The Economy of World of Warcraft

Making Millions of Gold and How Blizzard Knows You're Doing It, Using Splunk!

Shawn Routhier

Sr. Security Engineer | Blizzard Entertainment

Forward-Looking Statements

During the course of this presentation, we may make forward-looking statements regarding future events or plans of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results may differ materially. The forward-looking statements made in the this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, it may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements made herein.

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. Splunk undertakes no obligation either to develop the features or functionalities described or to include any such feature or functionality in a future release.

Shawn Routhier

Senior Security Engineer | Blizzard Entertainment

splunk> .conf20

Shawn Routhier

Human Rogue

Blizzard Entertainment - 5 years

- Security Professional for 11+ years… and counting
  - Booz Allen Hamilton, MIT – Lincoln Laboratory, Blizzard Entertainment

NPC “Shawn” in Nagrand (Outland)

- Met and proposed to my wife in WoW

Defcon25 Black Badge (Uber) Winner – Telephreak

Southern California User Group Leader

.Conf19 Speaker – Winning in Starcraft 2

Disclaimer

I'm not a WoW Dev

- I work on the Security Team at Blizzard
- I do not have any direct or indirect influence on World of Warcraft or it's development
- I cannot provide non-public information regarding Blizzard, World of Warcraft, etc.
  - For these questions, please email: pr <at> blizzard.com
- Please feel free to contact me with Splunk, Security, or WoW Economy-related questions
  - @0xShawn
  - Clock on Splunk Usergroups Slack

attr: Reddit - u/zulzulfie

Agenda

I'd like you to learn:

- Methodologies to normalize 100's of millions of events
- Parallels with SecOps, NetOps, SysOps, FraudOps
- Roadblocks, limits, & lessons learned
- Interesting WoW Metrics!

1. **World of Warcraft**
2. **Organizing the Objective**
3. **Summary Indexing & Lookups**
4. **Datamodels**
5. **Interesting WoW Metrics**

World of Warcraft

In the Age of Chaos, two factions battle for dominance!

World of Warcraft (2004); Classic (2019)

- Eight Expansions (2007, 2008, 2010, 2012, 2014, 2016, 2018, & 2020)

Massive Multi-Player Online Roleplaying Game (MMORPG)

- A networked role-playing game where a player adopts the role of a hero battling for their cause
- WoW is a high-fantasy themed game where players can adventure, dungeon delve, fight epic bosses, treasure hunt, or even go fishing!

Economy

- 10 Million+ pseudo-financial transactions per day
- An interesting data set for a universal problem


WORLD
OF
WARCRAFT
™

World of Warcraft Economy

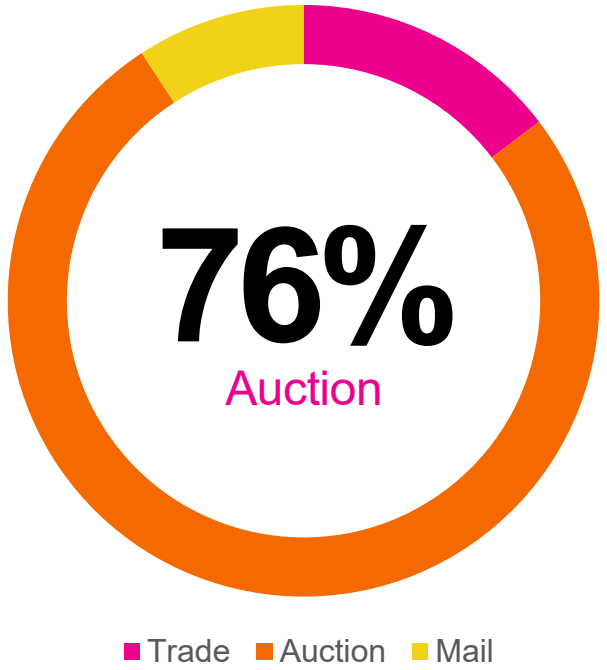
21 billion gold moves through WoW each day!

Abstract

- Correlating 100,000,000+ million events is difficult to scale with traditional SPL and search methods
- Utilizing summary indexing, lookups, and accelerated data models we can pre-calculate & correlate fields to reduce system resources used to search
- Methods to correlate thousands of events do not scale to hundreds of thousands.

Classic Transactions by Method

Retail Transactions by Method

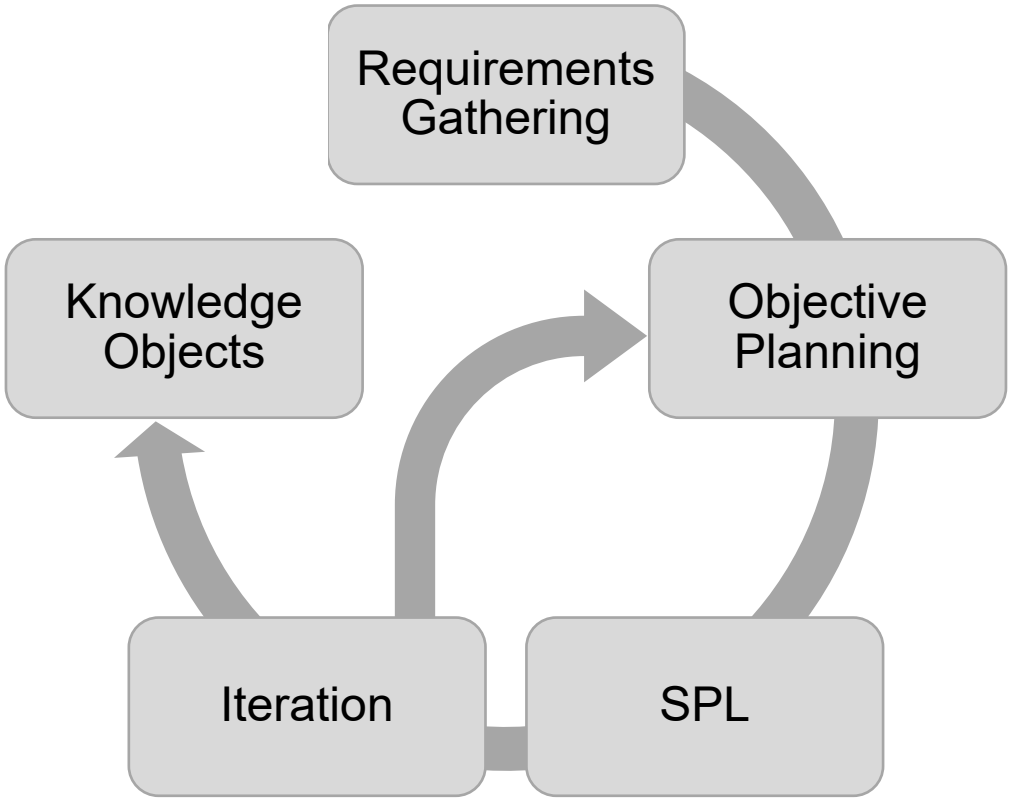


Organizing the Objective

Leeeeeeeeeroy Jenkins…

Process Oriented

- Requirements Gathering
  - Individual / team goals, expectations, ease of use, etc.
  - Dashboards, reporting, automation, integrations, etc.
- Objective Planning
  - "Simple, done well" – unknown
  - Ad-Hoc data enrichment & correlation
  - Frequency of summary index builders
  - Granularity for timeseries data
  - Lookup Insertion (Index-time OR search-time)
- Writing the SPL
- Iteration
  - Most difficult part: Knowing when to stop iterating
- Finalizing Knowledge Objects



Iterations

"Maybe we need another Healer?"

Breakdown of Efforts

- Requirements & Knowledge Objects – 5%
- Objective Planning – 45%
- SPL & Iteration – 50%

Major Refactors

- Dynamic Correlation -> Lookups
  - Reduced auto-finalization by 99%
- Item Value Overhaul
- Auction House update in v8.3
  - Required a new SI & correlation of two sourcetypes
- Item Value Overhaul 2.0

Total Gold Spent on Auctions by Realm Over 90 Days

Realm	Gold Trendline	Current
Azshara - KR Live		76072158.1398
Anzu - CN Live		15754152.2711
Area 52 - US Live		15674521.7752
Burning Blade - CN Live		14671499.4133
Stormrage - US Live		13913671.3360
Illidan - US Live		13896656.5570
Draenor - EU Live		12836609.8056
Silver Hand - CN Live		12280520.1803
Al'ar, Tortheldrin - CN Live		11720732.7942
Deathwing - CN Live		11456493.0070

Top 10 Auctioned Items' Value

itemName	Value Trendline	Current Value
Monelite Ore		10.0991
Riverbud		5.7036
Tidespray Linen		2.5035
Star Moss		9.4792
Zin'anthid		15.9332
Shal'dorei Silk		3.5605
Winter's Kiss		4.7160
Akunda's Bite		5.3950
Coarse Leather		3.3646
Deep Sea Satin		9.6951

WoW Event Metrics

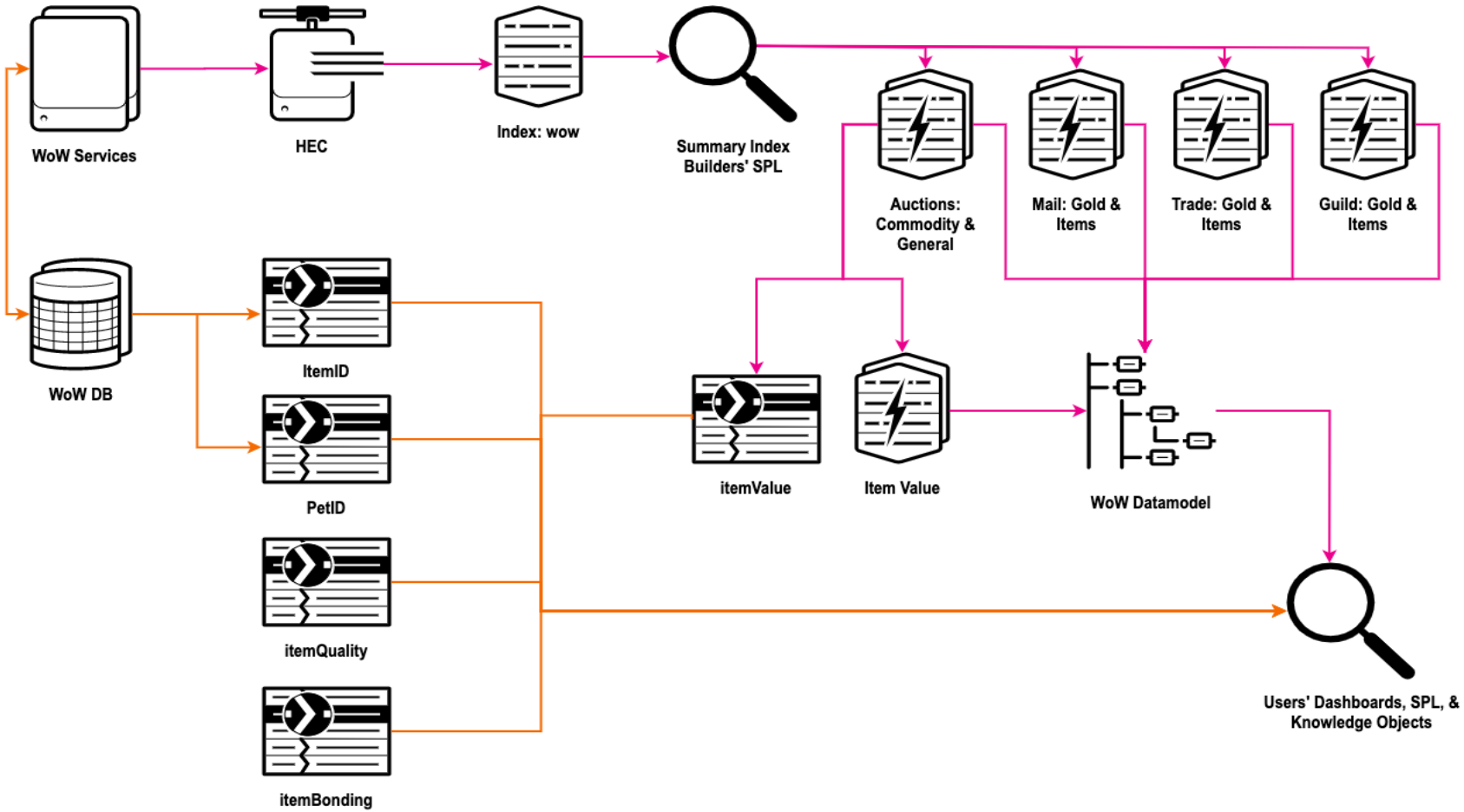
Summarizing & Accelerating at the Cost of Bag Space

	Simple WoW _raw	Summary Index	Accelerated Datamodel	Lookup
Format	JSON Structured _raw	KV Pair Structured _raw	Distributed TSIDX	CSV & KVStore
Location	Indexers	Indexers	Indexers	Search Heads Indexers • Replicated
Sample Search*	13,049,509,333 events 1,095.672 seconds	1,128,401,289 events 75.74 seconds	1,207,380,543 events 1.883 seconds	24,135,465 rows 210.079 seconds
Notes	• 90d retention • 95% of searches using >1 sourcetype would auto-finalize (fail)	• 97.23% reduction of storage • 24mon retention • By default, event distribution is poor with Summary Indexing	• 90d acceleration • 600 GB TSIDX with indexed buckets	• Efficient correlation • Enrich Summary Indexing • Offload common static fields

** All _raw & tstats searches are equivalent to: <base search> | bin span=1d _time | stats count by _time*

Data Flow Chart

As easy as playing Feral Druid



Summary Indexing

A Division of SI:7

Benefits

- Distribute computation expensive SPL to increase efficiency for extended timespan searches
- Normalize, correlate, lookup, and calculate fields at summary ingest
- Summary indexes have the same capabilities as a traditional index
  - Independent RBAC
  - Increased Retention
- Metricizing data
  - Economy data had a 97% _raw reduction

Drawbacks

- Summary time is reliant on scheduled interval
- Data redistribution is limited
  - Summary index events are written to disk as a ".stash_new" file
  - Default 30s load balance interval
- Changes to data are long-term investments
- Utilizing | Collect will also utilize license
- Unplanned execution of the summary builder will skew metrics

Summary Indexing

Auction SI Builder

```
earliest=-35m@m latest=-5m@m index=risk_wow sourcetype=blizzard:wow:auctionhouse message_name=AuctionHouse
| stats sum(payload.gold) as auctionGold sum(payload.item.stack_count) as auctionStacks by payload.from.bnet_guid, payload.from
    .player_guid, payload.item.enchants, payload.item.entry, payload.to.player_guid, payload.wow_context.realm_context.native_realm
    .realm_id, payload.wow_context.realm_context.native_realm.realm_region, payload.wow_context.realm_context.native_realm.realm_site
| rex field=payload.item.enchants "^Ench:(?<itemEnchant>.*)\sGems:(?<itemGems>.*)\sMods:(?<itemMods>.*)\sRandomPropertiesID
    :(?<itemPropsIDs>.*)\sContext:(?<itemContext>.*)\sBonuses:(?<itemBonuses>.*)$"
| rex field=itemMods "mod = 3, value = (?<petID>\d+)\)"
| fields - payload.item.enchants
| rename payload.from.bnet_guid as "sellerBNet", payload.from.player_guid as "sellerID", payload.item.entry as "itemID", payload.to
    .player_guid as "buyerID", payload.wow_context.realm_context.native_realm.realm_id as "realmID", payload.wow_context.realm_context
    .native_realm.realm_region as "realmRegion", payload.wow_context.realm_context.native_realm.realm_site as "realmSite"
| eval auctionGoldPerItem=floor(auctionGold/auctionStacks)
| lookup WoWEcon_itemID.csv itemID OUTPUT itemQuality itemBonding itemVendorBuy itemVendorSell itemDeleted
| eval petID=if(petID=="-NONE-", "0", 'petID')
| fillnull value="0" petID
| eval _time=now()
| table _time, sellerBNet, sellerID, buyerID, realmID, realmRegion, realmSite, itemID, itemQuality, itemBonding, auctionGold,
    auctionStacks, auctionGoldPerItem, itemEnchant, itemGems, itemMods, itemPropsIDs, itemContext, itemBonuses, itemVendorBuy,
    itemVendorSell, itemDeleted, petID
| collect index=wow_economy sourcetype=blizzard:wow:economy:auction
```

Summary Indexing

Commodity Auction SI Builder

```
earliest=-35m@m latest=-5m@m index=risk_wow message_name=AuctionEnd payload.reason IN (AUCTION_END_REASON_WON_BY_BID, AUCTION_END_REASON_BUYOUT)
| fields _time, message_name, payload.*, region
| rename payload.item_info{}.owner_context.* as seller_*, payload.item_info{}.* as seller_*, payload.buyer_context.* as buyer_*, payload.transaction_context
    .realm_context.native_realm.* as *
| eval seller_info = mvzip(seller_game_account_guid, seller_player_guid)
| eval seller_info = mvzip(seller_info, seller_item_id)
| eval seller_info = mvzip(seller_info, seller_stack_size_consumed)
| fields _time, message_name, buyer_bnet_account_id, buyer_game_account_guid, buyer_player_guid, seller_info, payload.sold_amount, payload.rake, payload.quantity,
    realm_id, realm_site, realm_region
| mvexpand seller_info
| rex field=seller_info "^(?<seller_game_account_guid>[^,]+),(?<seller_player_guid>[^,]+),(?<seller_item_id>[^,]+),(?<seller_stack_size_consumed>[^,]+)"
| eval auctionGold = floor('payload.sold_amount' / 'payload.quantity' * 'seller_stack_size_consumed')
    `comment("Removed the Rake calculation as it impacts historical item value by 10%")`
| eval auctionGoldPerItem = floor('auctionGold' / 'payload.quantity')
| rename buyer_bnet_account_id as buyerBNet, buyer_game_account_guid as buyerWoW, buyer_player_guid as buyerID, seller_game_account_guid as sellerWoW,
    seller_player_guid as sellerID, seller_item_id as itemID seller_stack_size_consumed as auctionStacks, realm_id as realmID, realm_region as realmRegion,
    realm_site as realmSite
| lookup WoWEcon_itemID.csv itemID OUTPUT itemQuality itemBonding itemVendorBuy itemVendorSell itemDeleted
| eval _time=now()
| table _time, sellerWoW, sellerID, buyerWoW, buyerID, realmID, realmRegion, realmSite, itemID, itemQuality, itemBonding, auctionGold, auctionStacks,
    auctionGoldPerItem, itemVendorBuy, itemVendorSell, itemDeleted
| collect testmode=f index=wow_economy sourcetype=blizzard:wow:economy:commodity
```

Lookups

/who

itemID	itemName	itemDesc	itemLevel	itemQuality	itemBonding	itemDeleted	itemVendorBuy	itemVendorSell	itemHoliday
17	Martin Fury	Test Martin Fury Programmer Test DO NOT DELETE	1	0	1	0	28	7	
25	Worn Shortsword	1H Starting Sword 01	1	1	0	0	18	3	
35	Bent Staff	2H Starting Stave 01	1	1	0	0	24	4	
36	Worn Mace	Starting Mace	1	1	0	0	19	3	
37	Worn Axe	1H Starting Axe 01	1	1	0	0	19	3	
38	Recruit's Shirt	Starting Shirt Human Dwarf Gnome Warrior Undead	1	2	2	0	1	1	
39	Recruit's Pants	Starting Pants Human Dwarf Gnome Warrior	1	1	0	0	13	2	
40	Recruit's Boots	Starting Boots Human Dwarf Gnome Undead Warrior	1	1	0	0	9	1	
41	OLDRecruit's Belt	HuWa Starting Belt 01	1	1	0	0	6	1	
42	OLDSquire's Belt	HuPa Starting Belt 01	1	1	0	0	6	1	

Benefits

- Translating programmatic IDs to human-readable
- Enrichment at summary index generation
- Default distribution of lookups to indexers
  - Note: Be careful on frequency of automated lookup builders.

itemQuality	itemQualityName
0	Poor
1	Common
2	Uncommon
3	Rare
4	Epic
5	Legendary
6	Artifact
7	Heirloom
8	Unique

itemBonding	itemBondingName
0	No Binding
1	Bind on Pickup
2	Bind on Equip
3	Bind on Use
4	Quest Item

Datamodels

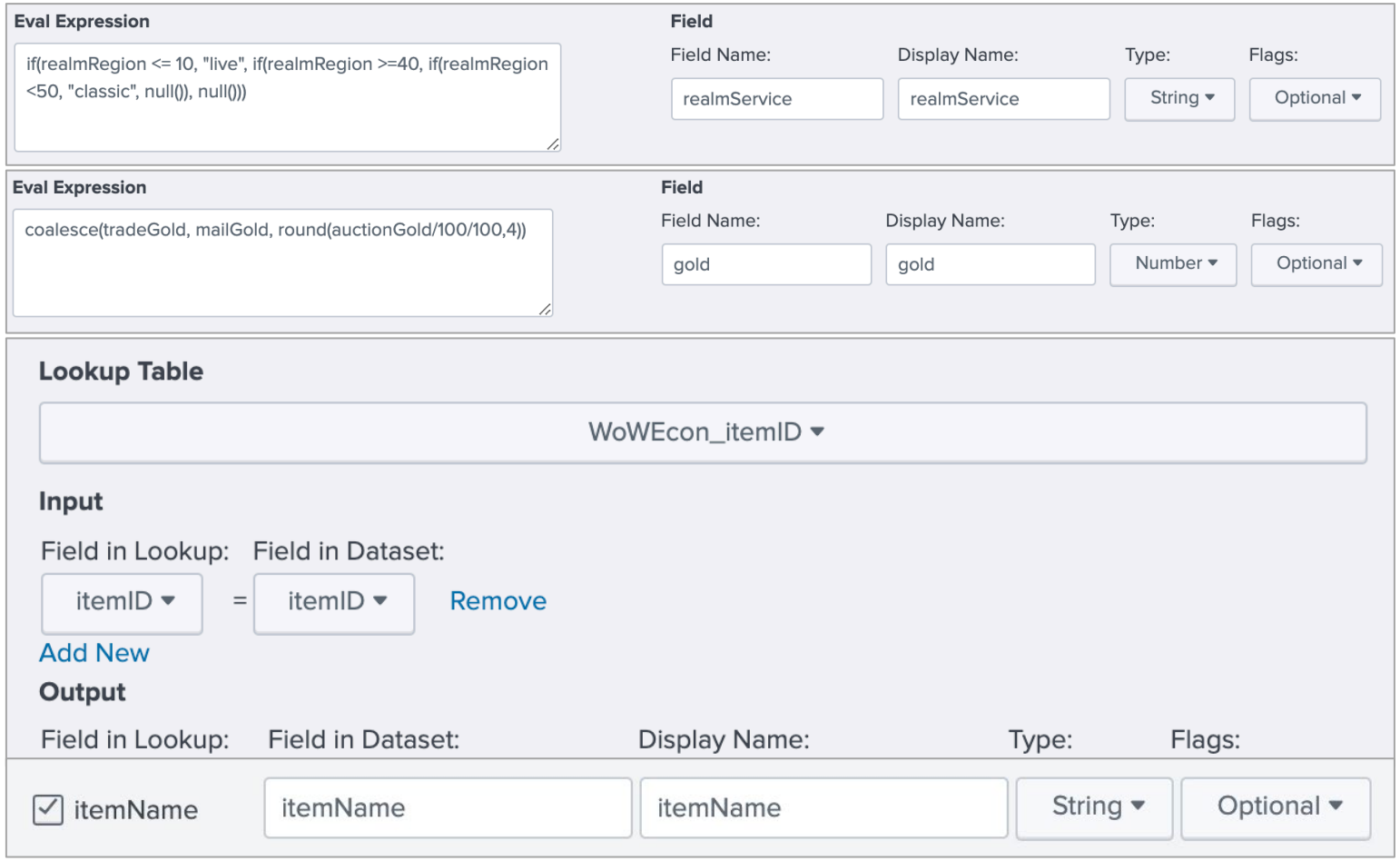
+ 20 Haste

Benefits

- Datamodels (DM) fields
  - Calculated fields using Eval
  - Automated lookup fields
- Extremely fast
  - 1.2 Billion events in 1.883 seconds

Drawbacks

- Learning curve
- Modifications require datamodel to be decelerated



Lessons Learned

Did Someone Say [Thunderfury, Blessed Blade of the Windseeker]?

SPL & Process

- "Simple, Done Well"
- Frequency of summary index builders
  - Meeting granularity requirements and expectations
- Correlation with Join or Subsearch is near-impossible
  - 50,000 & 10,000 event limits, by default
- Write a CIM for your data

Replication Configs

- distsearch.conf

```
[replicationSettings]
excludeReplicatedLookupSize = 50
```

- collections.conf

```
[wowecon_current_itemvalue]
replicate = false
```

Users

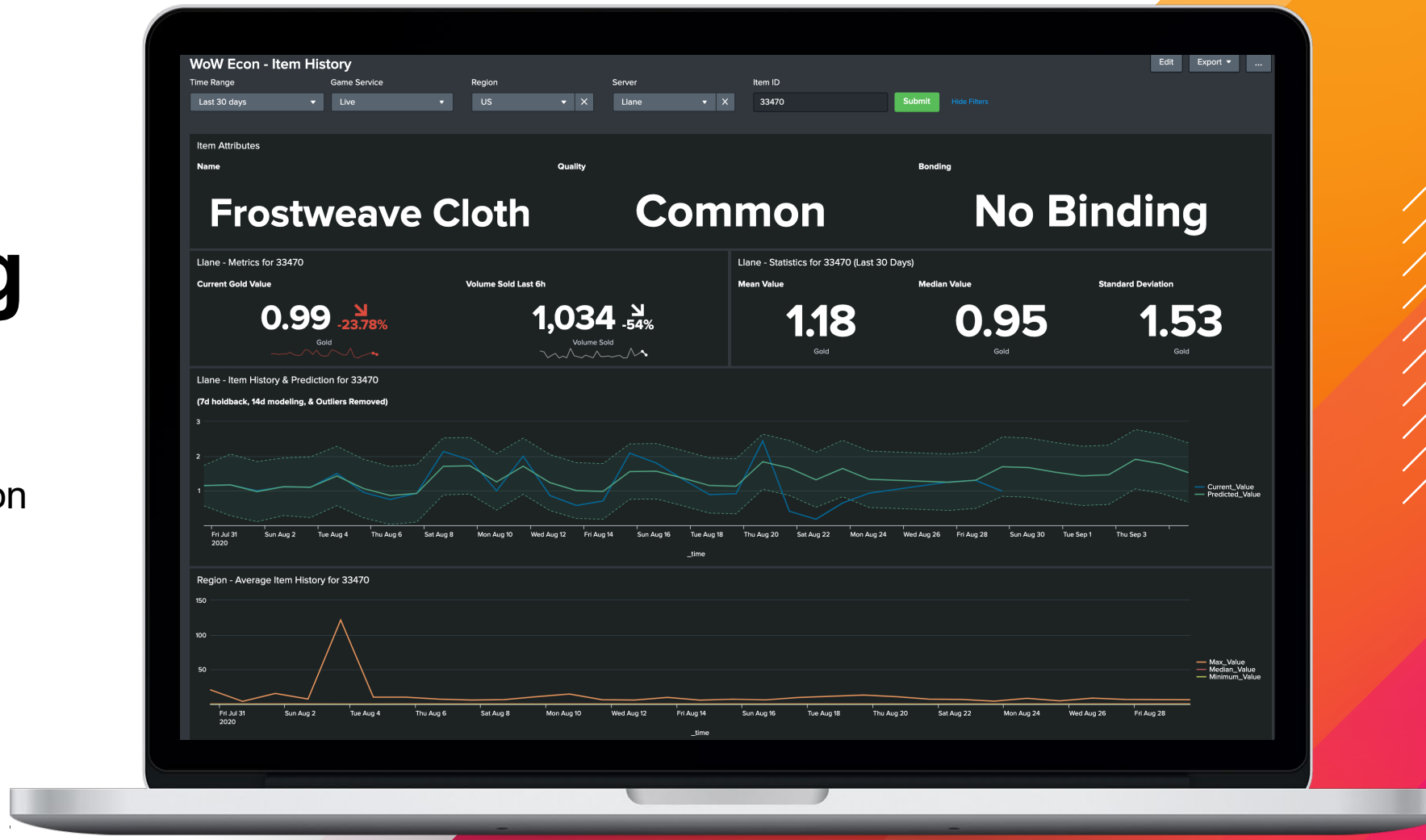
- Set expectations early. This is not a simple undertaking. Give yourself enough time.
- Users want to help. Plan accordingly.

Item Tracking

Proof of Concept…

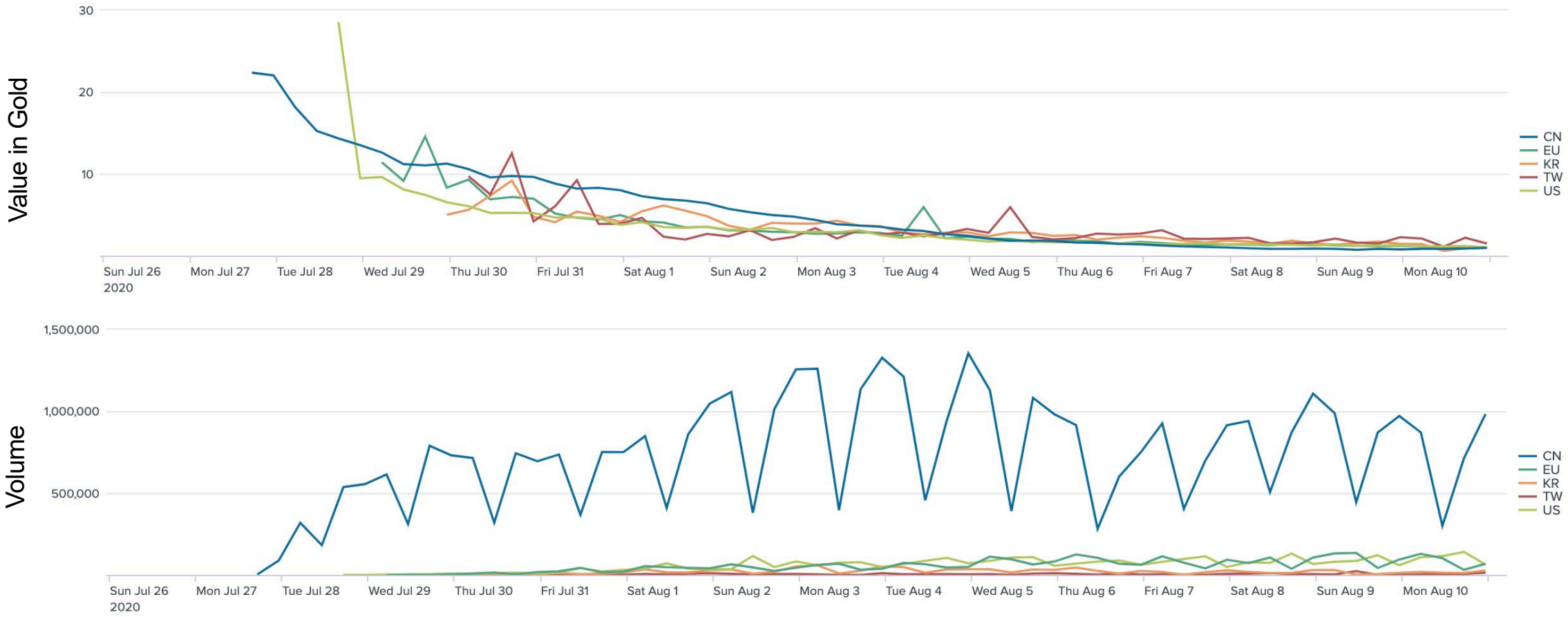
Premise for Automated Detection

- Historical & Trends
- Outliers
- Monitoring Accounts



Opening the Gates of Ahn'Qiraj

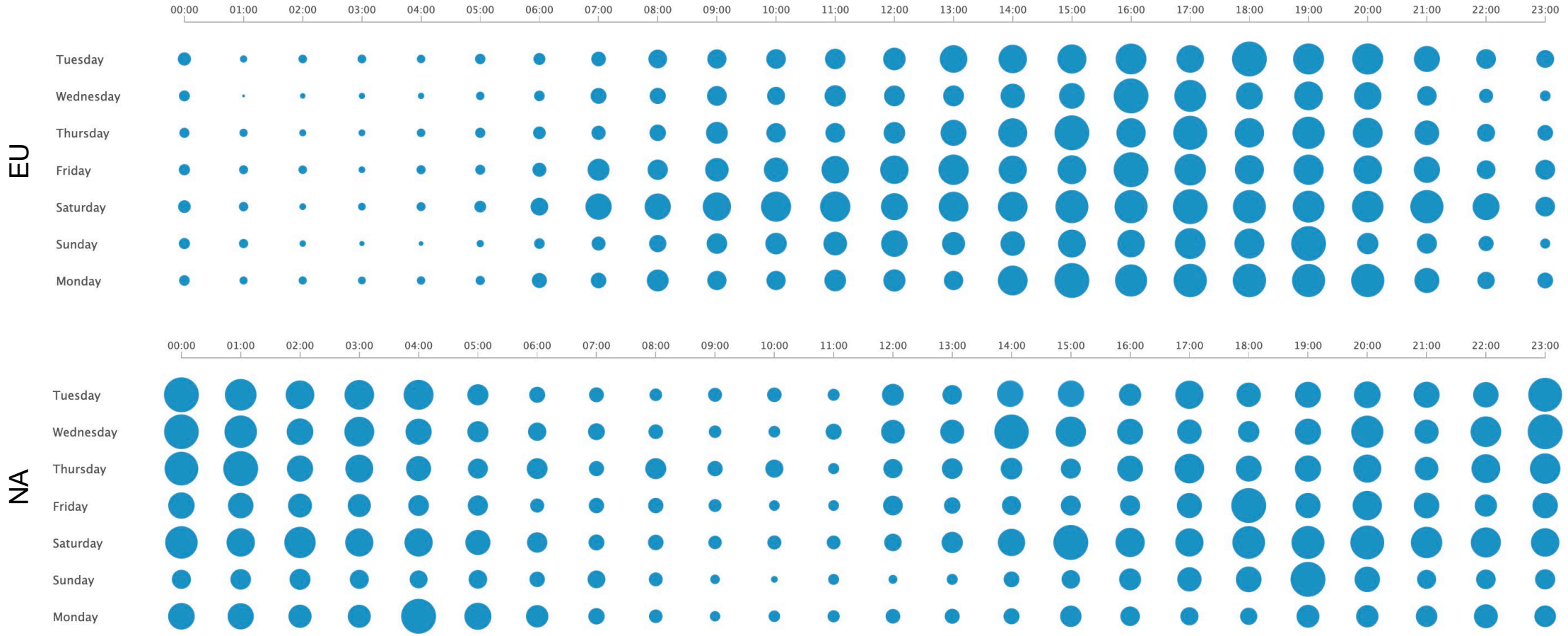
Silithid Carapace Fragments Sold on AH per Region



splunk> .conf20

When to Sell?

Day of Week & Time of Day (UTC) Auction Volume



Note: Splunk Created "Punchcard" Viz

splunk> .conf20

Who's Buying?

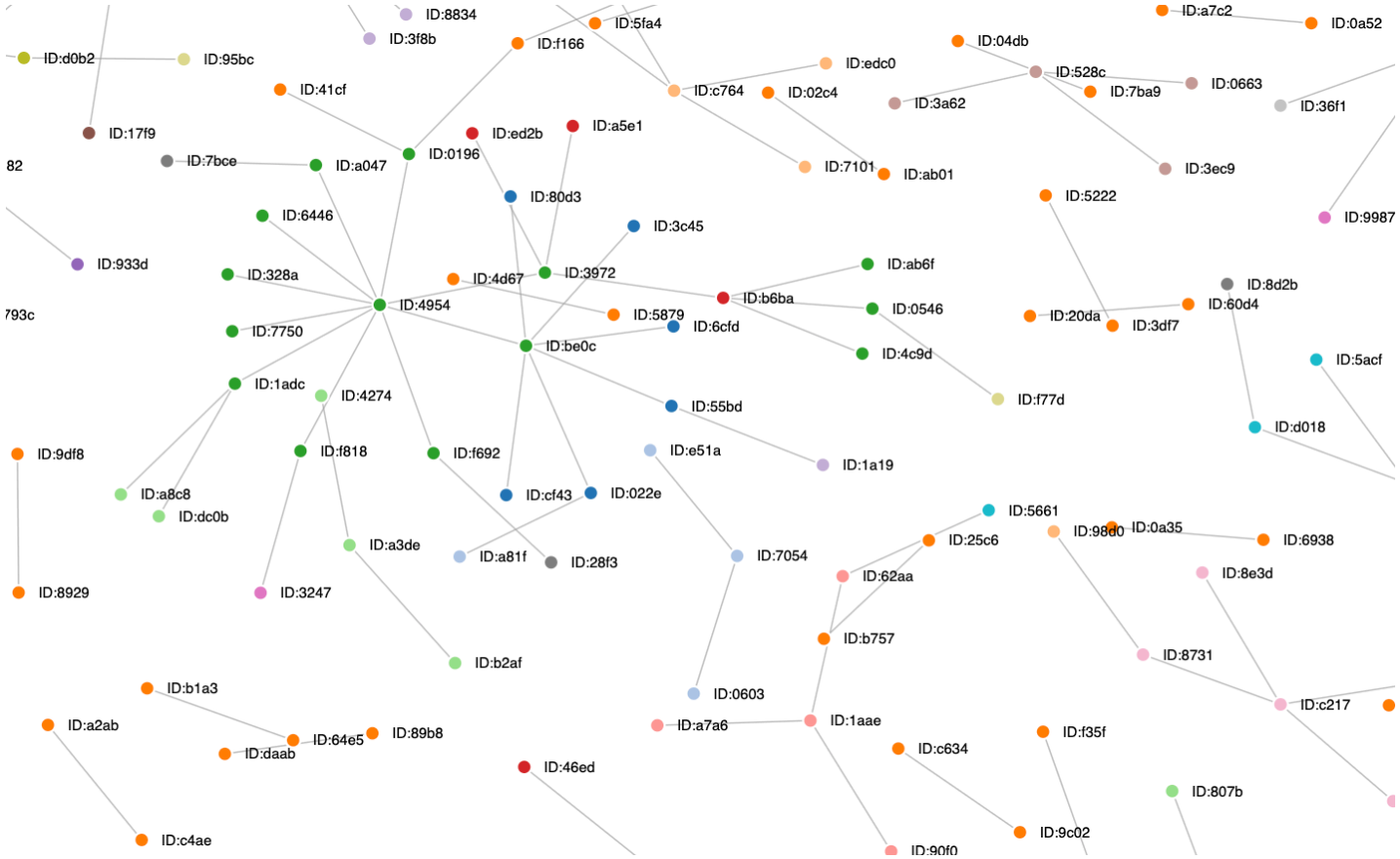
WTB Blacksmith Hammer PST

Visualizing Relationships

- Anomalous purchasing behaviors
  - Purchasing above expected values
- Automating detections of Gold Sellers
  - Maintaining Monitoring via Lookup & DMA

```
| where
    (auctionGold > auctionAGPI + auctionStD * 3) OR
    (auctionGold > auctionMax * 2) OR
    (auctionGold > auctionAGPI * 1.5 AND auctionRange * 1.5)

| where
    (isnotnull(monitored) AND outlier > 3)
```



Note: Example filtering, not production.

Note: Splunk Works Created "Force Directed App" Viz

splunk> .conf20

Applicability

+ 20 Versatility

	Security	Network	System	Fraud
Existing Datamodels	• Authentication • Endpoint • Malware • Vulnerabilities	• Network Sessions • Network Resolution • Network Traffic • Web	• Databases • Inventory • Updates	• None • Make your own!
Use Cases	• New Authentication • New Services, Daemons, Reg Keys, etc.	• New Executables Downloaded • Traffic to New IPs or Domains	• Change Control Validation • New Public-facing IPs	• Payment Fingerprinting - bin, billing, currency, ip, isp, pos • In-Game Detections

Existing Resources and CIM

- Splunk CIM app on Splunkbase (required for ES)
- Extensive Documentation on CIM

Thank You

Please provide feedback via the

SESSION SURVEY