osquery Super Features

Lauren Pearl
Head of Strategy & Ops @ Trail of Bits

Agenda

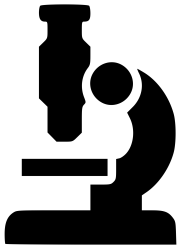
- **Introduction** - Trail of Bits, myself, our osquery user study
- **Super Features -** what they are, how to find, why they're important
- **Findings** - 3 Super Features for osquery
- **Conclusion** - what we're doing about it
- **Q&A (?)**

Trail of Bits

Cyber security research company - High-end security research with a real--world attacker mentality to reduce risk and fortify code.

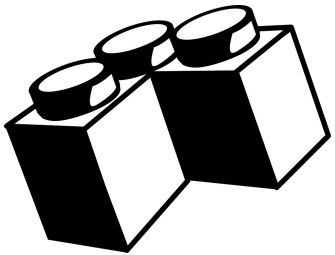
Security Research

- As a leading cybersecurity research provider to DARPA, the Army and the Navy – we create and release open source research tools



Security Engineering

- We offer custom engineering for every stage of software creation, from initial planning to enhancing the security of completed works



Security Assessments

- We offer security auditing for code and systems requiring extreme robustness and niche system expertise

Trail of Bits

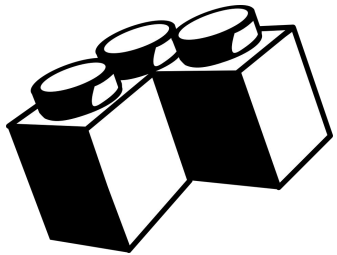
Cyber security research company - High-end security research with a real--world attacker mentality to reduce risk and fortify code.

Security Research

- As a leading cybersecurity research provider to DARPA, the Army and the Navy – we create and release open source research tools

Security Engineering

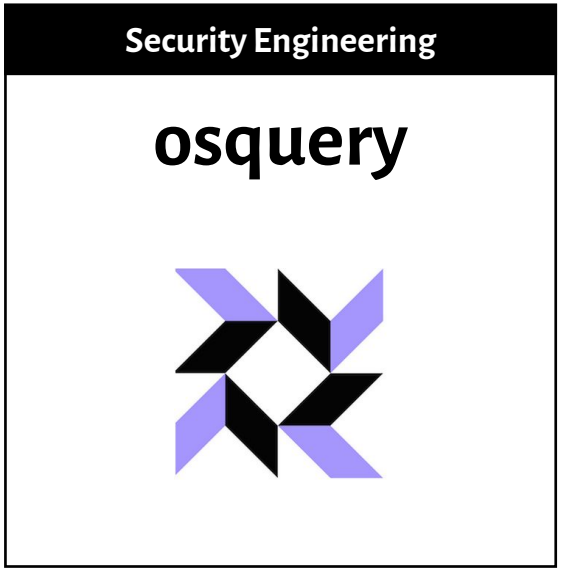
- We offer custom engineering for every stage of software creation, from initial planning to enhancing the security of completed works



Security Assessments

- We offer security auditing for code and systems requiring extreme robustness and niche system expertise

Trail of Bits - osquery



2016
- Facebook asked us to port osquery to Windows

2017
- AuditD-based File Integrity Monitoring
- Add Windows Event Log Logger Plugin
- Add Firehose/Kinesis support to Windows

2018
- Improve container introspection
- Trail of Bits extension repo
  - EFIgy Extension
  - Google Santa integration extension
  - NTFS extension
  - Firewall management extension

Who am I?

Name: Lauren Pearl
Title: Head of Strategy and Ops for Trail of Bits
Aka. Resident Business Nerd

What I am:
- Internal and external business analyst

Before Trail of Bits:
- Ran family a shoe retail company →
- Stint as a web app dev (lite)
- NYU MBA
- Deloitte strategy and ops consultant

osquery Blogs:
- How are teams currently using osquery?
- What are the current pain points of osquery?
- What do you wish osquery could do?

osquery User Study

- Interviewed 5 Silicon Valley tech companies
- Monitored osquery GitHub issues
- Added insights from pool of Trail of Bits clients
- Technical insights from Trail of Bits developers
- Management insight from dog-fooding osquery internally
- Edited and gut-checked by peers in the osquery community

What are Super Features?

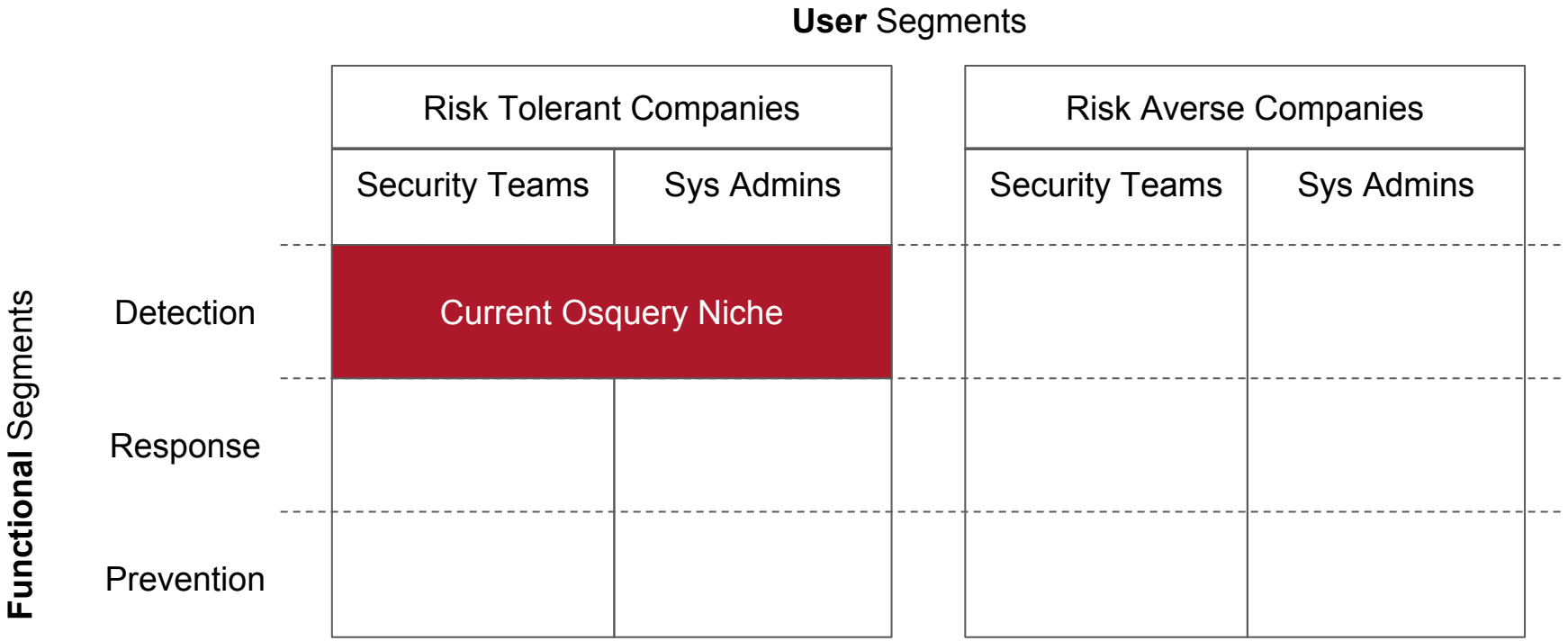
Super Features

Definition: Product attributes that represent a **foundational expansion** in a product's utility

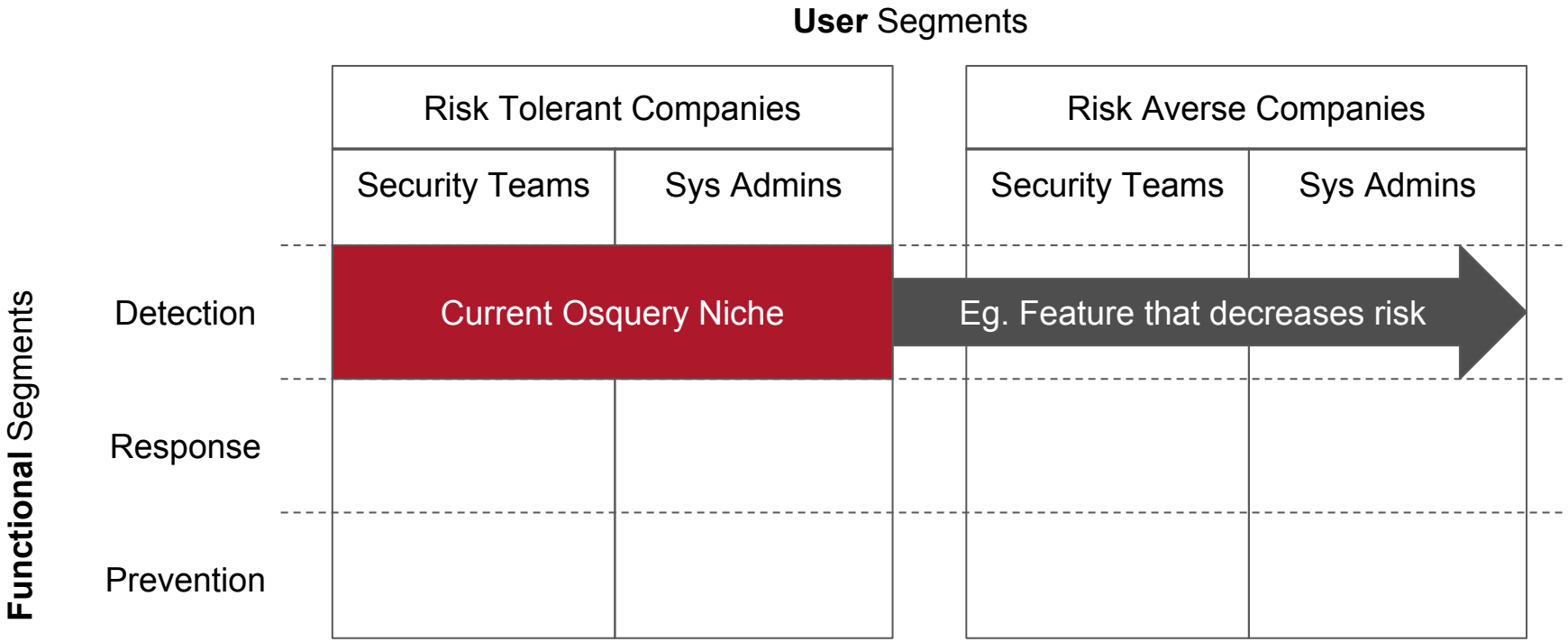
In order to be a Super Feature, a potential feature must:

- Shift product niche into an additional market segment
- Must increase the consumer surplus
- Must not destroy existing value for users

Expanding product niche



Expanding product niche



Increasing consumer surplus

Consumer Surplus = Technology Value - Technology Price

In order to increase Consumer Surplus with a new product, you have to provide **value advantages or price advantages** over the existing market technology

Why identify osquery Super Features?

Value maximization - Focus on the features that beget the most value for users overall

Development coordination - No wandering dev path from different teams who want different things

Product momentum - Generate excitement by picking features that bring the product to the next level

Findings!
3 osquery Super Features

Super Feature #1:
Write Access for Extensions

Nightmare - HACKERS!!

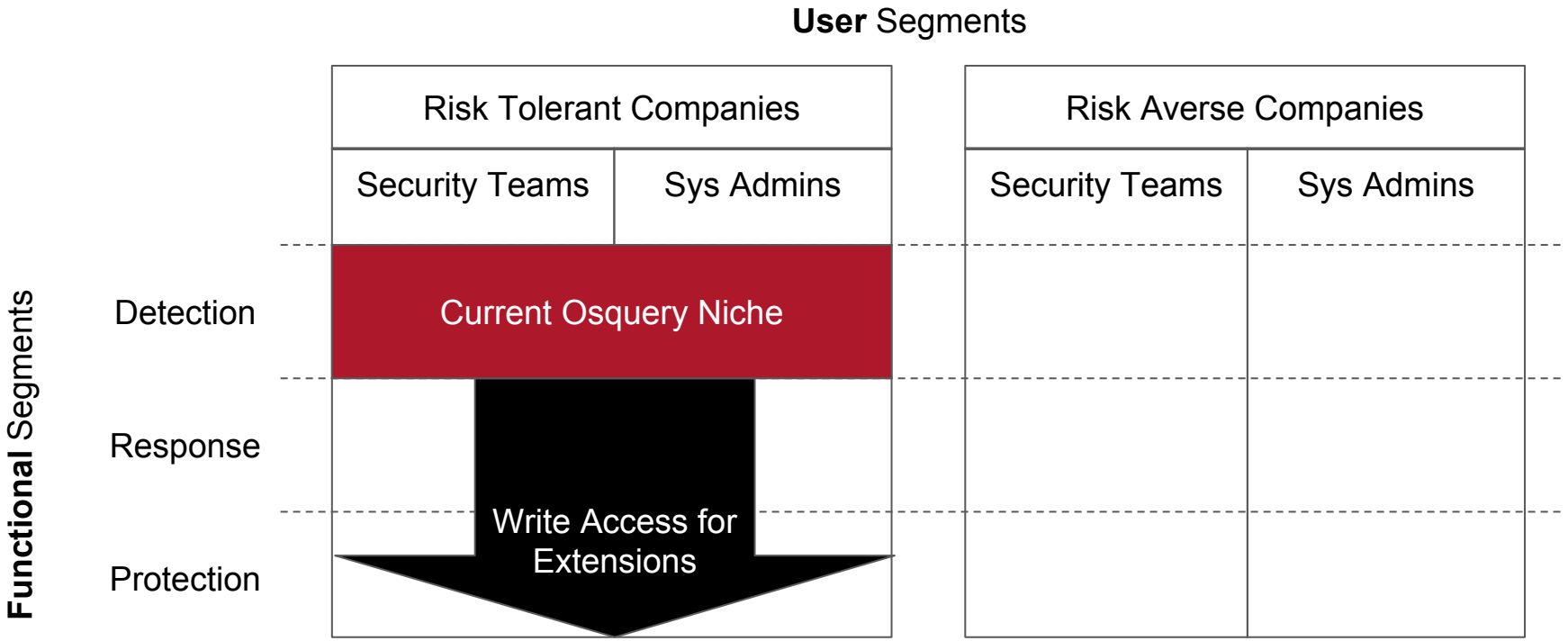
Reality - Stay safe by using extensions

- Read access only

Extensions

- Only has write access to (non-core) tables that specifically enable the feature
- Constrained write access doesn't allow executables - it's just a list of addresses
- Utilizes least privilege by design

Expanding osquery product niche



Write Access for Extensions

Increase consumer surplus	Advantages among commercial orchestration tools: ● Users could harden the system right from the SQL interface ● Can cover all these needs, with more limited permissions: ○ Application whitelisting and enforcement ○ Managing licenses ○ Partitioning firewall settings ○ Force password changes ○ Revoke accounts
Doesn't destroy value	● osquery core continues to only have read-access ● Write permission with least privilege in narrow channels
Bonus!	We've actually already built this! It's in a PR awaiting review. It enables: ● Our firewall management extension ● Our Google Santa integration extension

Super Feature #2:
Triggered Response on Detection

Triggered Response on Detection

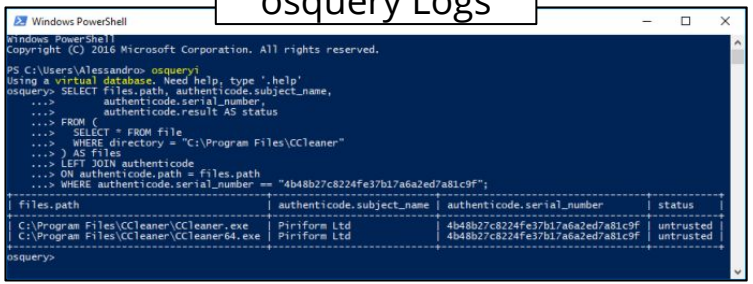
IoA Repositories

VirusTotal

REVERSING LABS

OpenDNS

osquery Logs



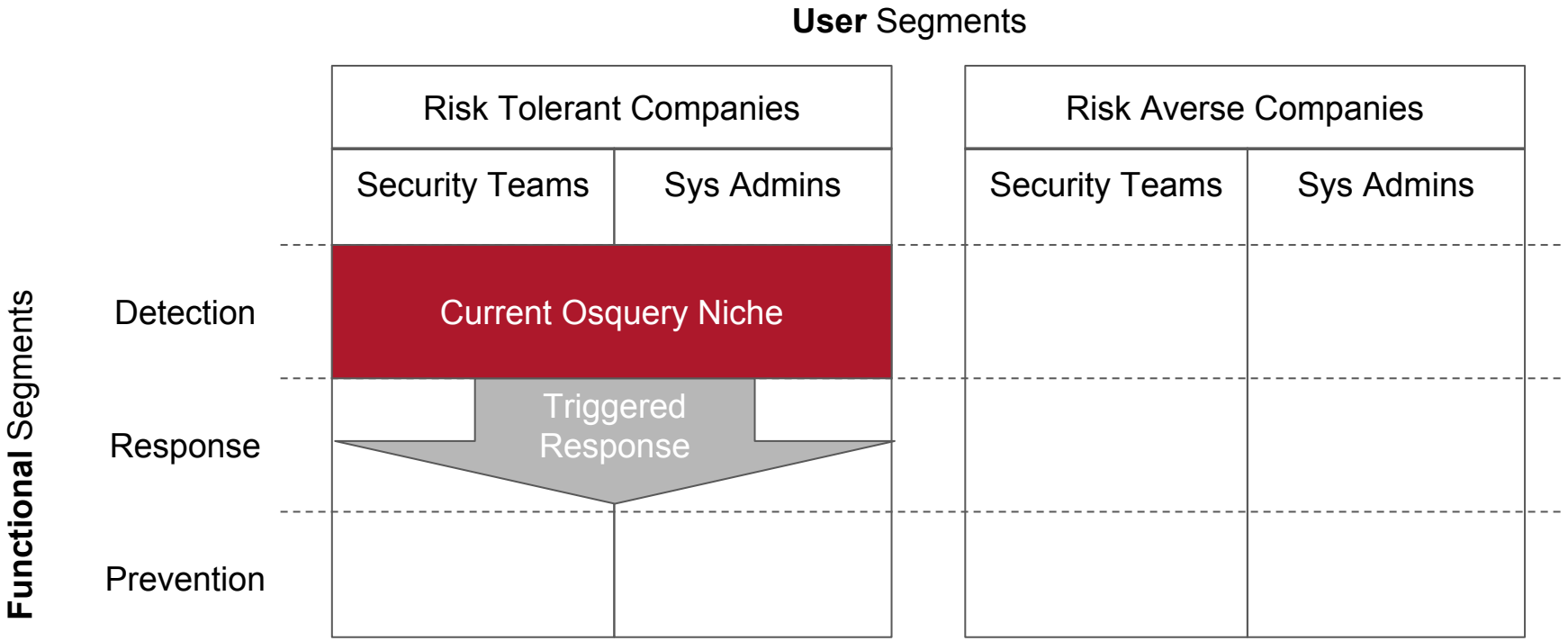
This log matches a list of bad things!

Texts a Number

Quarantines Endpoint

Sends logs to analysis tool

Expanding osquery product niche



Triggered Response on Detection

Increase consumer surplus	Advantages among current incident response tools: ● osquery would be more transparent and flexible ● Triggers and responses are infinitely customizable. Some examples: ○ *"…Upon detection of X log, query this table more often"* ○ *"…If a process from this blacklist is logged, send all endpoint's query data to This Tool for analysis"* ○ *"…If log Y is reported, quarantine the endpoint and send a message to CISO's pager"*
Doesn't destroy value	● Users can customize triggers and responses to minimize service disruptions from false positives

Super Feature #3:
Technical Debt Overhaul

Technical Debt Overhaul?

How is this a Super Feature?

Requests we heard

Guardrails & rules for queries:

- Resources and parameters to prevent users from making mistakes

Enhance Deployment Options:

- Easier deployment & updating

Integrated Testing, Debugging, and Diagnostics:

- More resources for testing and diagnosing issues that help improve reliability and predictability

Enhanced Event-Driven Data Collection:

- Better event-handling configurations, published best practices, and guardrails for gathering data

Enhanced Performance Features:

- Do more with fewer resources. Either enhance performance, or allow osquery to operate on endpoints with low resource profiles or mission-critical performance requirements.

Better Configuration Management:

- Out of the box custom tables and osqueryd scheduled queries for differing endpoint environments

Support for Offline Endpoint Logging:

- Forensic data availability to support remote endpoints requiring offline endpoints to store data locally –- including storage of failed queries –- and push to the server upon reconnection

Support for Common Platforms:

- Support for all features on all operating systems.

Requests we heard …are from technical debt

Guardrails & rules for queries:
- Resources and parameters to prevent users from making mistakes

Enhance Deployment Options:
- Easier deployment & updating

Integrated Testing, Debugging, and Diagnostics:
- More resources for testing and diagnosing issues that help improve reliability and predictability

Enhanced Event-Driven Data Collection:
- Better event-handling configurations, published best practices, and guardrails for gathering data

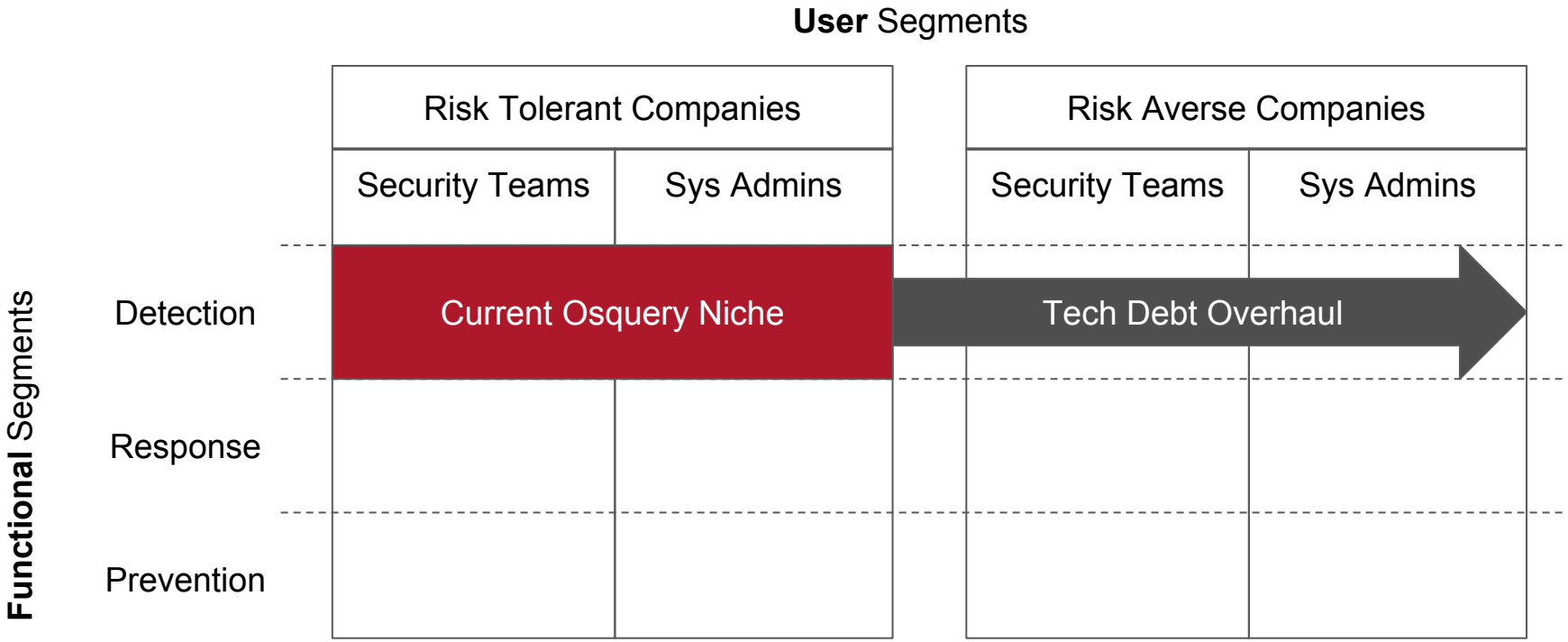
Enhanced Performance Features:
- Do more with fewer resources. Either enhance performance, or allow osquery to operate on endpoints with low resource profiles or mission-critical performance requirements.

Better Configuration Management:
- Out of the box custom tables and osqueryd scheduled queries for differing endpoint environments

Support for Offline Endpoint Logging:
- Forensic data availability to support remote endpoints requiring offline endpoints to store data locally –- including storage of failed queries –- and push to the server upon reconnection

Support for Common Platforms:
- Support for all features on all operating systems.

Expanding osquery product niche



Technical Debt Overhaul

Increase consumer surplus	Increases advantages currently realized by osquery users, and increases the number of users who can access these advantages: ● Clears a majority of user issues around performance, reliability, and ease of use
Doesn't destroy value	● Doesn't, almost by definition

Where to now

osquery Development Support Plans!

Support Plans

12-Month Assurance Plan:
"All you can eat" osquery bug fixes and feature enhancements including:

- Root-cause and fix issues
- Develop new tables and extensions
- Redesign parts of osquery core as required

Bespoke osquery Development:
One-off engagements focused on individual features such as:

- Porting osquery to a new platform
- Proprietary or non-core features
- Forks

Resources for All Clients

- Private Trail of Bits Slack channel
- Trail of Bits osquery Clients group membership
- Bi-Weekly Iteration Planning Meeting
- Private GitHub repo with issue tracker
- Special access and support for Trail of Bits osquery extensions
- Early access to all software increments

And here are the Benefits

- No show-stopping bugs
- Direct access to our team of engineers
- Peace of mind - no internal engineers have to worry about issues with osquery
- First access to our latest releases means consistently cutting-edge technology
- Users drive the product direction of osquery, while Trail of Bits handles the heavy lifting

Contact Us

Lauren Pearl

Head of Strategy and Operations @ Trail of Bits

Lauren@trailofbits.com

www.trailofbits.com

Appendix

Write-Access for Extensions - IRL Proof

fwctl osquery Extension https://github.com/trailofbits/osquery-extensions/tree/master/firewall

Provides osquery with the ability to:

- View and *manage* the OS-native firewall rules and /etc/hosts file (port and host blocking)
- Verify what your endpoints are blocking, and add new blocking rules as needed

Triggered Response - IRL Proof

osquery suites that have alerting:

KOLIDE

Uptycs

doorman

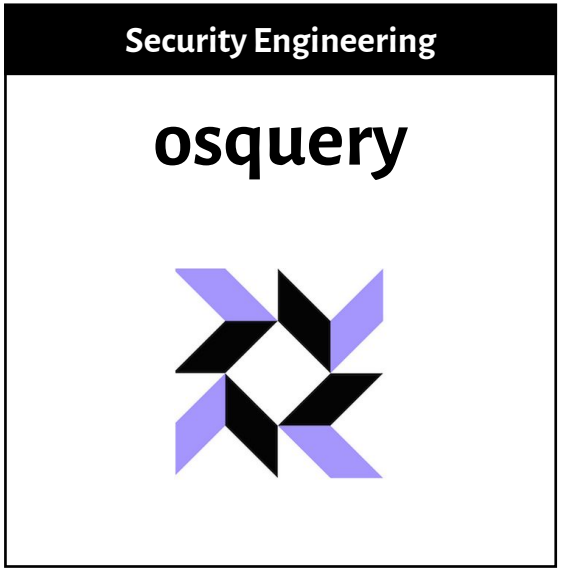
Example of custom alerting techniques:

elasticsearch

ElastAlert

Jira

Technical Debt Overhaul - IRL Proof



2016
- Facebook asked us to port osquery to Windows

2017
- AuditD-based File Integrity Monitoring
- Add Windows Event Log support
- Add Firehose/Kinesis support to Windows

2018
- Improve container introspection
- Trail of Bits extension repo
- EFIgy Extension
- Google Santa integration

Increasing consumer surplus - Open Source

Definition: Consumer surplus is the difference between what users are willing to pay (what they value) and what they actually have to pay

	Commercial Product	Open Source Product
Price	$$$$$ - Subscription	$ - Shared investment
Ownership	Suppliers	Users
Features	Based on supplier needs	Based on user needs

If you replace a commercial solution with an equivalent or better open source one, consumer surplus is increased

osquery users

Known user industries:

- High-tech service and products
- Mobile payments
- Media & telecom
- Retail
- Consulting & security services

Known user departments:

- Security
- System administration

Expanding osquery product niche