

# Blazing-Fast Security Ops

Unleashing Splunk ES 8.0 for  
Speed and Scale

SEC1668

Brent Davis & Bhanu P Karumuri



# Forward-looking statements

This presentation may contain forward-looking statements regarding future events, plans or the expected financial performance of our company, including our expectations regarding our products, technology, strategy, customers, markets, acquisitions and investments. These statements reflect management's current expectations, estimates and assumptions based on the information currently available to us. These forward-looking statements are not guarantees of future performance and involve significant risks, uncertainties and other factors that may cause our actual results, performance or achievements to be materially different from results, performance or achievements expressed or implied by the forward-looking statements contained in this presentation.

For additional information about factors that could cause actual results to differ materially from those described in the forward-looking statements made in this presentation, please refer to our periodic reports and other filings with the SEC, including the risk factors identified in our most recent quarterly reports on Form 10-Q and annual reports on Form 10-K, copies of which may be obtained by visiting the Splunk Investor Relations website at [www.investors.splunk.com](http://www.investors.splunk.com) or the SEC's website at [www.sec.gov](http://www.sec.gov). The forward-looking statements made in this presentation are made as of the time and date of this presentation. If reviewed after the initial presentation, even if made available by us, on our website or otherwise, it may not contain current or accurate information. We disclaim any obligation to update or revise any forward-looking statement based on new information, future events or otherwise, except as required by applicable law.

In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not be incorporated into any contract or other commitment. We undertake no obligation either to develop the features or functionalities described, in beta or in preview (used interchangeably), or to include any such feature or functionality in a future release.

---

Splunk, Splunk> and Turn Data Into Doing are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names or trademarks belong to their respective owners.  
© 2025 Splunk LLC. All rights reserved.



# About Us



**Brent Davis**

Sr. Principal Software Engineer  
Splunk Platform



**Bhanu P Karumuri**

Principal Software Engineer  
Splunk Enterprise Security

# Our Focus on Performance and Scale

Splunk's highly scalable platform + best-of-breed SIEM



Continuously Improving Splunk Performance and Scale

# Two Goals Today



# Time is of the Essence...

Every second matters in the SOC



**MTTD**  
Intrusion → lateral movement  
51s - 58m

**MTTR**  
faster page loads & searches  
critical

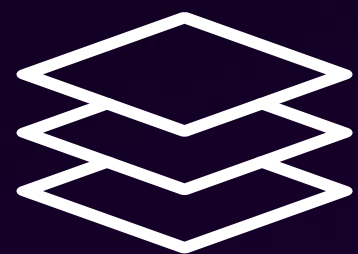
Growing data  
⇒  
Slowing KPIs

# Foundations of ES Performance

# Performance Ingredients



**Enterprise Security**



**Splunk Platform**

**FrontEnd (JavaScript)**

**Search (SPL)**

**BackEnd (Python)**

**KVStore**

**Web Server**

**Search Infra**

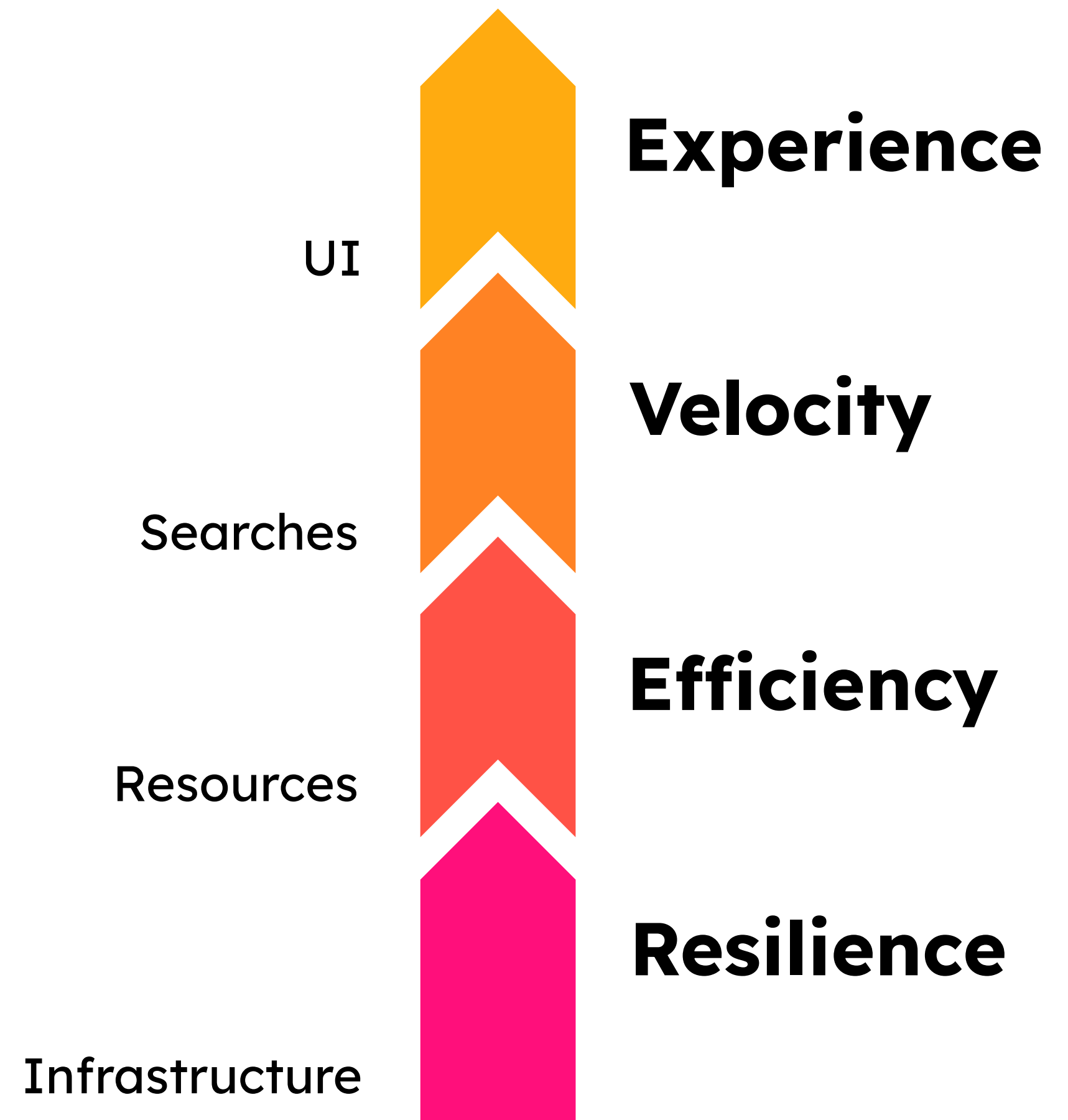
**Layout & APIs**



# Four Pillars

To Achieve our Goals of:

- **Fast Detection**
- **Fast time-to-acknowledge**
- **Scale w/Growth in Data**





**Experience**

**Velocity**

**Efficiency**

**Resilience**

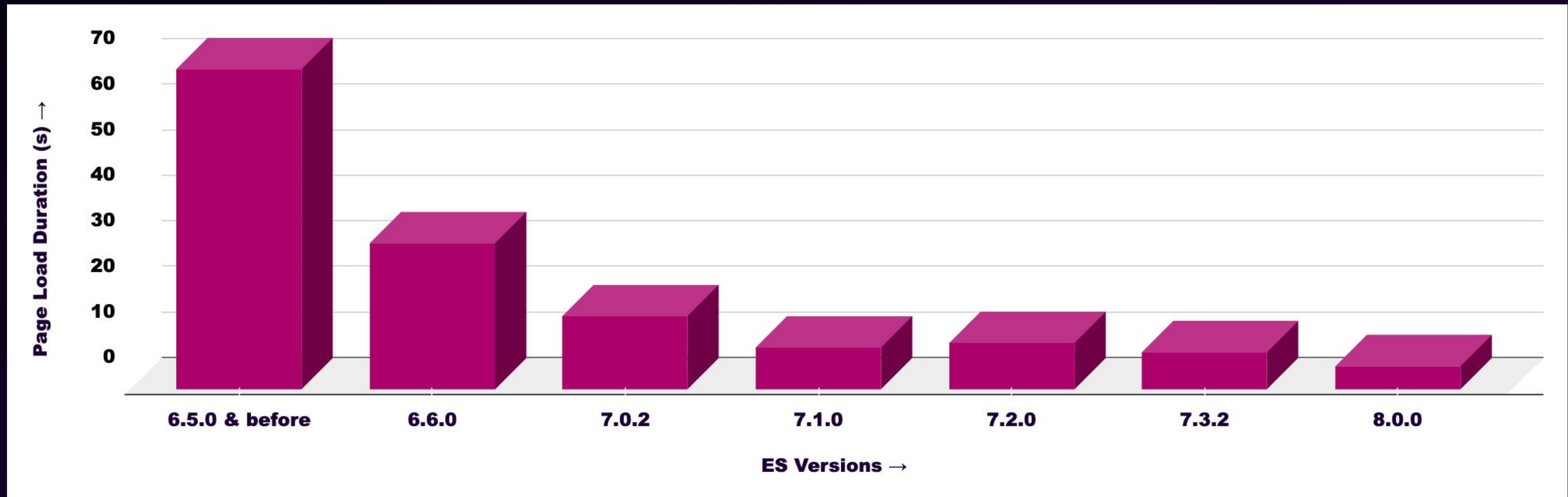


# How Splunk Can Help Your **Experience.**

## Product Improvements

- Page-load duration
- Asynchronous resource loading
- Analyst Queue
- SID Caching

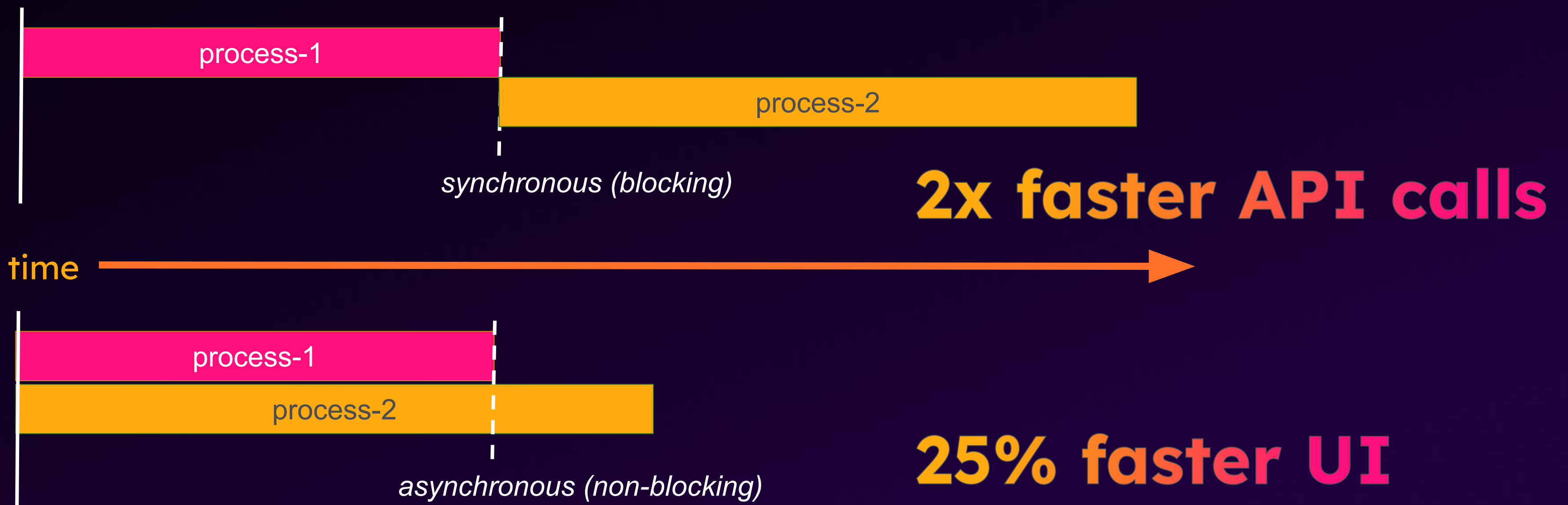
# Experience - ES Improvements over the years





# Experience - Parallel Sequencing

synchronous vs asynchronous



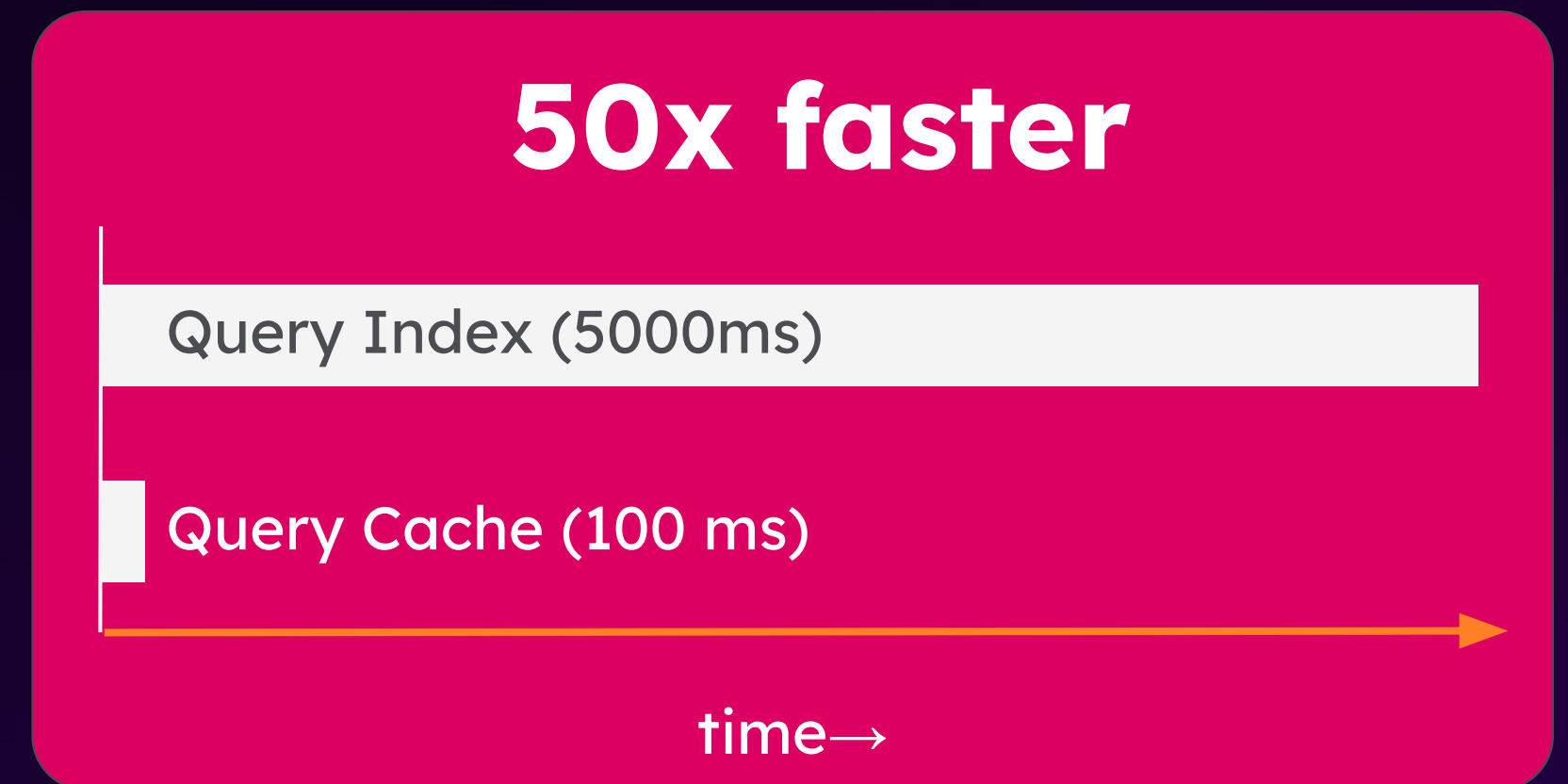
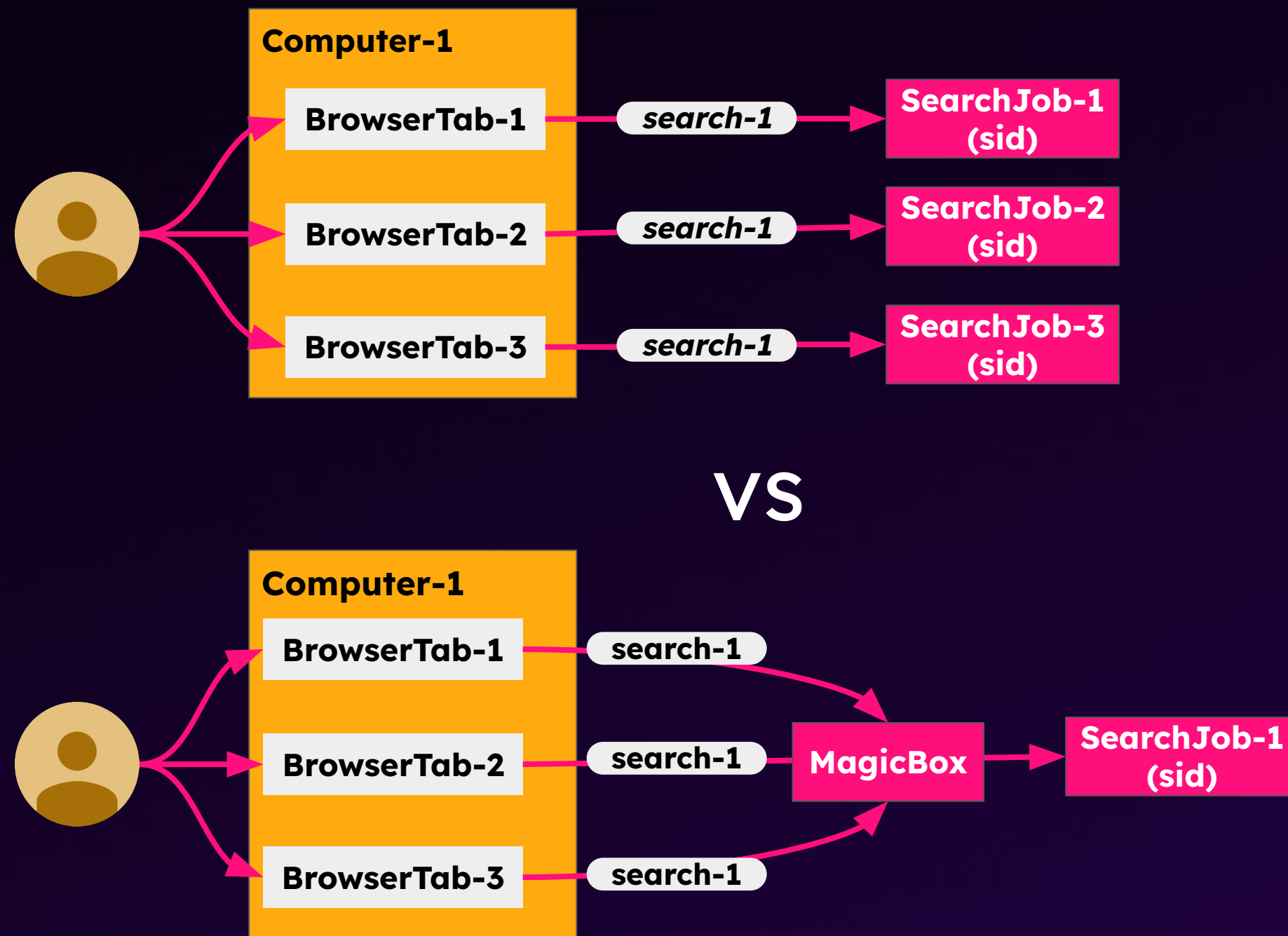
# Experience - Improvements to Analyst Queue



**50%+ Improvement**

# Experience - SID Caching

Coming in 8.2

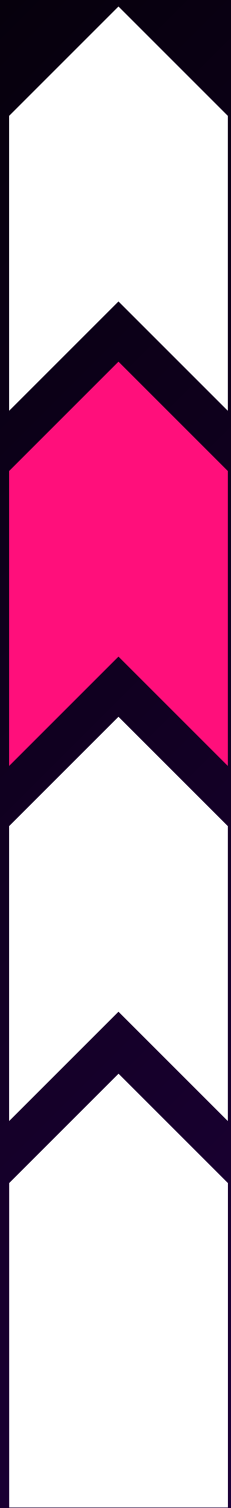


What you  
can do **Today.**



# Experience - What You Can Do Today

- Keep duplicated search jobs to a minimum: keep the analyst queue to a single tab
- When using Analyst Queue, follow Splunk search best practices! (filter by user, time, status, severity, etc.)
  - Use care when modifying the core analyst queue searches.



**Experience**

**Velocity**

**Efficiency**

**Resilience**



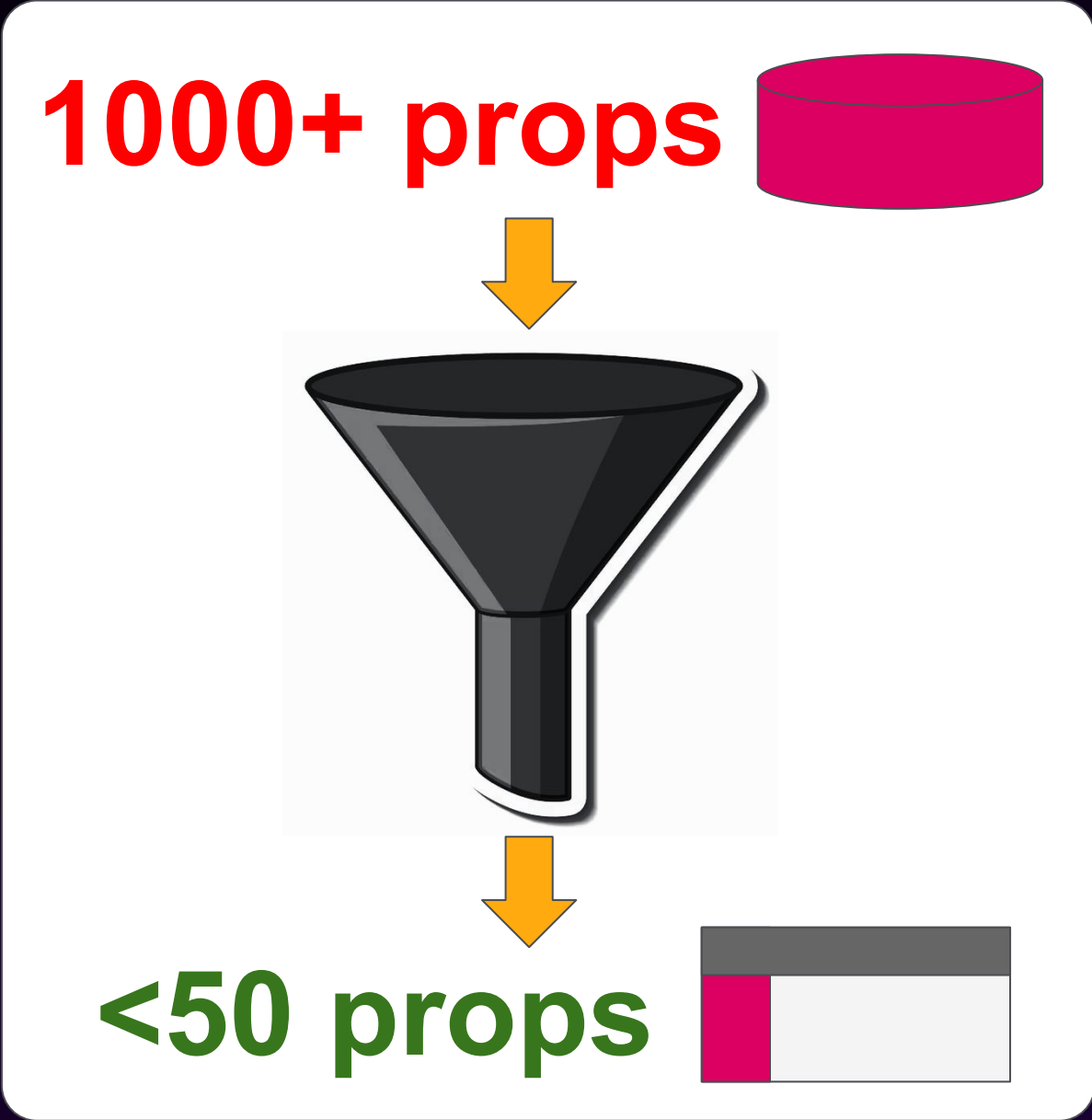
# How Splunk Can Help Your **Velocity**.

## **Product Improvements:**

- API optimizations to over 13 separate pages
- Custom commands vs native SPL
- Enrichment with Lookups
- SmartStore fetch improvements
- Indexing throughput



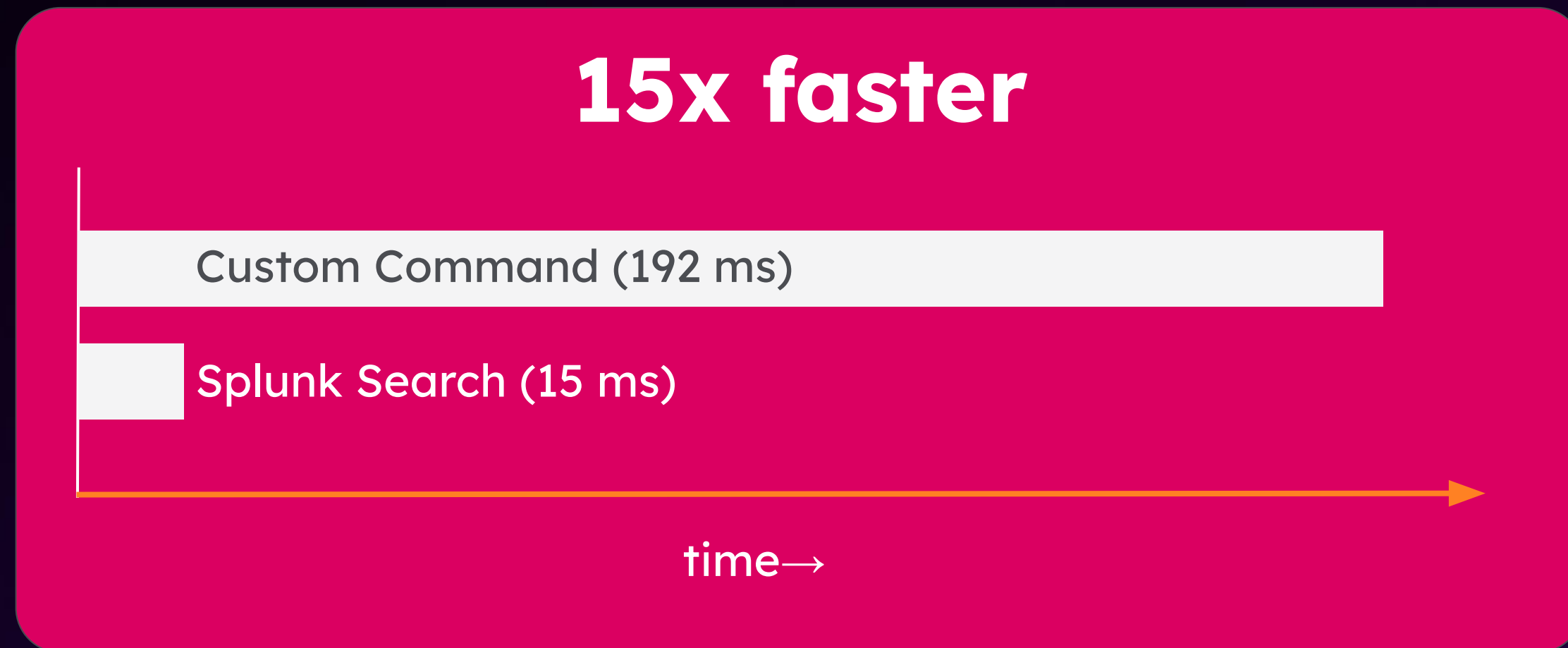
# Velocity - API/Search Optimization



data.page	Speed Improvements	Drop in API Payload
incident_review	2X	10X
correlation_search_edit	2X	10X
ess_content_management	5X	10X
ess_swimlane_new	1.8X	10X
ess_key_indicator_edit	1.8X	10X
ess_swimlane_edit	1.8X	10X
ess_key_indicator_new	1.8X	10X
ess_search_driven_lookup_editor	1.8X	10X
asset_investigator	1.8X	10X
identity_investigator	1.8X	10X
ess_analytic_story_details	1.8X	10X
ess_analytic_story_edit	1.8X	10X
ess_use_case_library	1.8X	10X



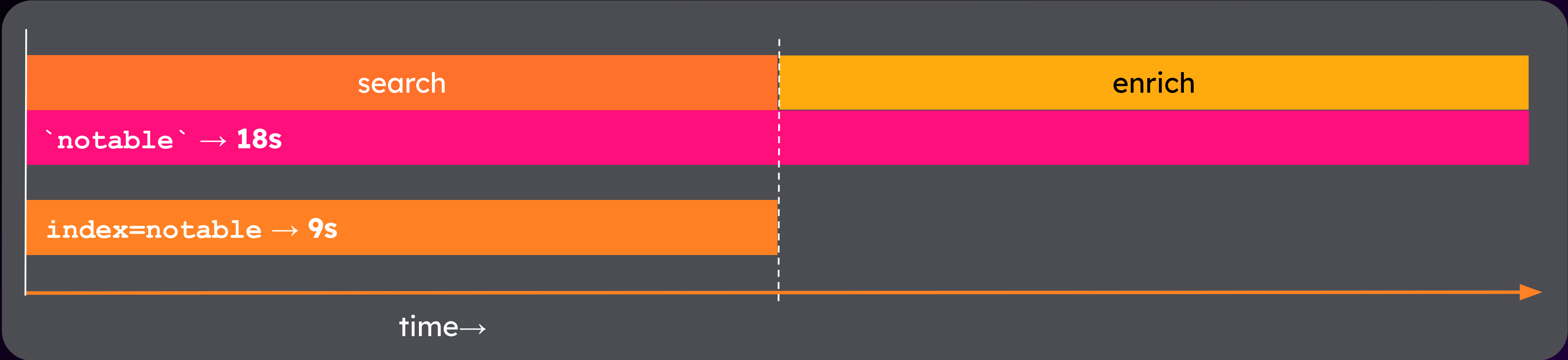
# Velocity - Custom Command vs Macro



✗ Custom command - execution on search head

✓ Macro - execution on indexer (distributed search)

# Velocity - Cost of enrichment



## Pages Benefitted

Analyst Queue	Analyst Queue Main Table	Analyst Queue Side Panel	Analyst Queue Bulk Update
Investigations	Investigations Risk Event Timeline	Investigations AI Assistant	Investigations SOAR Integration

## OUTCOMES

5 lookups eliminated  
10 joins removed  
30% faster page loads

What you  
can do **Today.**

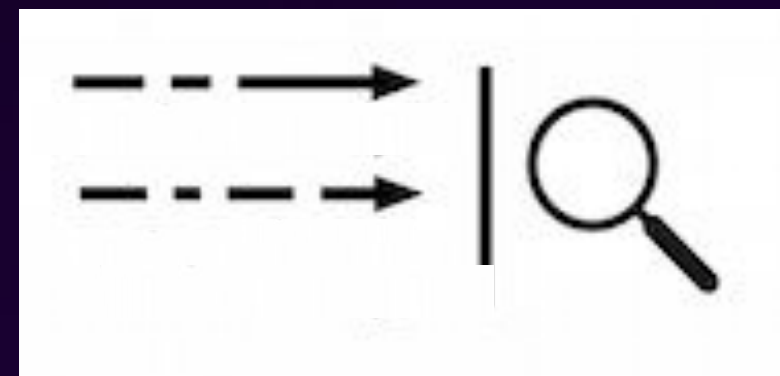
# Velocity - What You Can Do Today

## Don't overuse your Search Head

Distributable vs. Non Distributable commands



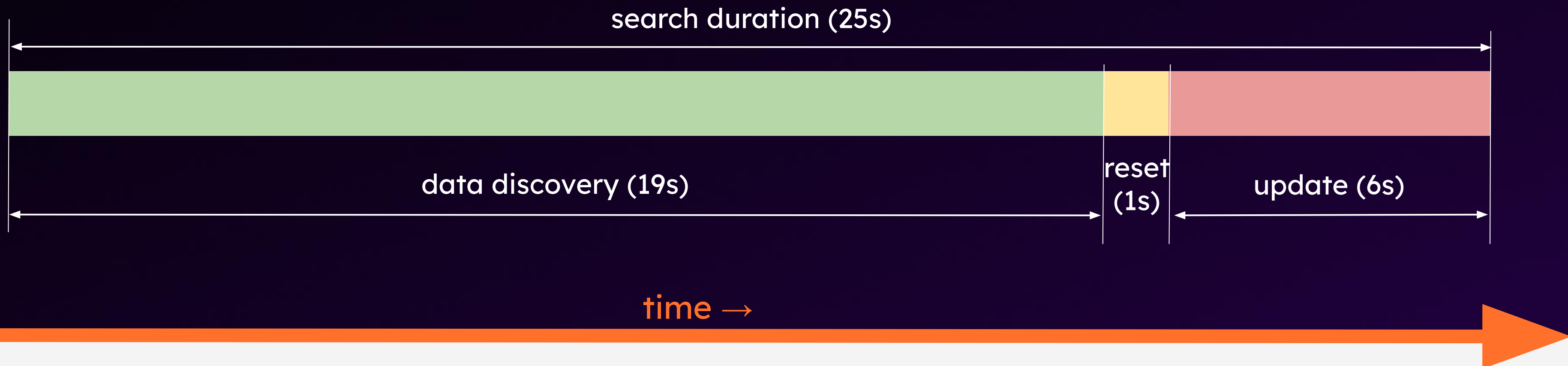
**vs**



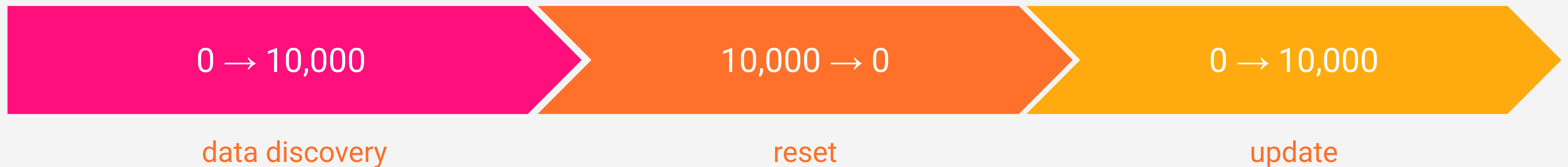


# Velocity - What You Can Do Today

example command: eventstats

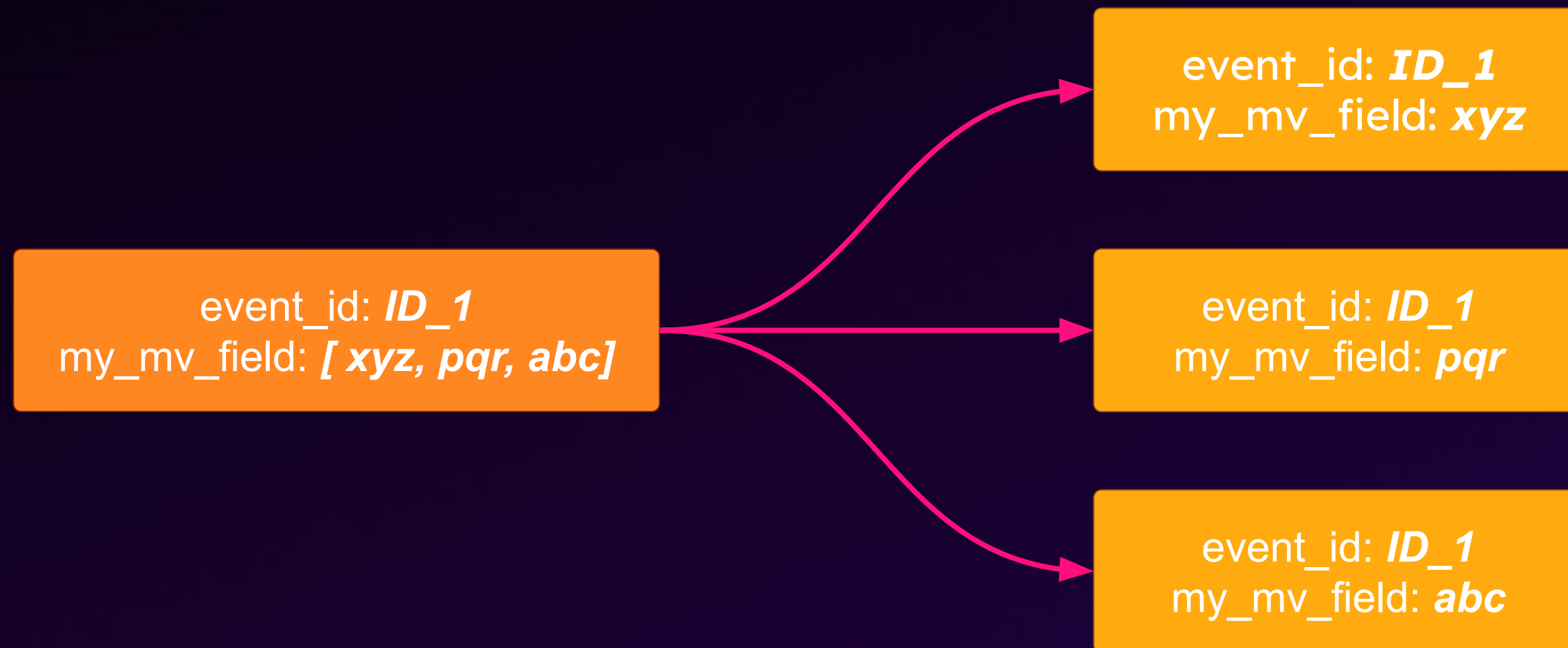


Event Count per phase



# Velocity - What You Can Do Today

example command: mvexpand



# **Velocity** - What You Can Do Today

## **Attend Our Session on Search Performance!**

PLA1685 - Finding a Needle in a Haystack at Speed: Leveraging Splunk 10 for Faster Searches

Wednesday, 9:30AM



**Experience**

**Velocity**

**Efficiency**

**Resilience**





# How Splunk Can Help Your Efficiency.

## Product Improvements:

- KV data retention policies
- Distribution of scheduled searches

# Efficiency - KV Retention Policy

## Retention Policies:

- Size
- Time
- Size *and* Time

```
{
  "_key": "aba16994-cb8b-4528-b944-b5ee1072ce23",
  "retention_time": 180, //in days
  "retention_size": 20, // in GB's
  "create_time": 1696027757.8004212379,
  "update_time": 1696027757.8004212379,
  "id": "aba16994-cb8b-4528-b944-b5ee1072ce23",
  "collection_name": "mc_incidents",
  "checksum": "120EA8A25E5D487BF68B5F7096440019",
  "cron": "0 0 * * *"
  "dependent_collections": ["mc_notes", "mc_attachments", "mc_attachments_chunks"]
}
```

Settings | Splunk

Not Secure https://sh1.splunk-vineet-git-131b.stg.splunkcloud.com/en-US/manager/launcher/data/inputs/mc\_kv...

splunk>cloud Apps 4 Messages Settings Activity Find Splunk Administrator

KV Store Collection Retention

Data inputs » KV Store Collection Retention

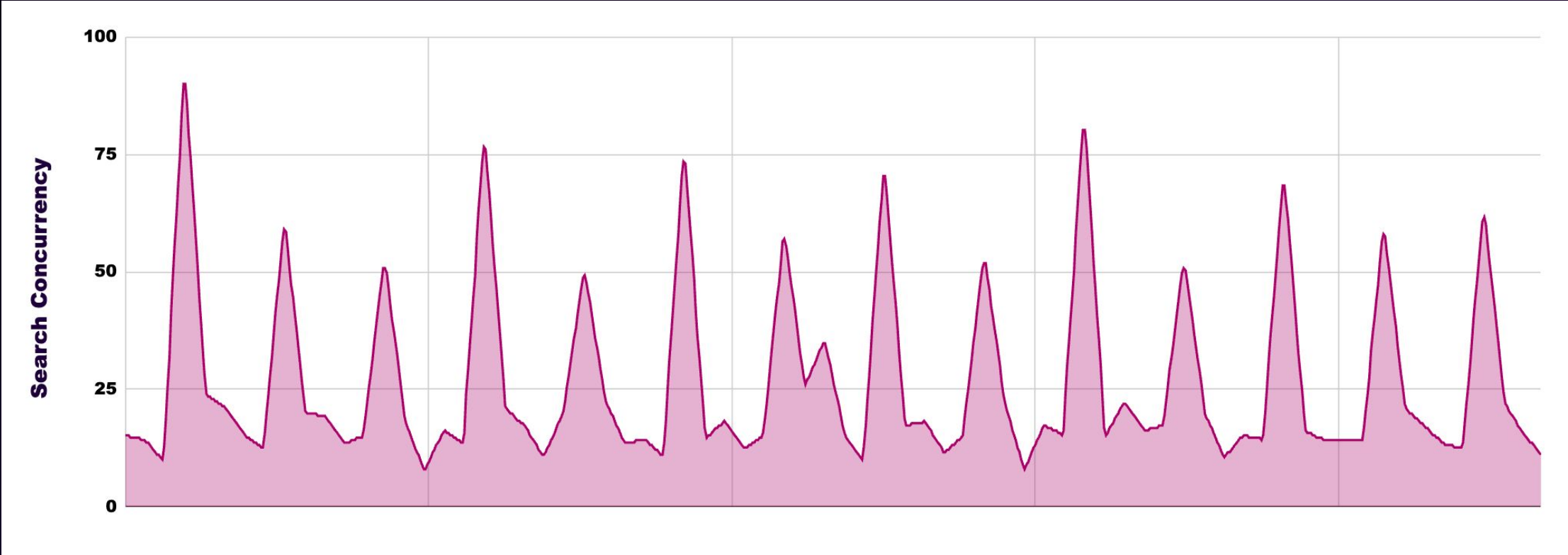
Showing 1-15 of 15 items

filter 25 per page

name	Debug	Max Age	Max Size	Source type	Index	Status	Actions
da-ess-networkprotection.vulnerability_tracker	0	-1	25	mc_kv_store_retention	default	Enabled   Disable	Clone
da-ess-networkprotection.whois_tracker	0	-1	25	mc_kv_store_retention	default	Enabled   Disable	Clone
da-ess-threatintelligence.file_intel	0	-1	25	mc_kv_store_retention	default	Enabled   Disable	Clone
missioncontrol.findings	0	-1	25	mc_kv_store_retention	default	Enabled   Disable	Clone
missioncontrol.im_threat_indicators	0	30	-1	mc_kv_store_retention	default	Enabled   Disable	Clone
missioncontrol.investigations	0	-1	25	mc_kv_store_retention	default	Enabled   Disable	Clone
missioncontrol.tim_iocs	0	30	-1	mc_kv_store_retention	default	Enabled   Disable	Clone

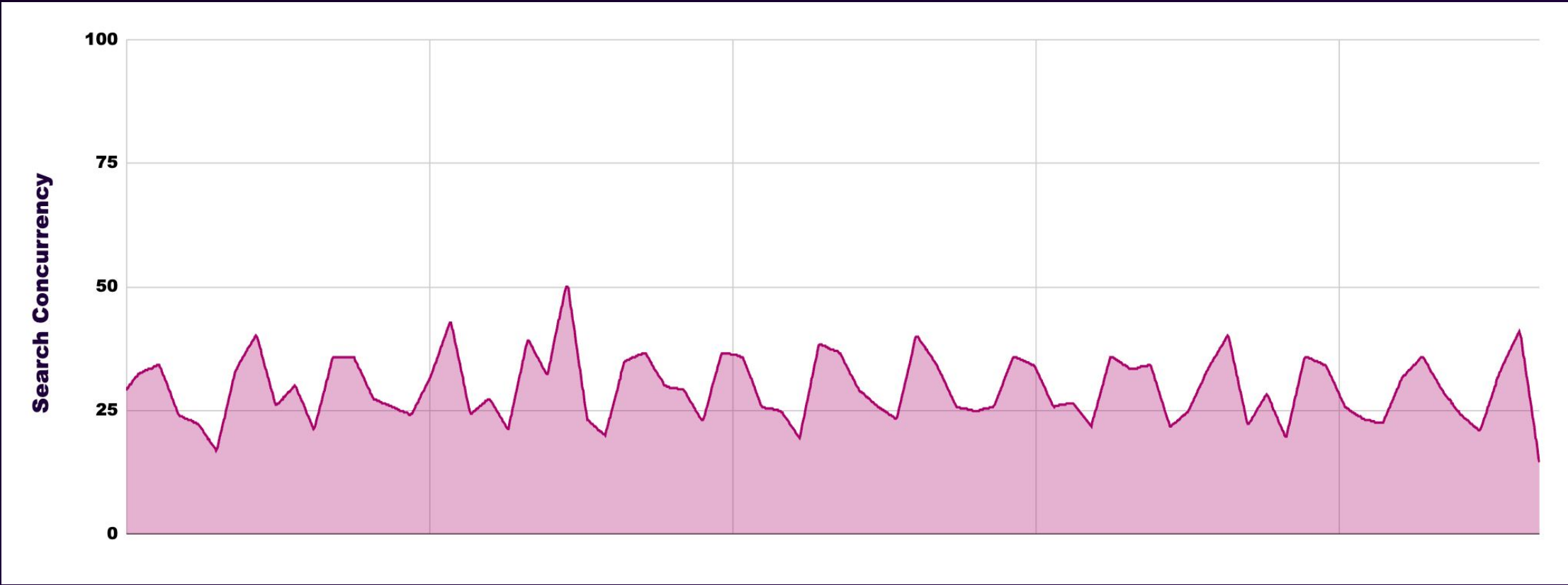
# Efficiency - Scheduled Searches

Before



allow\_skew

After



What you  
can do **Today.**



# Efficiency - What You Can Do Today

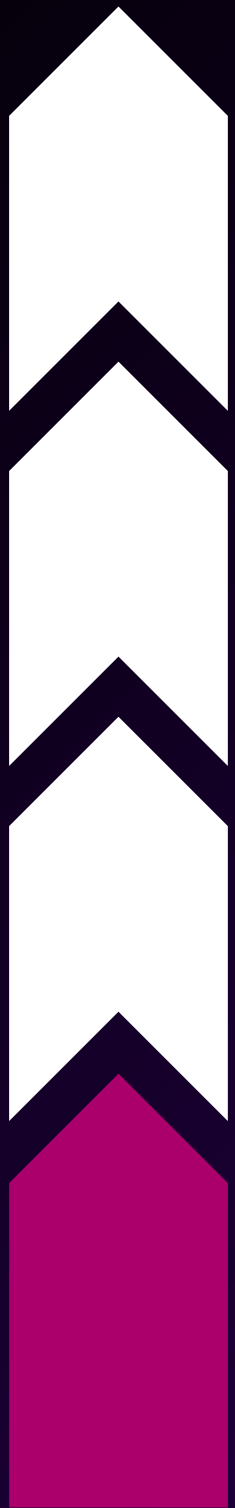
## Managing Indexer Utilization

- Prune lookup tables
- Use `allow_skew` and skewable cron patterns
- Carefully schedule searches to reduce concurrency
- Consider stack sizing

# Efficiency – What You Can Do Today

## Scheduled Data Model Accelerations

- Optimize Data Model SPL searches
- Scan only the data needed (specify indexes, sourcetypes, tagging)
- Optimize Data Ingest, could you use an ingest action?
- Don't use custom commands in DMAs



**Experience**

**Velocity**

**Efficiency**

**Resilience**





# How Splunk Can Help Your Resilience.

## Product Improvements:

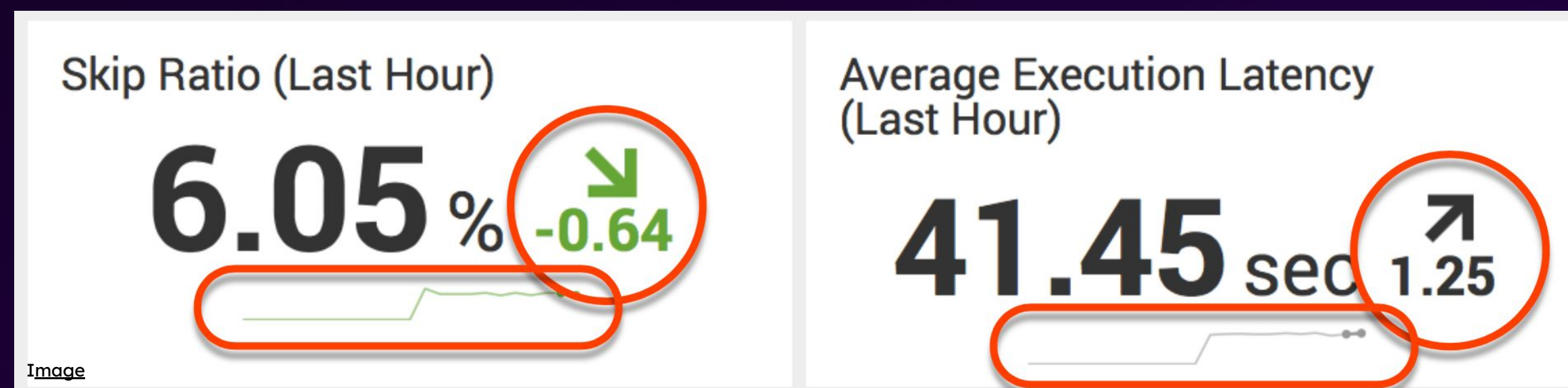
- Enhanced Workload Management
- Cross-product Integrations
- Splunk Classic Replication
- Cross-region DR in Cloud.



What you  
can do **Today.**

# Resilience - What You Can Do Today

- Use Splunk Workload Management to quarantine resource usage on ad-hoc searches
- Ensure you're on Victoria Experience (higher scale limits) - most of you - only 8% on Classic in cloud
- If using Splunk Enterprise, ensure your stack is properly sized and Cluster Manager is tuned



# **Resilience** - What You Can Do Today

## **Attend Our Session on Workload Management!**

PLA1696 - Smooth Operations: Managing Splunk 10 Workloads for Speed and Stability

Wednesday, 9:00AM

# Real World Impacts!

# ES 8.0 High Scalability

**250 TB**


Per day ingest comprehensive  
scale test on Splunk Cloud Victoria

**1.2M+**

Over 1.2M searches/day

**2M**

Two million entities

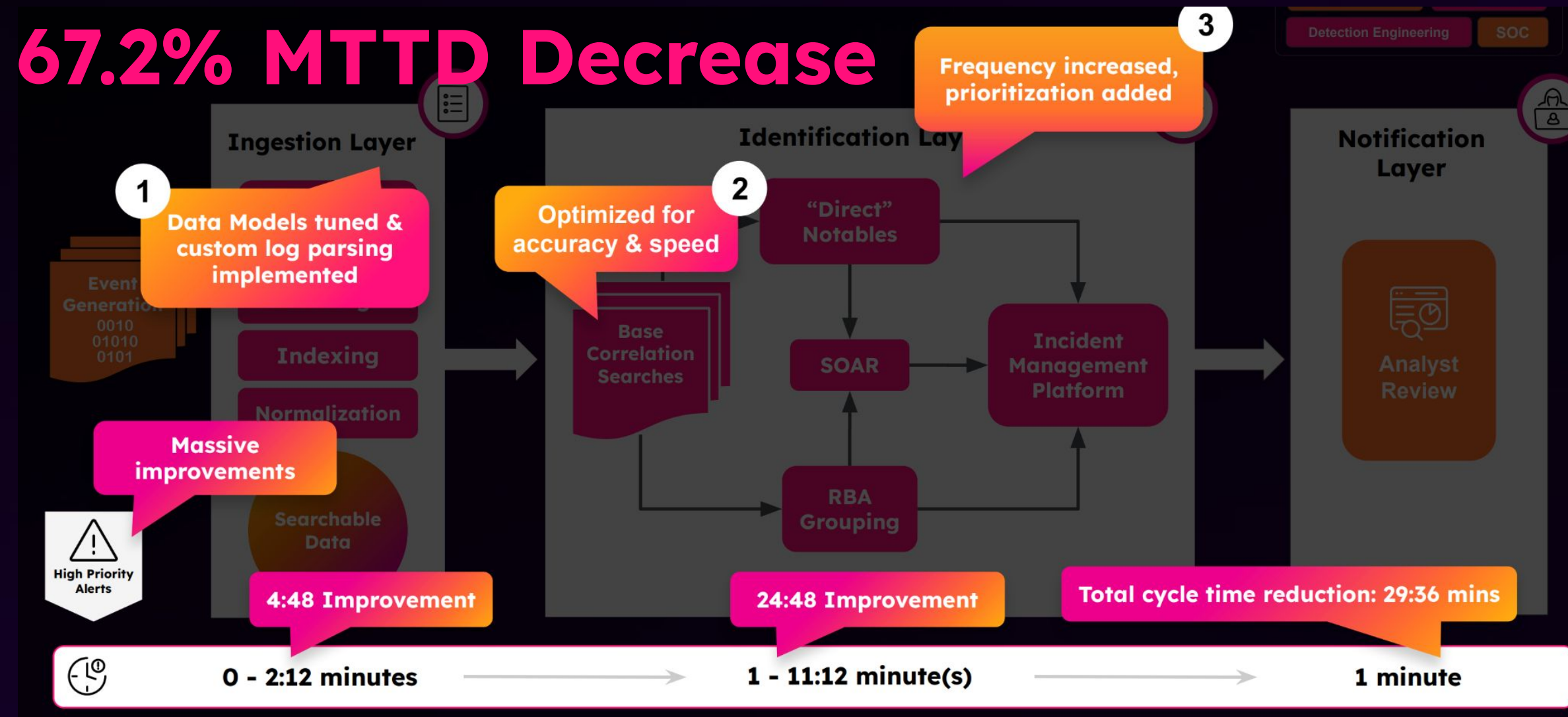


**3x** All Prior ES  
Service Limits  
Achieved



# Splunk SOC and Splunk Cloud

conf24: SEC11935 The Evolution of Splunk Products in our own SOC



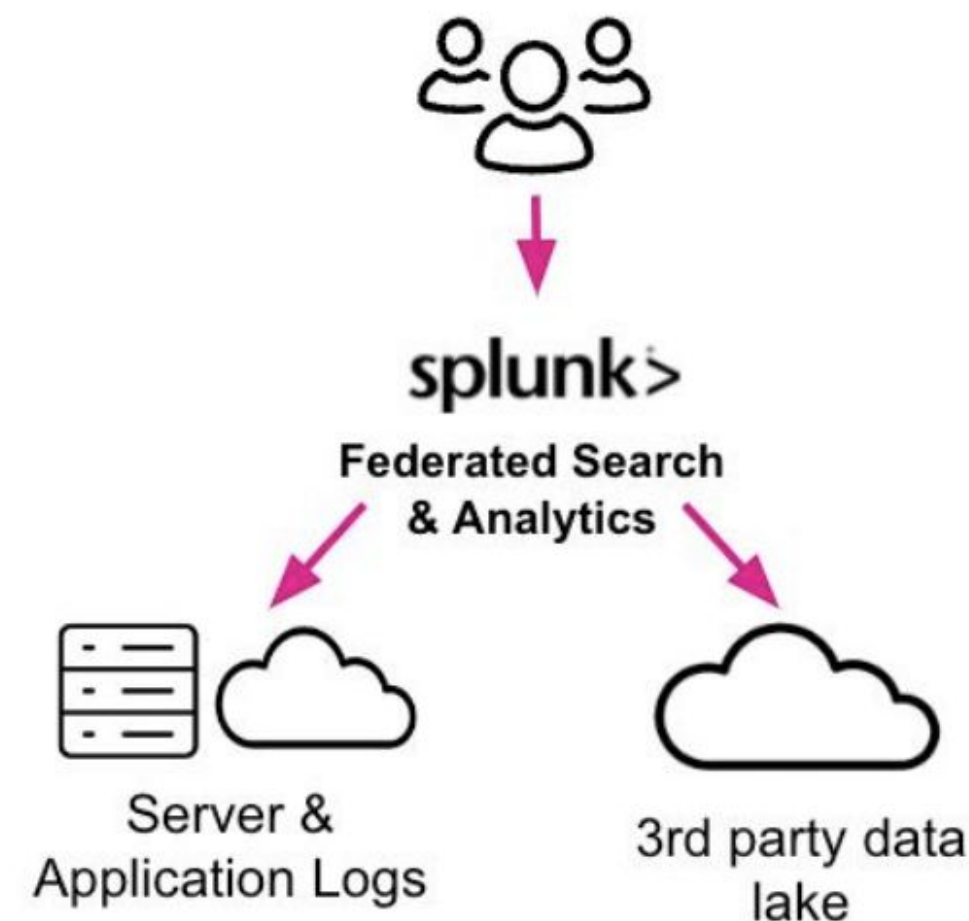
Splunk Enterprise Cloud  
**2 Billion** ES Searches each month

# Accelerating the Future

# Federated Search and Analytics

Check out these sessions

- PLA1788 - Amazon Security Lake: Detections and Investigations Made Easy with OOTB Support
- SEC1779 - Federated Search: FINRA's Secret to Cost-Effective Scalable Security Analytics
- PLA1760 - Unlocking Security Insights from Amazon S3: How Splunk Cloud on AWS Users Effortlessly Utilize Federated Search on S3 for Security Analytics



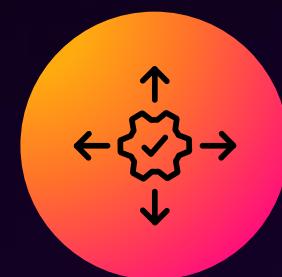
# SnapAttack Acquisition

A premier threat detection engineering platform, integrating directly into Splunk Enterprise Security



## Detection Strategy

Identify and prioritize threats based on existing detection coverage, data availability, and detectability and plan the detection development



## Threat Coverage

Measure detection coverage across the relevant threat landscape and enable easy detection development and deployment




## Continuous Testing


Ensure threats can be detected reliably, accurately, precisely, efficiently and actionably.



# Key Takeaways




Many exciting enhancements ahead of us!



Evaluate your install for tech debt and lookup bloat.



Pay attention to search tuning and scheduling.



Consider WLM for enhanced resiliency.

# Thank you

