RSAConference2021
May 17 – 20 | Virtual Experience

SESSION ID: **TECH-W16**

Beyond endpoint security using osquery at scale

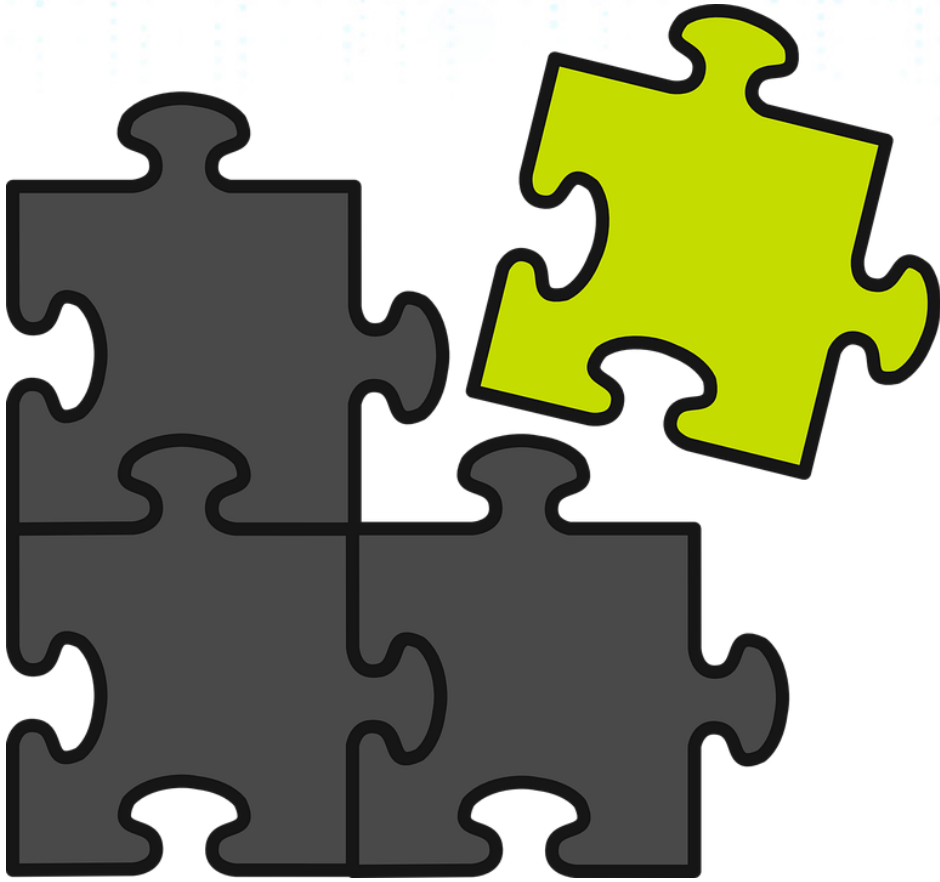
Prateek Kumar Nischal
Senior Software Engineer
WM Global Tech India
@pikaynu

Prasoon Dwivedi
Staff Software Engineer
WM Global Tech India
@mitprasoon

Why endpoint security is important?

Challenges with Endpoints in an Enterprise setup

- Visibility on heterogeneous resources
- Keeping up with the trend
- Overcomplicating endpoint security
- Accountability and ownership
- Overprioritizing antimalware
- Regulatory, compliance and Policy Enforcement



RSAConference2021

Introduction to Endpoint Security

Collecting the right events is just half the solution

Endpoint Security: Requirements

- Endpoint agents
- Immutable event pipeline
- Alerting and triaging setup
- Easy and reliable extraction of information for compliance audits
- Events should be actionable and open to stakeholders

Compliance Requirements

- Detect vulnerable infrastructure
- Audit trail for every resource all the time
- Proof of integrity or detect compromised audit pipeline
- Visibility into the state of audit for a network

Infrastructure Setup for Endpoint Security

Deploy event collectors (agents) everywhere

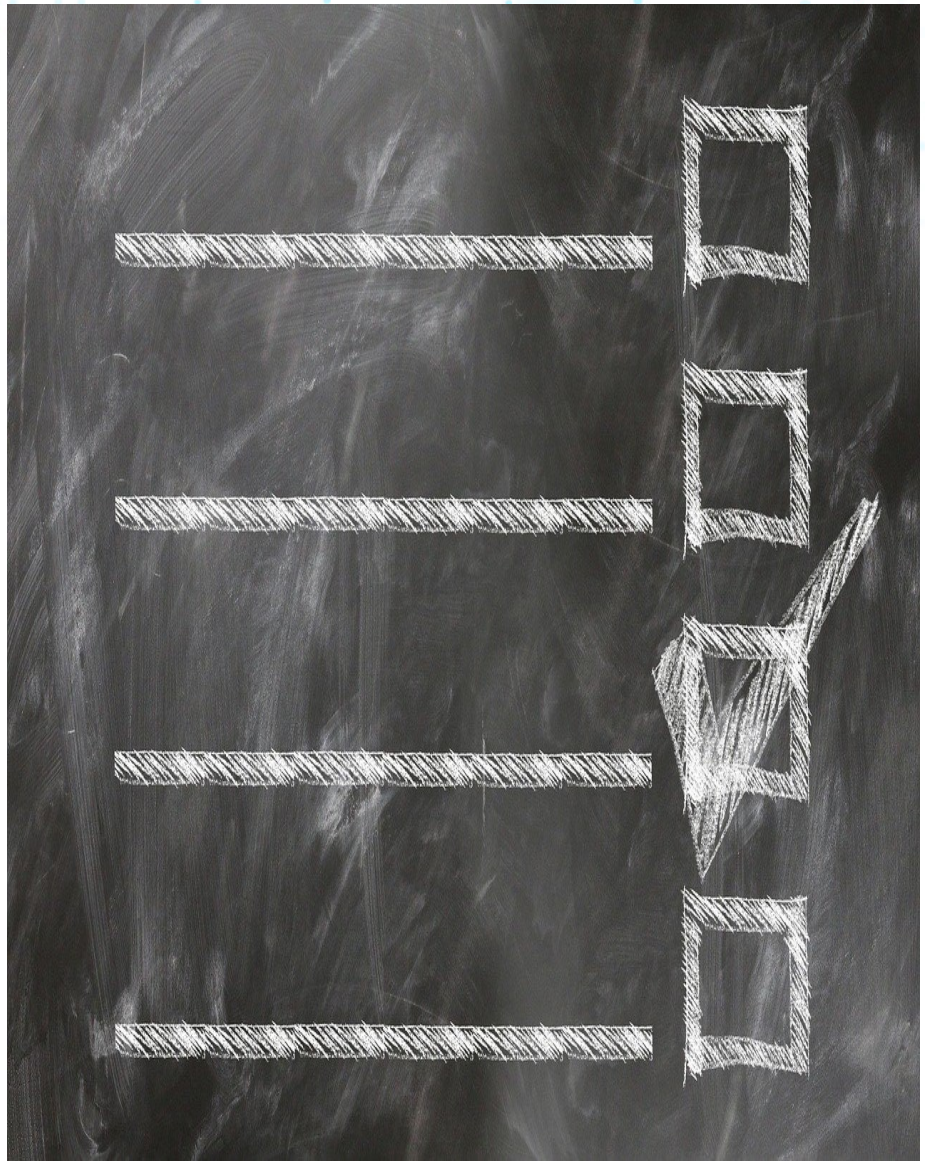
Normalize events from all agents

Setup trusted transport for events

Setup command and control server for config distribution

The Wishlist

- ✓No custom or complex deployments
- ✓Guaranteed configuration integrity
- ✓Ownership and identity tagging for faster triaging
- ✓Unified control across the agents
- ✓Native and resilient logging solution across the organization



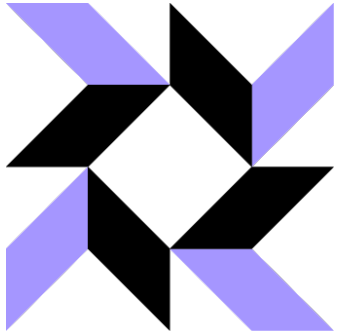
RSAConference2021

The Audit Framework

An attempt to achieve a trusted event pipeline to serve as evidence in compliance

osquery – For endpoint security

osquery by facebook



osquery is an opensource endpoint visibility tool that exposes OS events and information via a SQL interface.

osquery – For endpoint security

osquery by facebook

Why osquery?

- Implements TLS config plugin and TLS logger plugin
- Can get configuration from remote host
- Can send logs to remote endpoint
- Extremely flexible

The Audit Framework

What it does?

- The Endpoint agent(s) behavior
- Configuration build and distribution
- Integration with the Linux audit framework

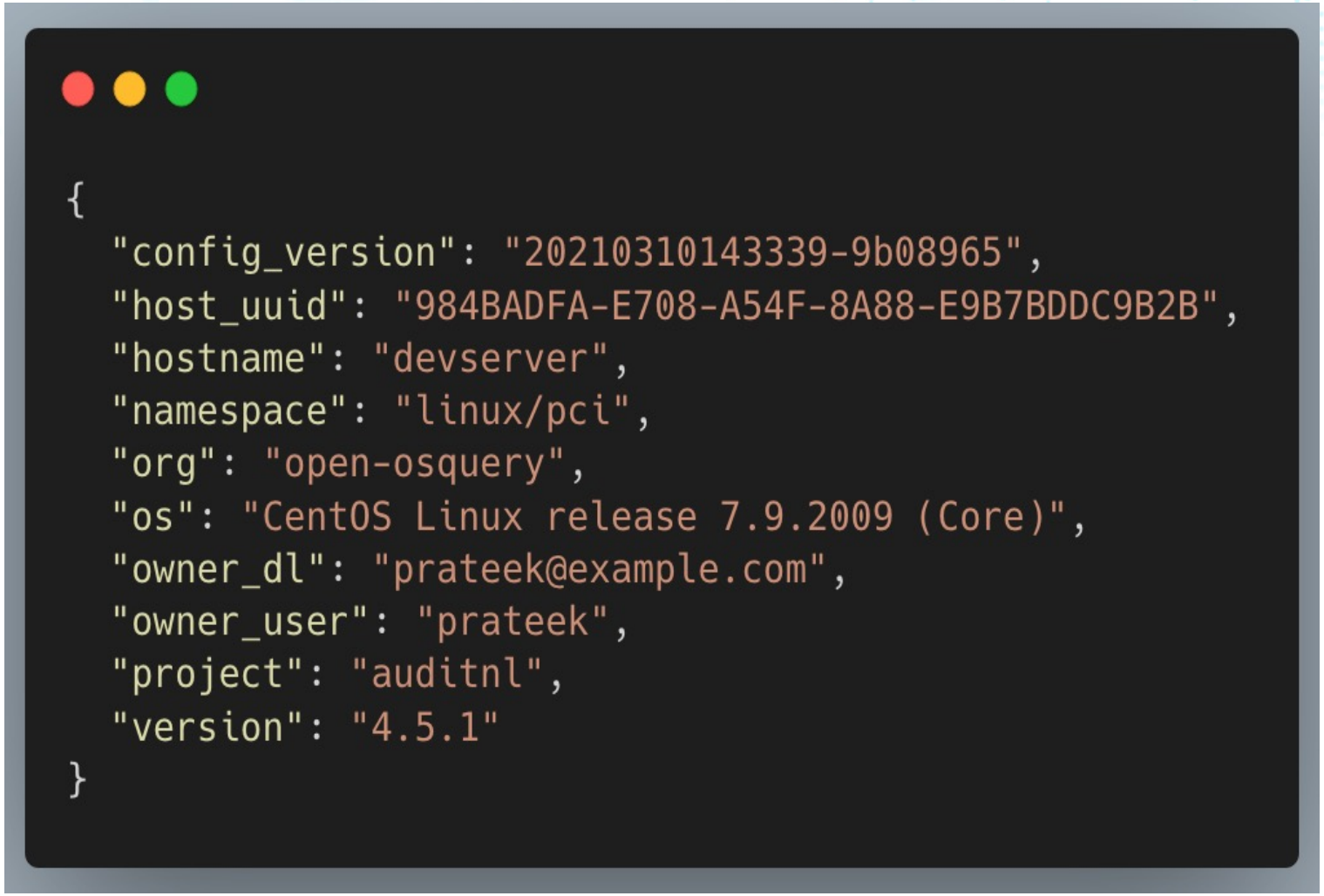
Ensure Integrity & Compliance

Monitor

- Version of the agent(s) deployed
- Integrity of the agent(s)
- Any permission changes to the agent(s)
- Uptime / heartbeat for the agent(s)
- Any config generated at runtime

Event tagging for triage and accountability

- Host Identifier, IP
- Configuration version
- Organization Segment
- Owner Group
- Owner



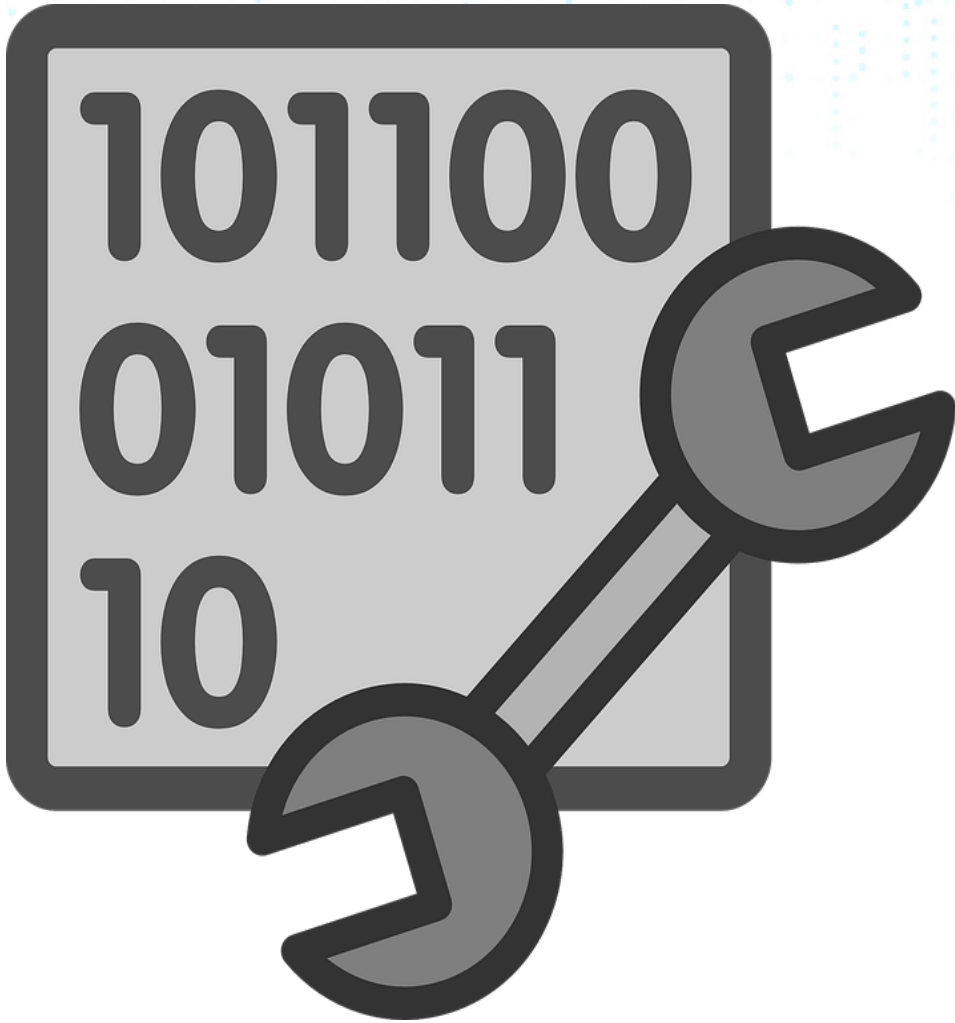
RSAConference2021

Configuration build and distribution

Perhaps one of the most important component in the pipeline

Configuration Management

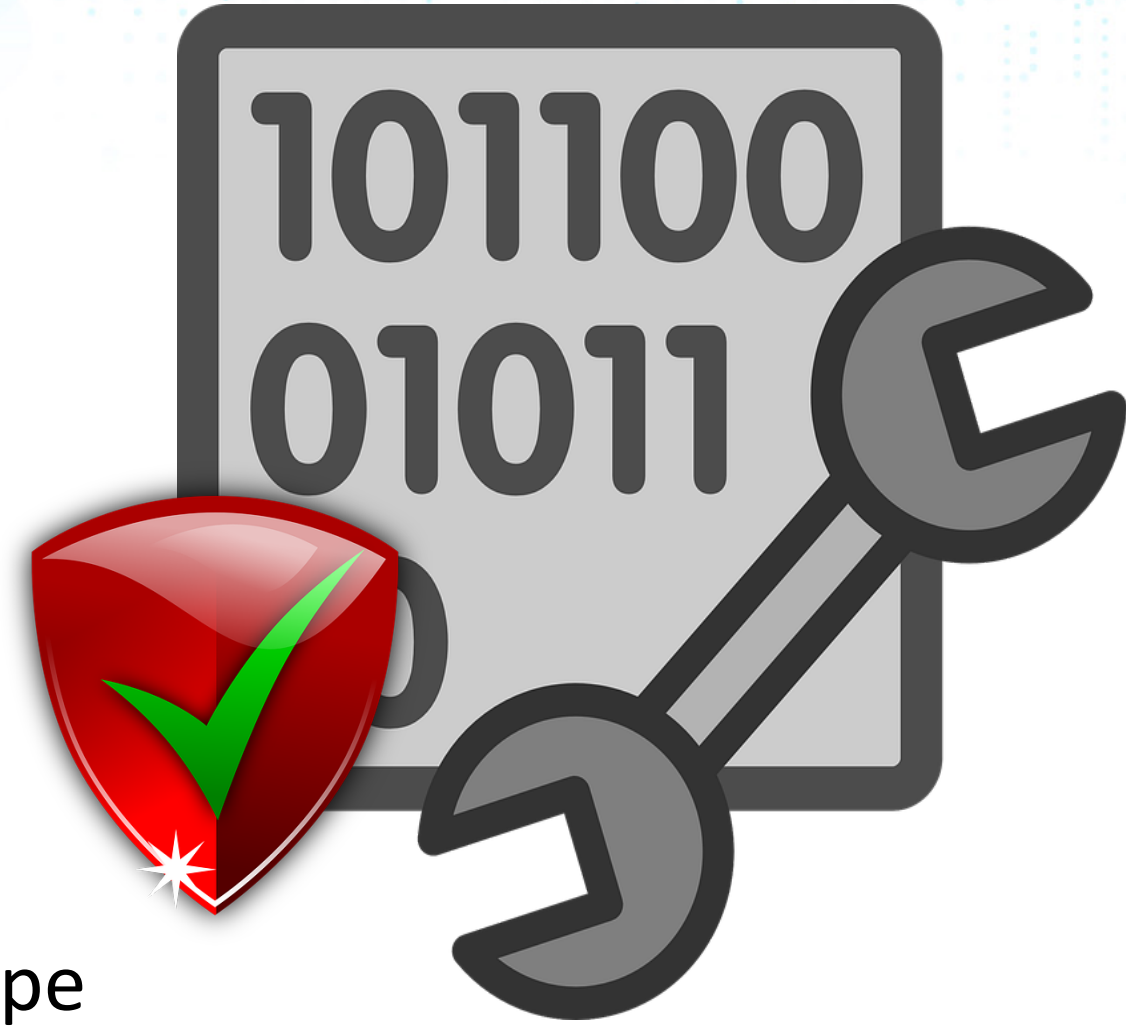
- Implement osquery's built-in TLS config plugin
- Extend the plugin to handle varied configurations not just osquery's
- Simplify bootstrap process by serving the config from a simple file server which can also extend to a full-fat API server



Configuration Management Continued…

How to ensure CIA?

- Digitally sign configuration made available through HA setup
- Trust based on PKI and x509 certs
- Custom certificate attributes
- Versioned configuration
- Metadata embedded with configuration under security envelope



Benefits of an explicitly secure configuration

- Insecure fileserver can be used out of the box
- HTTP GET based fetch enables easy integration with orchestrators
- Easy determination of state of running config through versioning
- Trust relies on CA and not on shared secret
- Self-serviced with minimal components

RSAConference2021

Integration with the Linux audit framework

Most trustworthy source of information - A beast that needs taming

Linux Audit Service

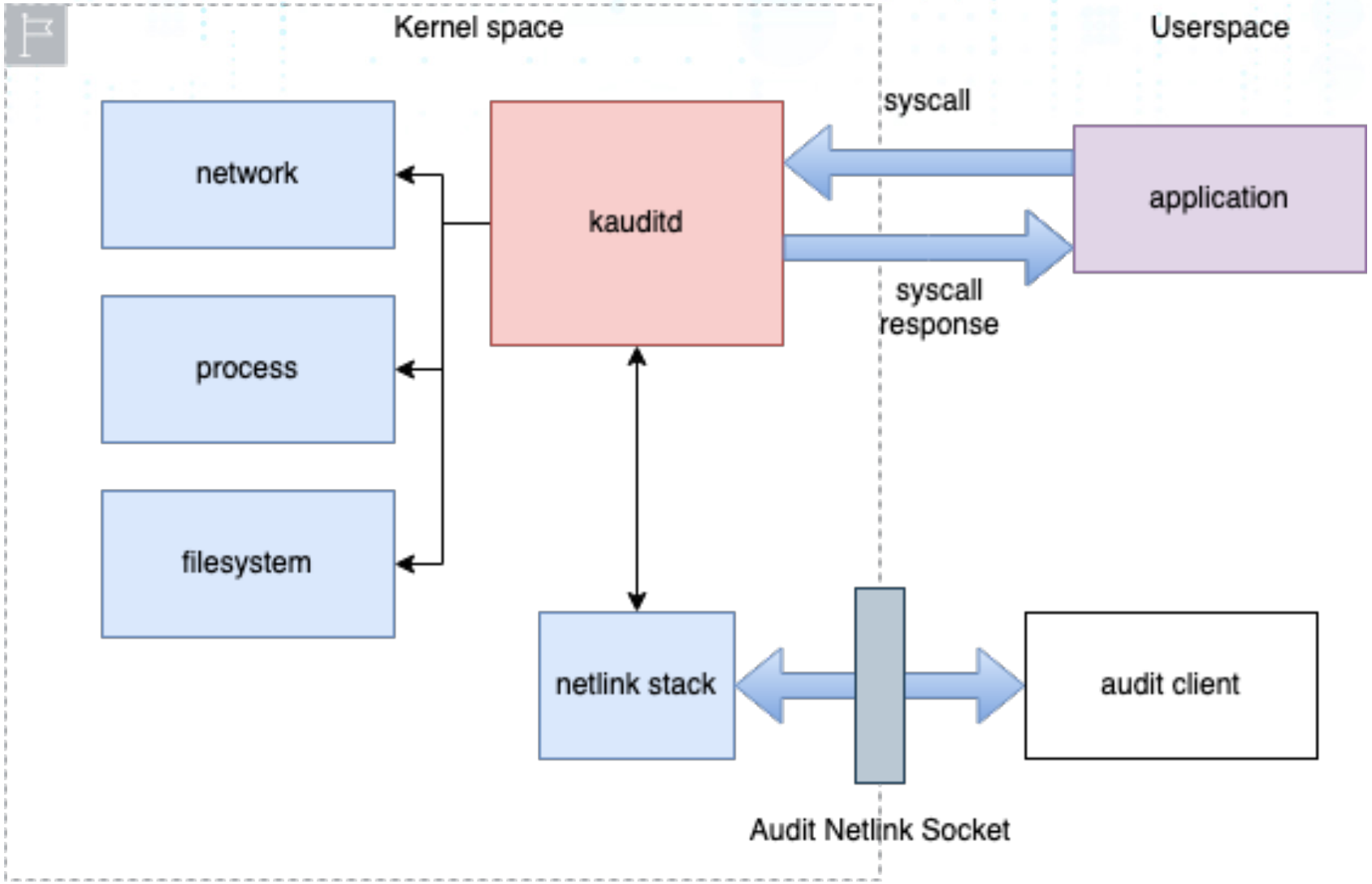
What can it do?

- Process execution and malware detection
- syscall auditing for sensitive files
- File integrity monitoring for read and write operations
- User activity
- Network activity

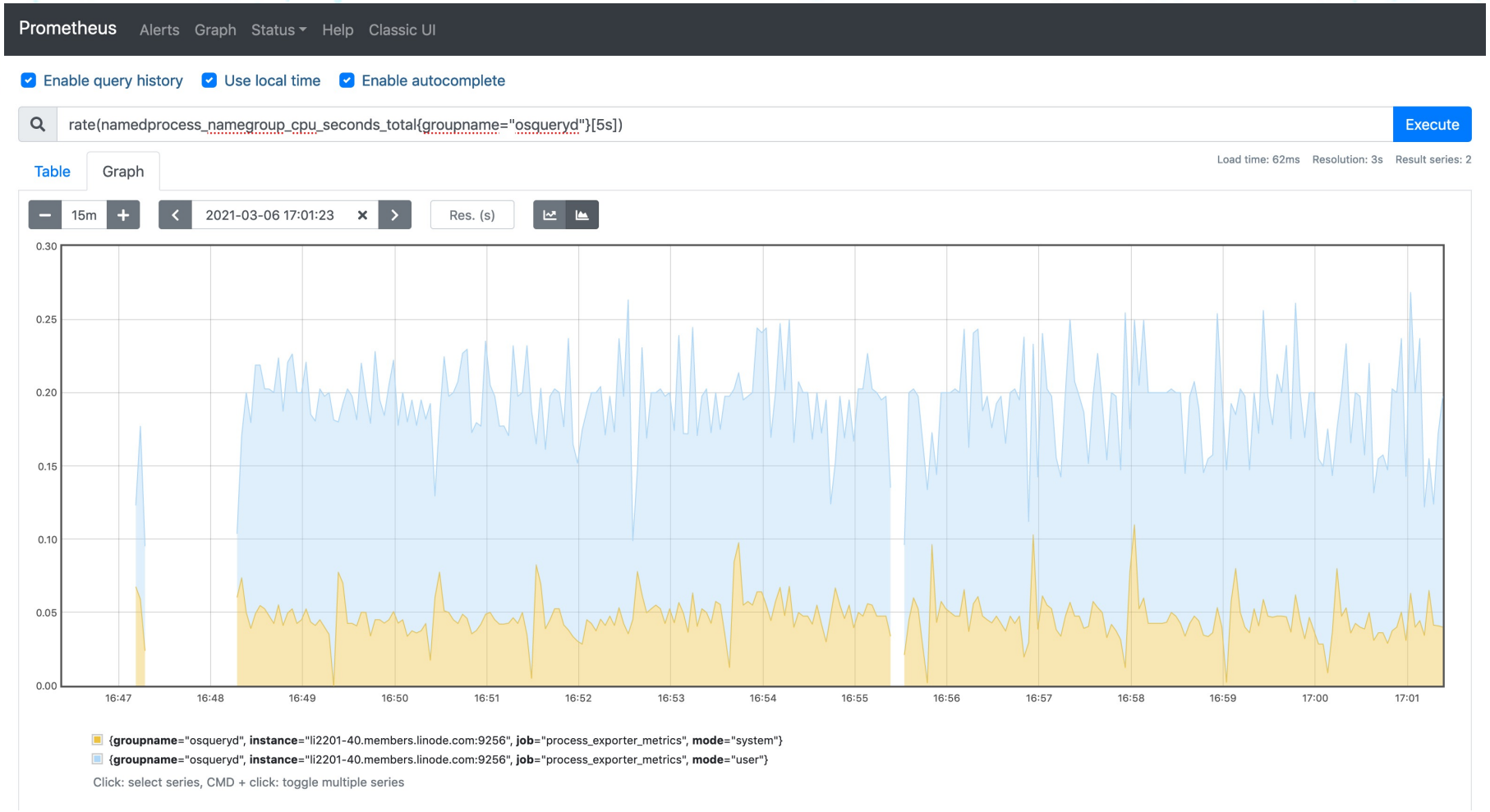
Challenges with the Linux Audit framework

- Too static, configured using auditctl(8)
- Does not support patterns and globs
- Emitted logs require post processing

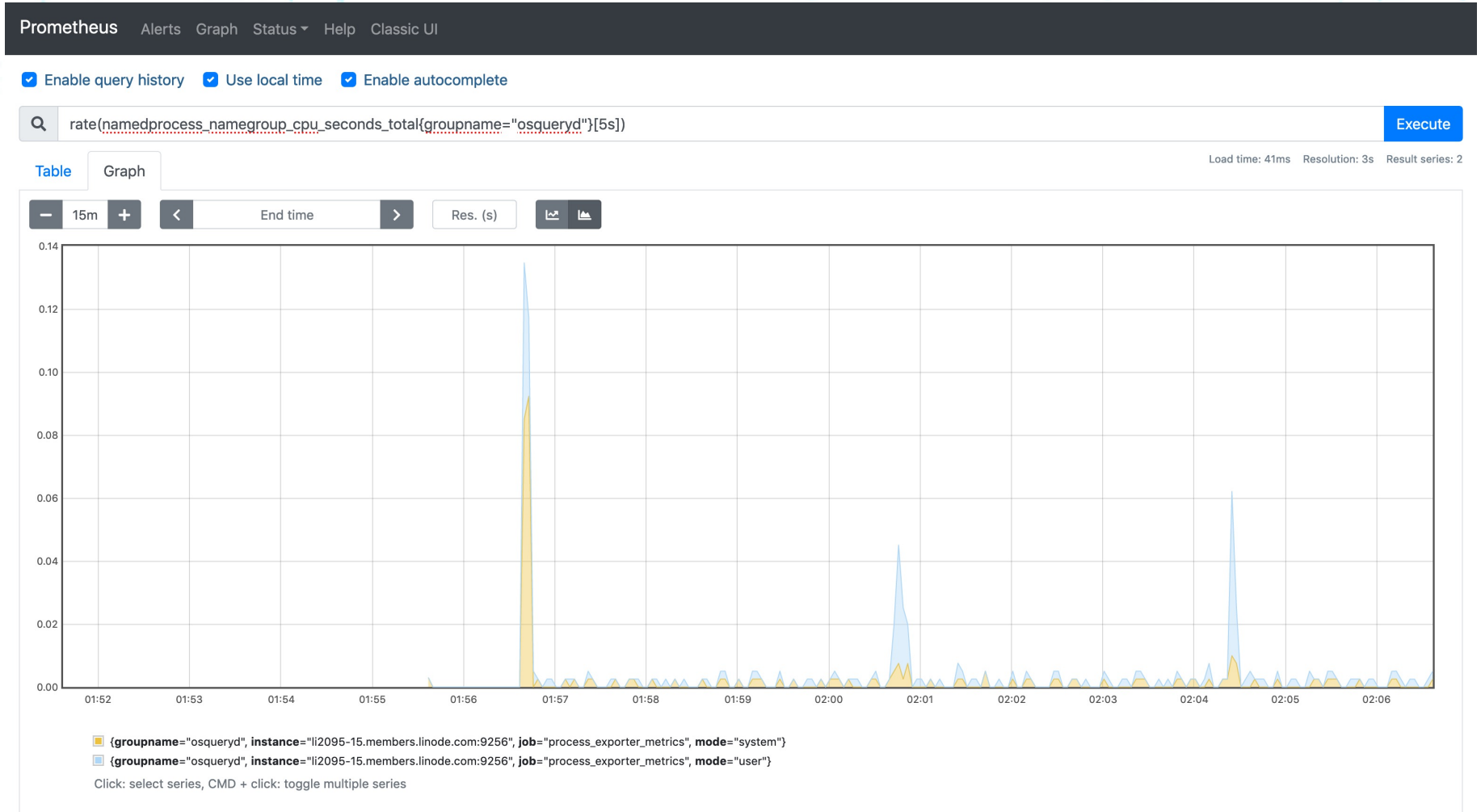
How does osquery handle audit events



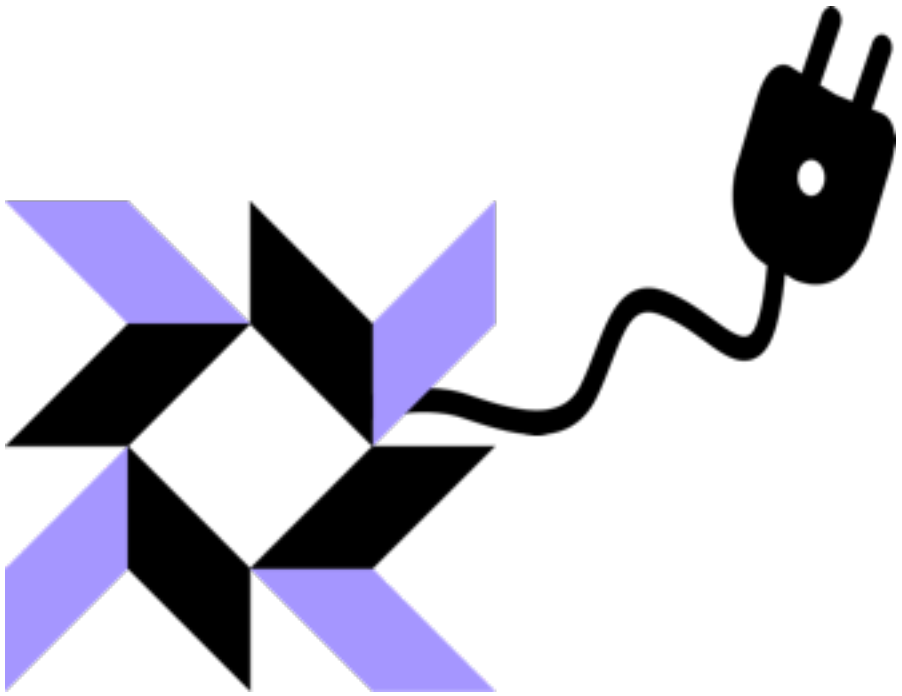
osquery performance with bulk event filtering



osquery performance assisted by Linux Audit



Extension framework for osquery



Best of both worlds

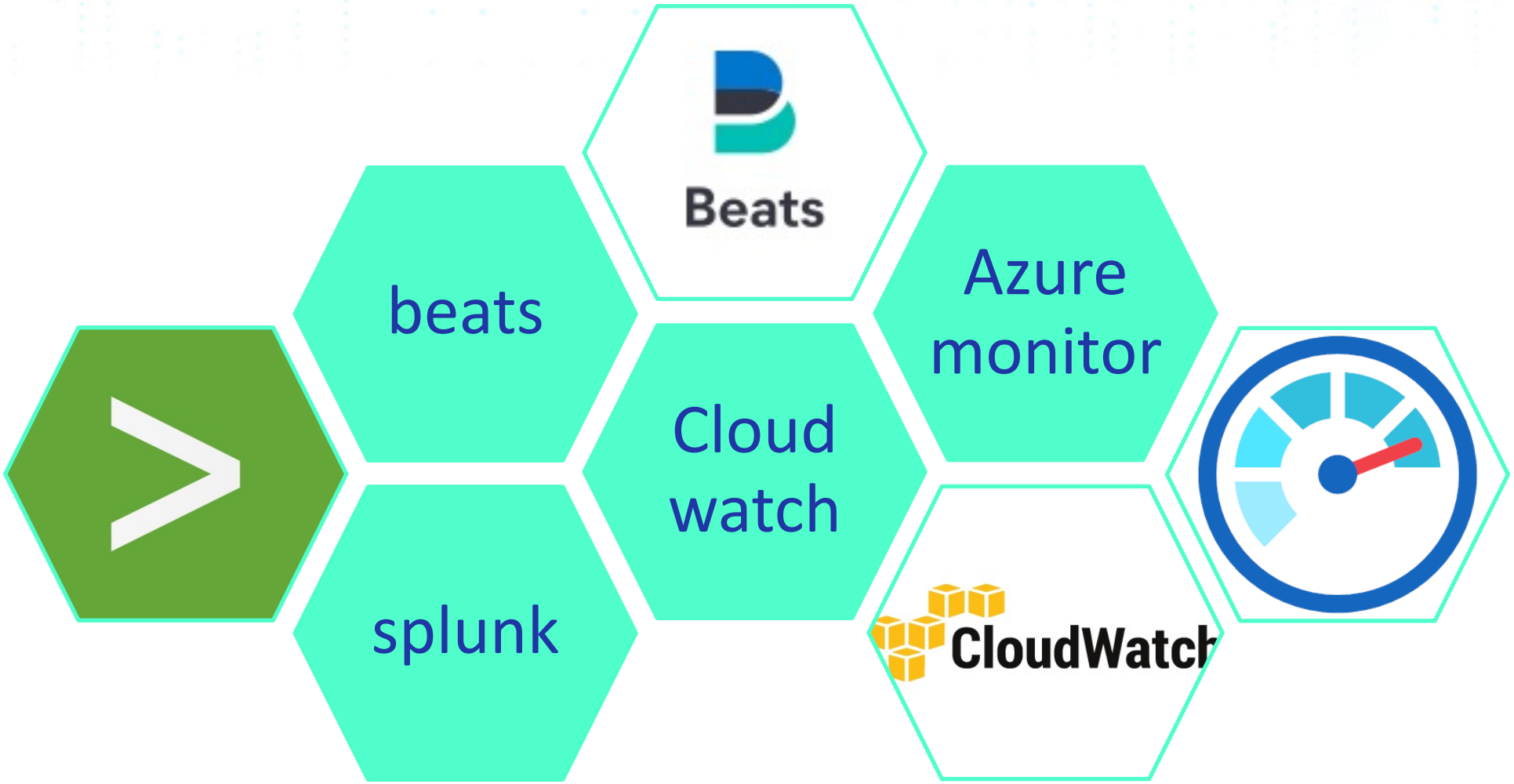
- The efficient kernel space filtering using tailored rules
- osquery to trigger, manage, consume and filter data using it’s SQL engine
- Annotate the data with the required metadata and publish.

RSAConference2021

Log aggregation and alerting

Once you have the events, getting insights from it should be accessible

Log aggregation and alerting

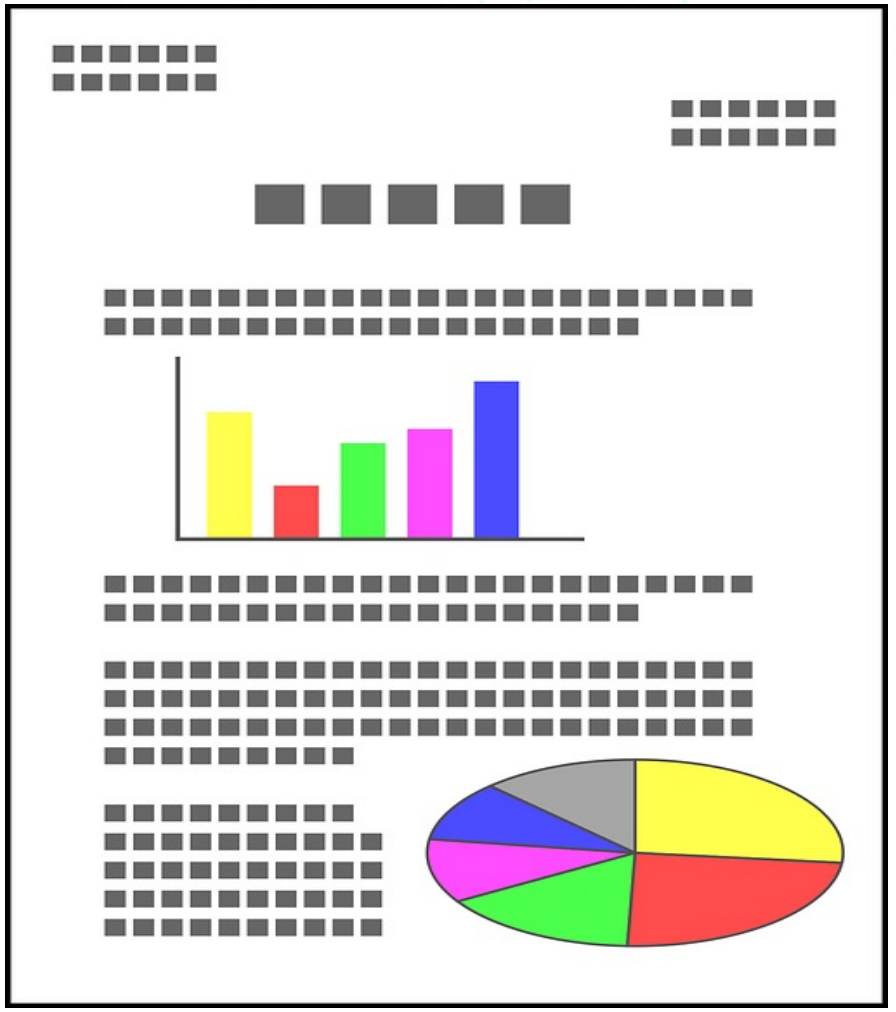


Alerting

- Detect anomalies like dead agents, agent uptime changes, config hash/version, agent hash/version changes etc.
- Live deterministic classifiers to detect security events in near real time
- Use this semi-classified data for machine learning based threat scoring and detection

Reporting and Inventory Management

- Generate reports on events periodically for audit evidence collection
- Expose the events as read-only for everyone to view and analyze
- Serve as inventory for triaging, building audit trails and ownership



RSAConference2021

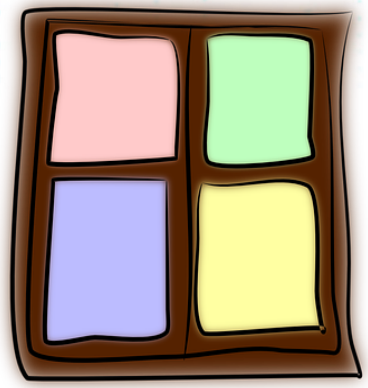
Can this extend to Mac and Windows

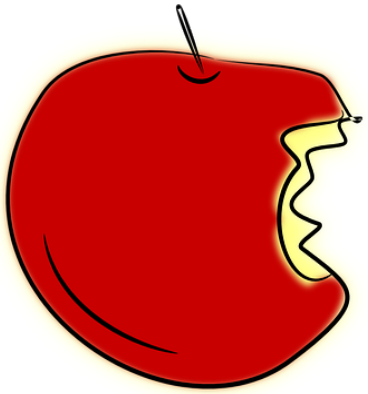
Linux is not the only platform out there

What about Mac and Windows?

Linux audit equivalents for Windows and MacOS

- Windows event logs
- EndpointSecurity Framework





What more could it do?

The Roadmap

- Integrate distributed query mechanism
- More flexible and expressive audit rules
- Add tables to process the Linux audit logs
- Publish config and queries for opensource log aggregators

How to apply the frameworks

Evaluate – What do you need?

- How long does it take for you to track an event to a resource
- What's the scope of your compliance in terms of controls
- What data points you need for your compliance
- How complex is your infrastructure

Evaluate – What do have?

- How visible are your servers
- What components can you reuse for implementing the audit framework as they are first class citizens
- What controls you already have and how many of them are redundant

Resources

Implementations and more details can be found at

- github.com/open-osquery/framework
- github.com/open-osquery/trails-ext
- github.com/open-osquery/libauditgo
- github.com/open-osquery/trailsc
- github.com/open-osquery/benchmark