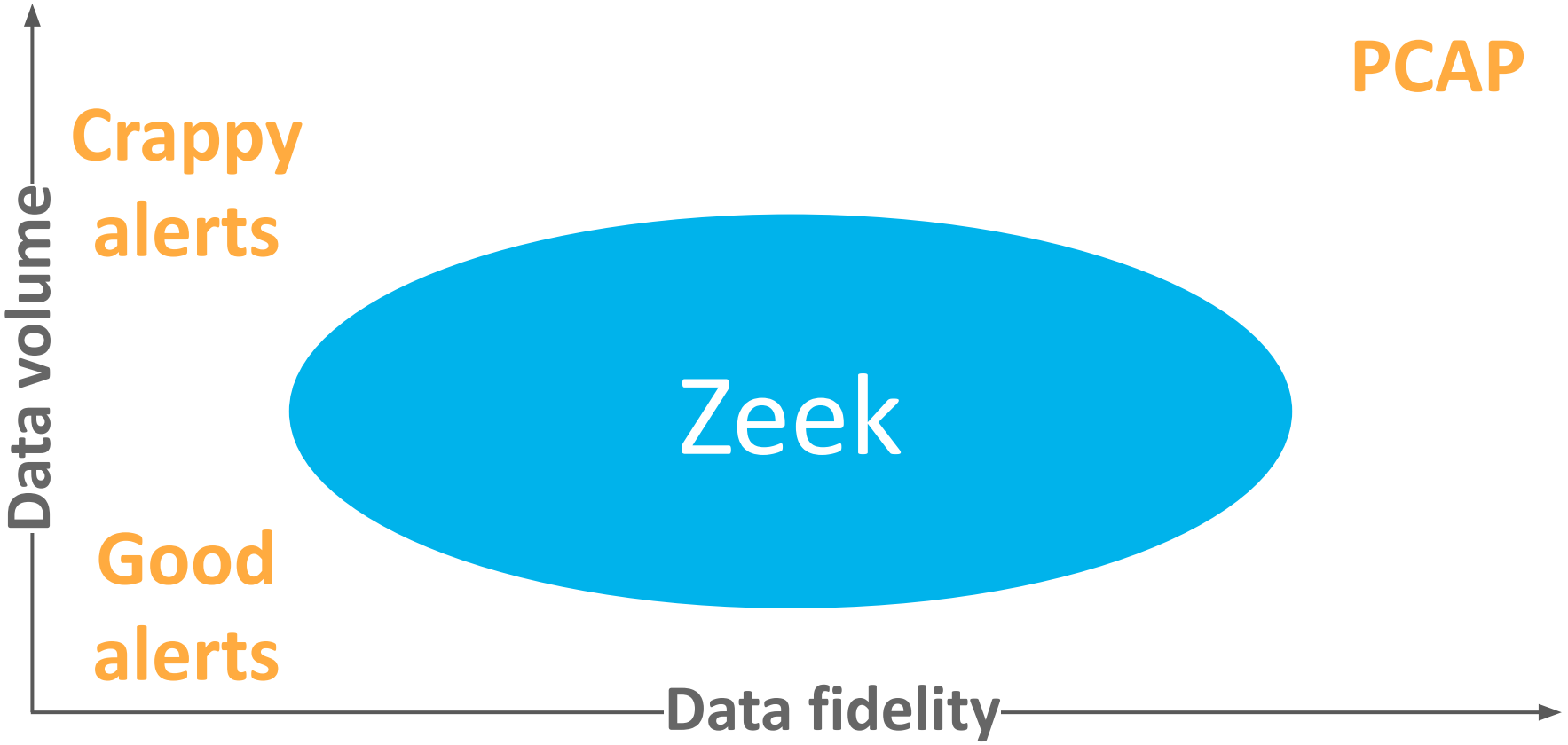
So, what is Zeek?


Auth logs
Endpoints
System logs
Databases
SIEM


Network
?
SIEM


Network
zeek®
SIEM

Better network data




zeek
NETWORK
FLIGHT
RECORDER

Threat Hunting & Incident Response	Threat Detection	Monitoring & Operations
Pivot into PCAP files via Zeek's event timestamps.	Detect lateral movement by illuminating suspicious east-west traffic.	Monitor self-signed, expired, or soon-to-expire, SSL certs via Zeek's ssl.log
Verify containment by doing post-breach traffic monitoring.	Detect ransomware by monitoring unusual file entropy increases (i.e. encryption)	Flag unencrypted email transmissions via Zeek's smtp.log
Reduce alert backlogs by finding and filtering out false positives.	Detect common network services running on non-standard ports.	Inventory network-connected devices & software without installing host agents.
Identify all hosts that downloaded a malware file via Zeek's files.log.	Detect beaconing activity by streaming Zeek logs to Real Intelligence Analytics (RITA).	Monitor the use of Russian character set keyboards in your environment via Zeek's rdp.log.

We enable defenders:

Solid network evidence

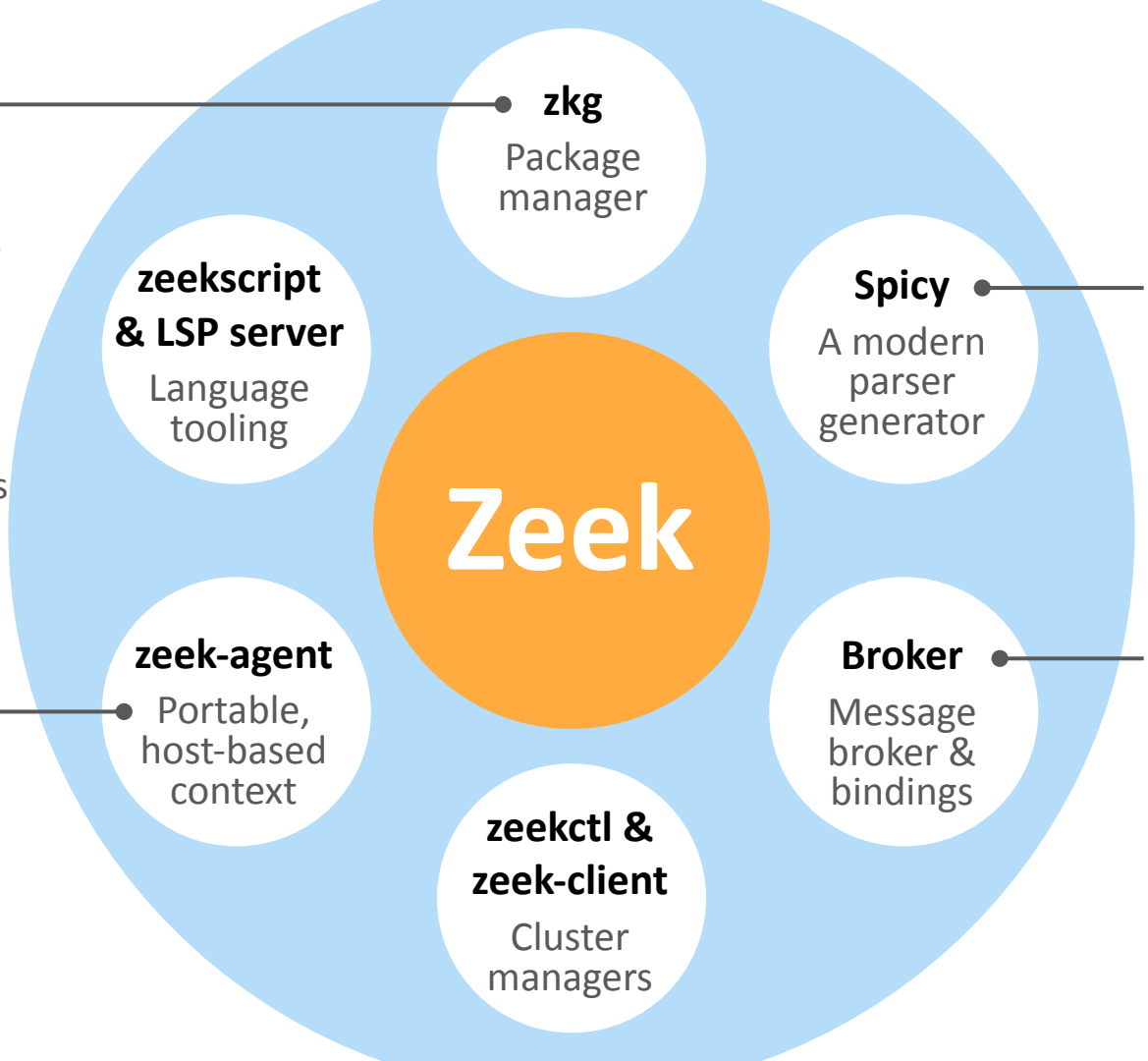
Powerful toolchain

Pervasive extensibility

We ~~do not~~ RARELY build detections.

The state of **what Zeek does**:

What are we ***really*** building? And ***how***?



- 240+ packages
- NIC support
- Log writers
- Functional add-ons
  - Log extensions
  - Storage I/O
  - File extraction
- Protocol analyzers
  - ICS, QUIC, VPNs, …
- Behavioral analyses
- Detections
  - Two dozen+ CVEs since 2020

- Zeek eventing for host-based activity
  - Processes, open sockets, users, …
- Linux, Mac & Windows

- DSL for syntax & semantics of protocols
- Compiles to C++
- Designed for streamed data
- Not tied to Zeek

- Topic-based pub/sub
- Telemetry & storage
- WebSocket layer
- Python & Go bindings

That's a lot.

Meet the main Zeek developers

Meet the main Zeek developers

Arne Welzel

Tim Wojtulewicz

Benjamin Bannier

Robin Sommer

Christian Kreibich

Johanna Amann

Evan Typanski

Dominik Charousset

That's ~~a lot~~.

TOO MUCH

Microsoft's Port of Zeek for Windows 🎉🪟 #2518

Merged **timwoj** merged 72 commits into `zeek:master` from `microsoft:master` on Nov 11, 2022

Conversation 56 Commits 72 Checks 31 Files changed 84

voidbar commented on Oct 31, 2022 • edited Contributor

This is Microsoft's Port and Adaptations of Zeek for Windows 🪟.
Using these changes, one can compile Zeek natively on a windows machine using MSVC and then run the resulting executable.

After brewing this for over a year, spending countless developer hours, and cooperating with the Corelight team, we are excited to share with the community our fruits of labor.
Also, big thanks to Brim as some of their initial contributions helped us bootstrap our own.

Accompanied to this PR, there are numerous submodules that have already been adated to Windows and already pushed to upstream:

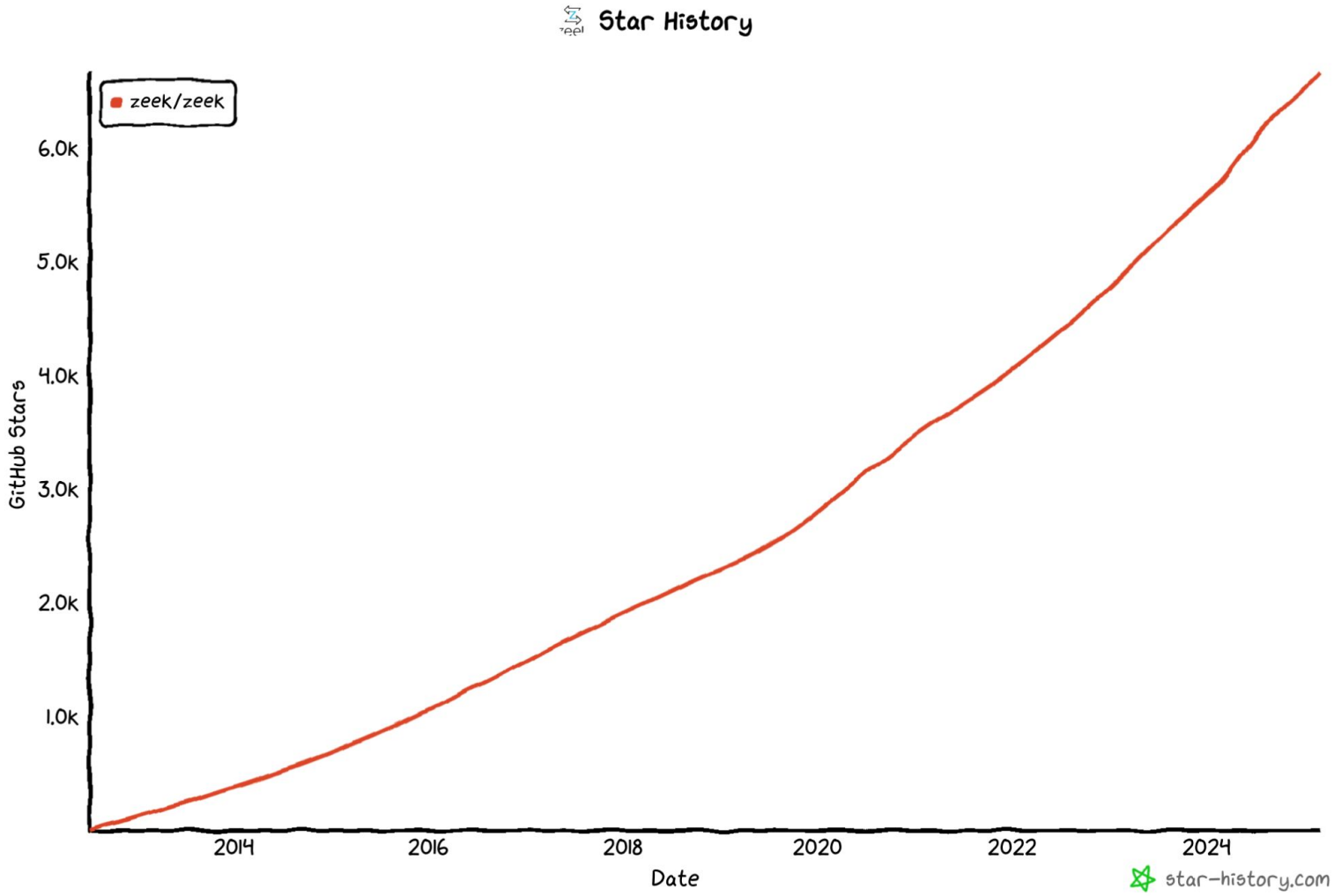
- CMake: **Added support to MSVC compiler under Windows** cmake#49
- Paraglob: **Adapted paraglob to compile with MSVC for windows environment.** paraglob#21

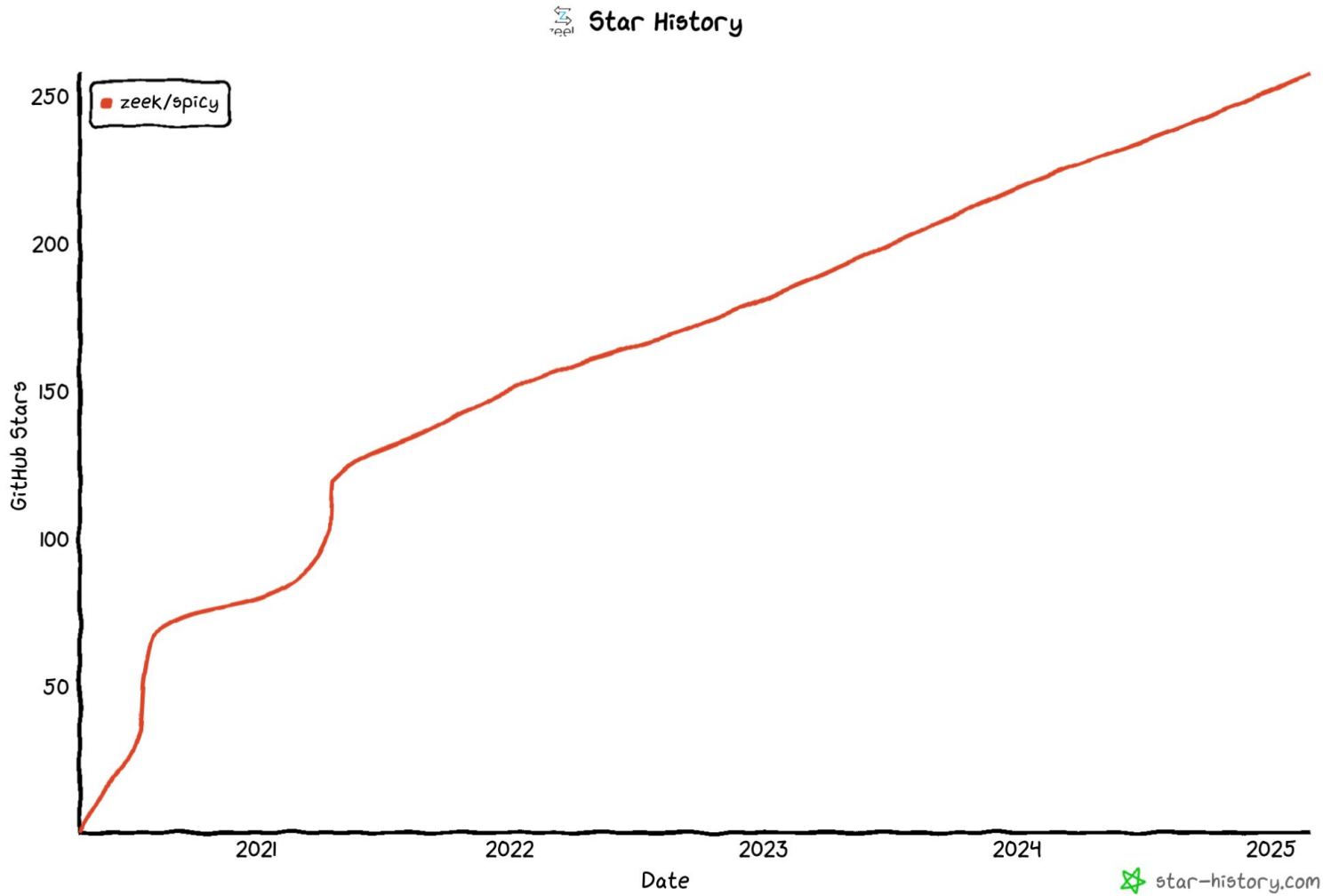
Seeking Windows contributors

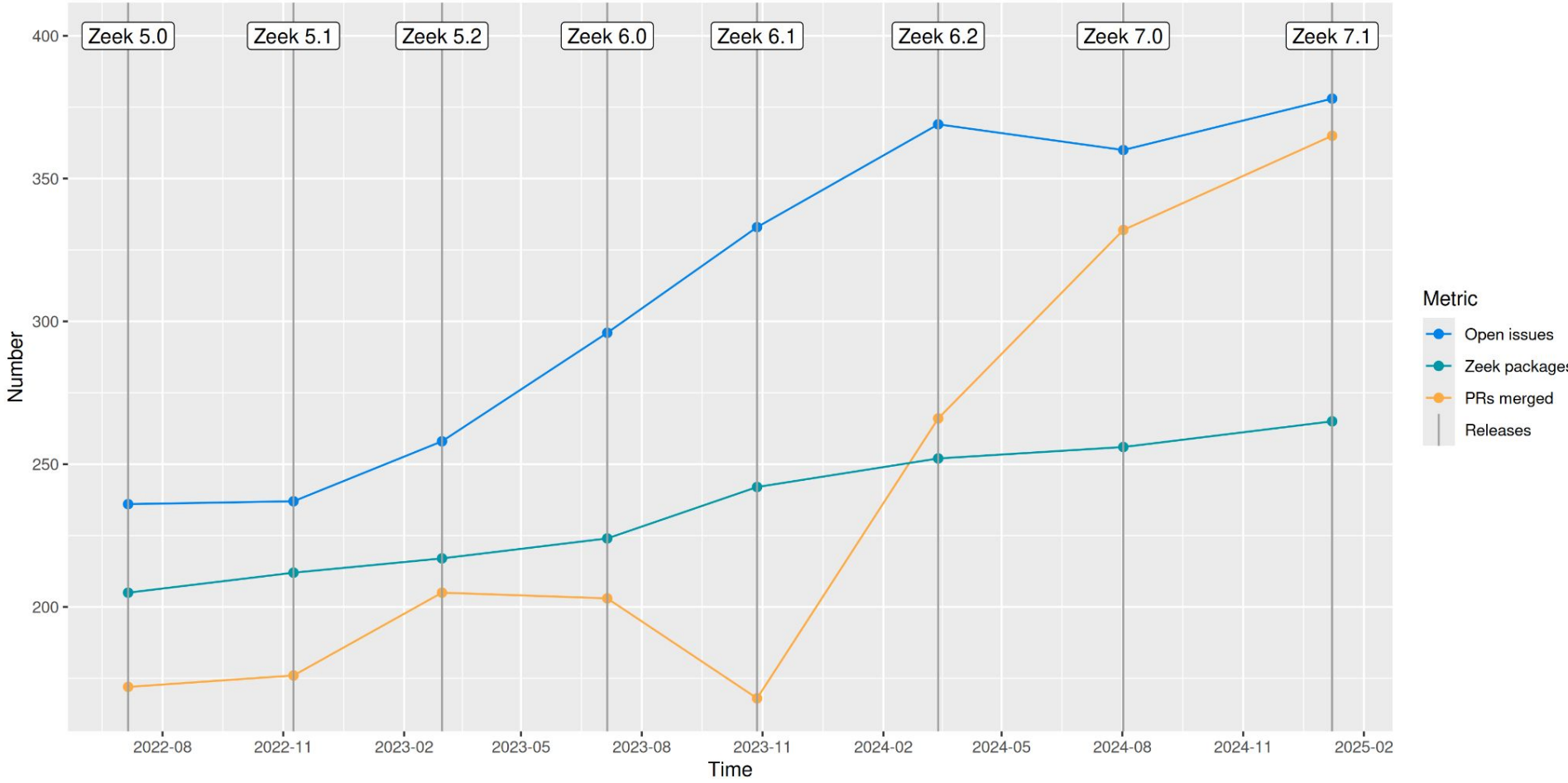
by Christian Kreibich | Feb 20, 2024 | community, development, infrastructure, open-source, Windows, Zeek

Since we announced experimental Windows support in 2022, we've received a slow but constant influx of bug reports and support requests for this platform. Over the past months our workload has increased substantially, for reasons that we're very happy about: Spicy has attracted a lot of attention, we're deep in a refactoring effort that restructures the boundary of Zeek and Broker, several new protocol analyzers have landed in Zeek, and our community's engagement on Slack and Discourse has grown as well. The downside of this increased activity is that our small team can no longer keep up on all fronts, and areas that aren't central to our focus are falling behind.

Windows support is one of these areas. So today we're asking for your help: if you're a Windows developer eager to improve Zeek, please get in touch. There's a growing backlog of Windows issues that we cannot currently take on. You don't need to be a networking wizard to contribute to Zeek: most of the open issues simply require close familiarity with Windows, which we lack. Some of the work also straddles projects; for example, we've hit several interesting issues in libkqueue that need addressing.


Star History
zeek/zeek
6.0k
5.0k
4.0k
3.0k
2.0k
1.0k
GitHub Stars
2014
2016
2018
2020
2022
2024
Date
star-history.com


Star History
zeek/spicy
250
200
150
100
50
GitHub Stars
2021
2022
2023
2024
2025
Date
star-history.com


Zeek 5.0
Zeek 5.1
Zeek 5.2
Zeek 6.0
Zeek 6.1
Zeek 6.2
Zeek 7.0
Zeek 7.1
400
350
300
250
200
Number
2022-08
2022-11
2023-02
2023-05
2023-08
2023-11
2024-02
2024-05
2024-08
2024-11
2025-02
Time
Metric
Open issues
Zeek packages
PRs merged
Releases

The state of **what and how we build**:

Beyond ***building stuff***

Research

Engineering

Product Management

Customer Support

Marketing / Outreach

Research

Engineering

Product Management

Customer Support

Marketing / Outreach

Research

Engineering

Product Management

Customer Support

Marketing / Outreach

Research

Engineering

Product Management

Customer Support

Marketing / Outreach

The State of **Zeek's engineering organization**:

We need you!

This is an exciting time for Zeek.
This community is unique.
Tell us what is good, and what is not.
If you cannot tell us, tell us that. :-)

Share feedback

- 🍪 Tell us your use cases
- 🍪 File new GitHub issues — don't be shy
- 🍪 Comment on existing ones, PRs, proposals, Slack threads
- 🍪 Speak up on Discourse or start a GitHub Discussion

Contribute code

- 🍪 See our GitHub Wiki for processes & contribution guide
- 🍪 Find tickets to work on (“good first issue” tag), or just ask
- 🍪 Have larger ideas? Sync up early and we’ll help guide

Not a coder? Not a problem!

- 🍪 Help other users
- 🍪 Help test! We need more live testing environments
- 🍪 Help the documentation & training teams

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