
13TH ANNUAL LEADERSHIP EVENT
CYBER SECURITY SUMMIT
cybersecuritysummit.org
RESILIENCE UNLOCKED
TITLE SPONSOR
Island
#cybersecuritysummit #css13

Three Ways to Use An Observability Pipeline to Transform Your SIEM

SIEM architecture is holding Cybersecurity teams back!

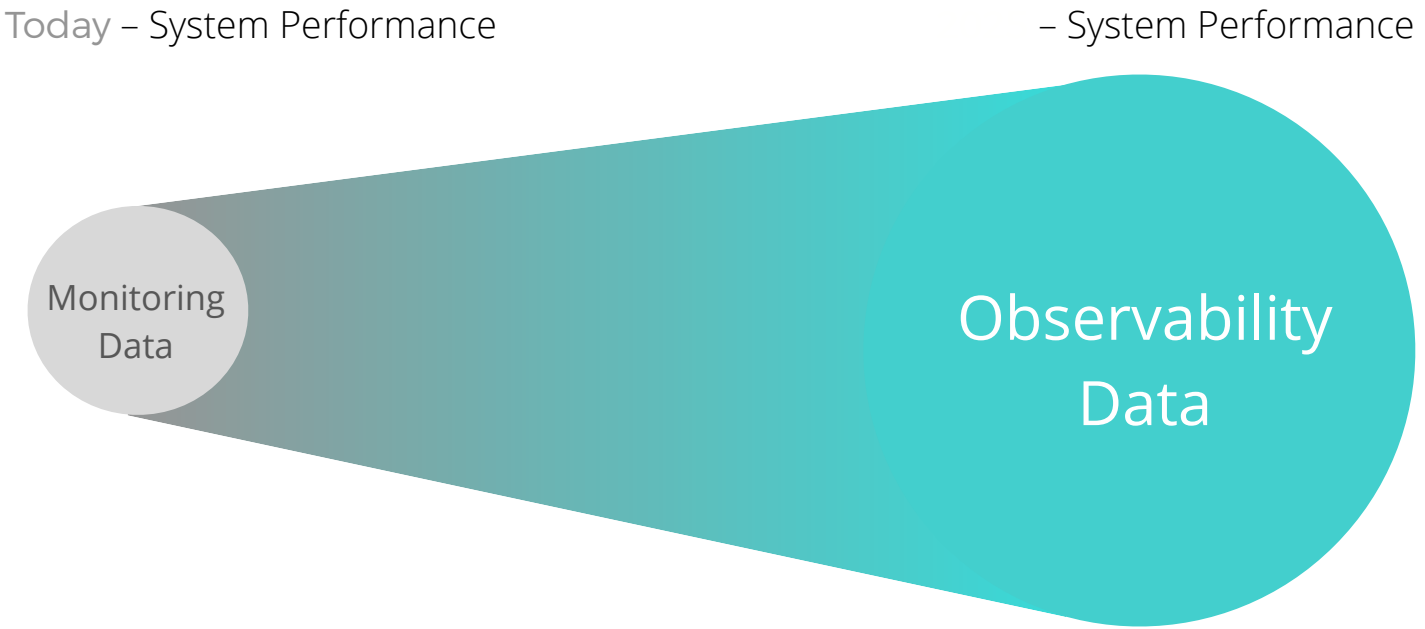
Ed Bailey

Senior Staff Technical Evangelist

Cribl, Inc.

The **struggle**.

Distributed Systems Driving Evolution

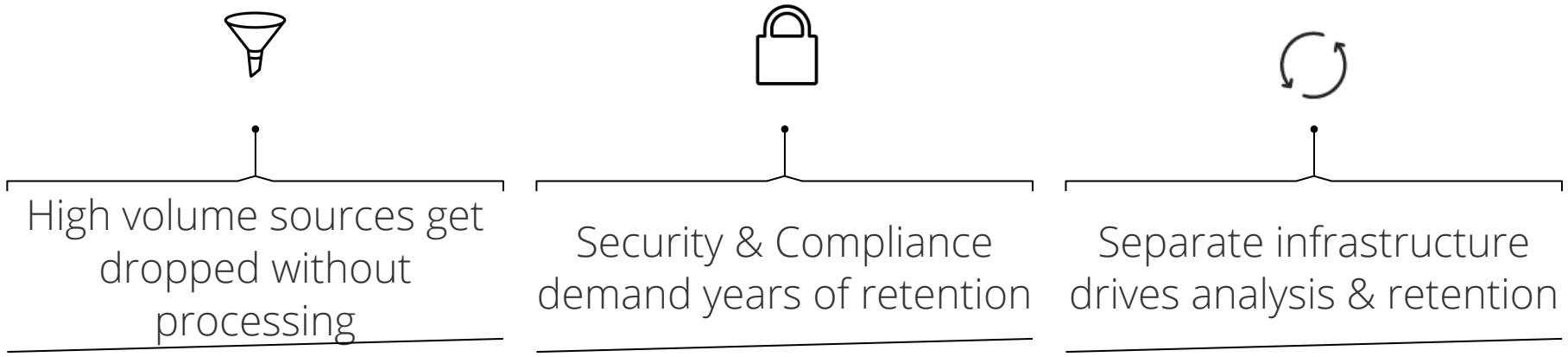


The average enterprise has
10 or more tools for security/analytics

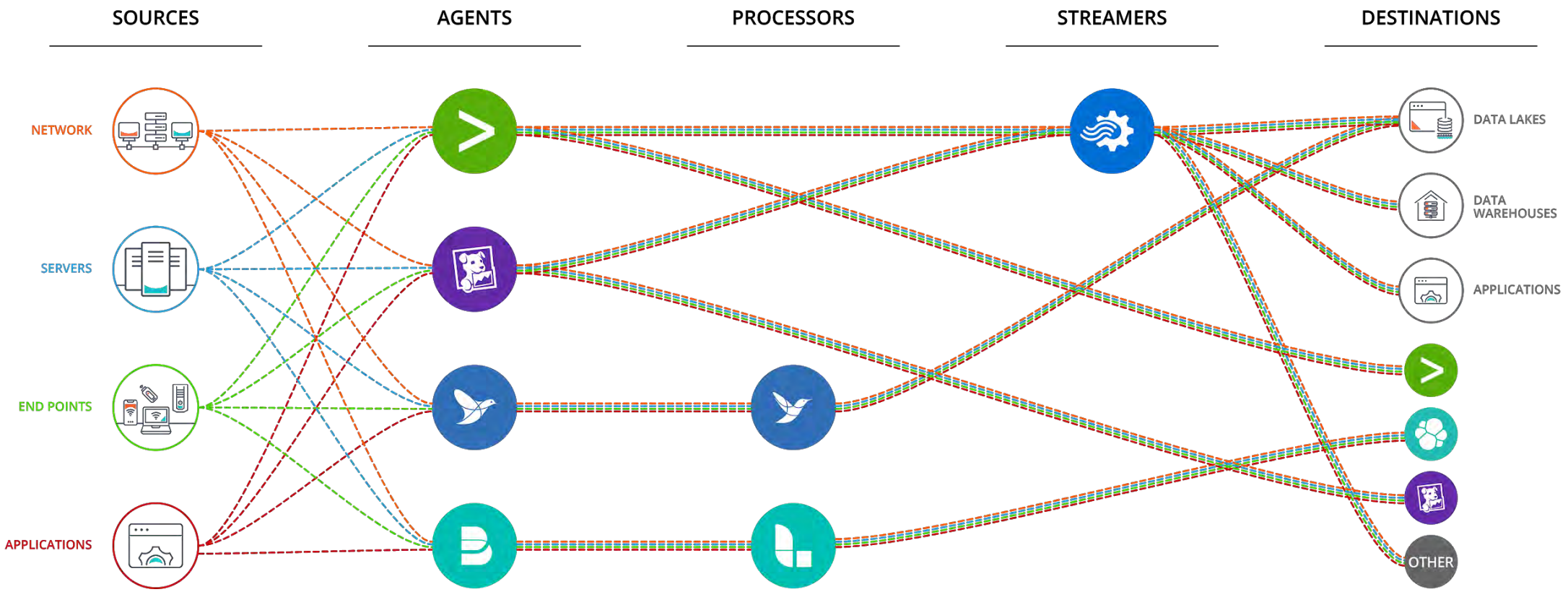
By 2025, enterprises will be managing
250% more data than in 2020!

Organizations are Retaining More & Longer

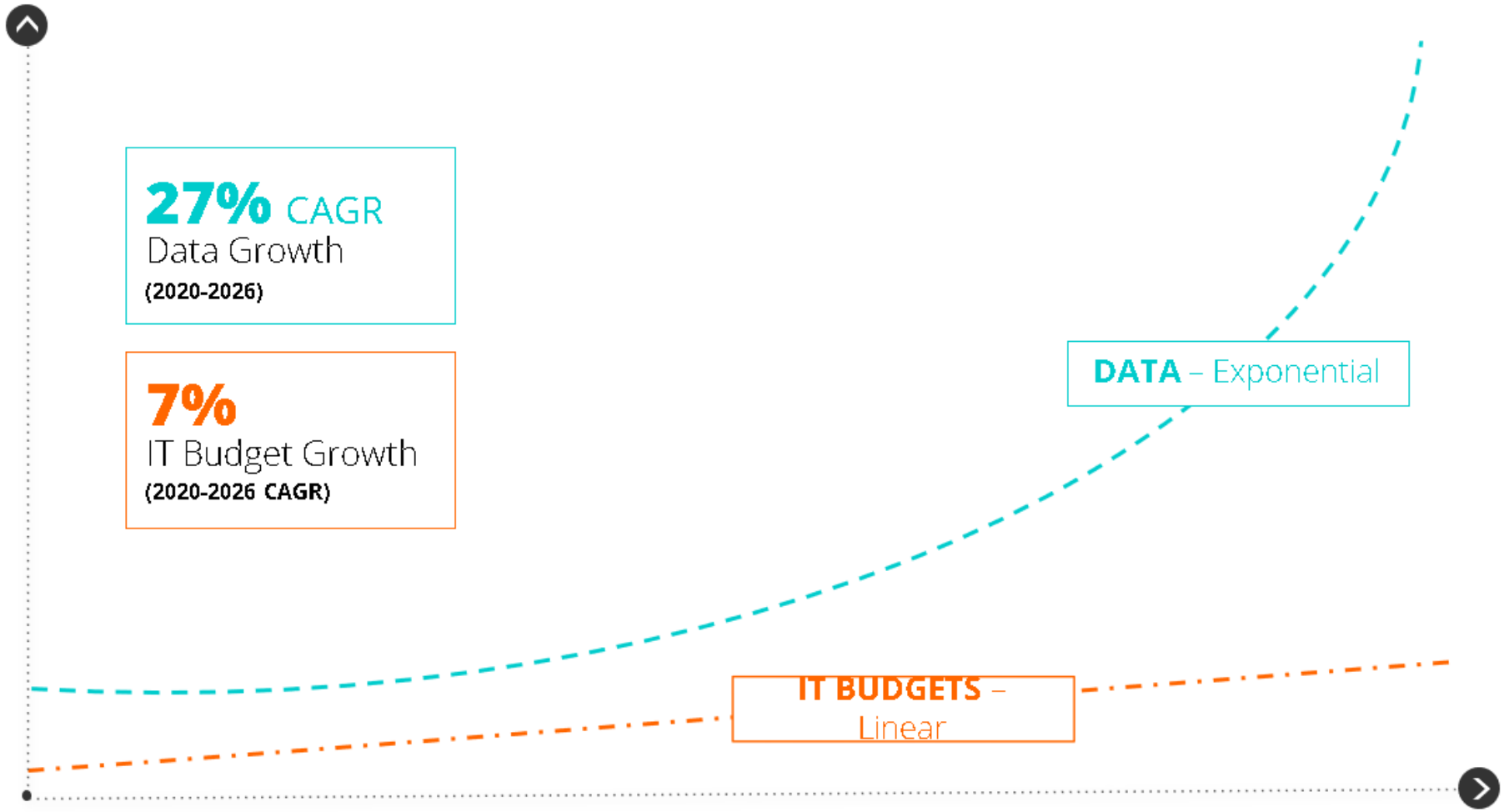
We have a long backlog of data sources to onboard —
more than **5 times the capacity** we have!



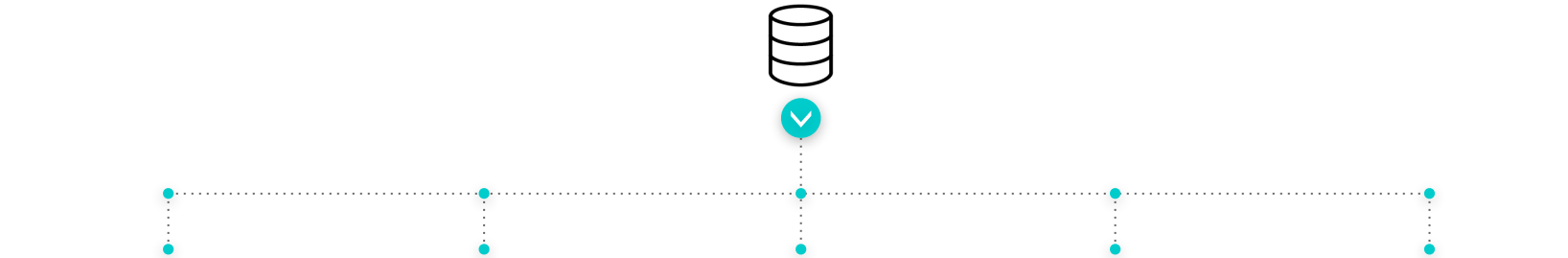
Collect Data by Exclusion: Complex & Inflexible



Budgets Aren't Keeping Up



So Data Management is Evolving...



Object Storage
Cheap storage for long-term retention

Time Series Databases
Optimized for fast time-series analysis

Indexed Log Analytics
Powerful engines for investigations and searches

SIEM / UEBA
Great for security incident correlation and user analytics

Data Lakehouses
Storage for long-term retention and analysis

.....but each requires its **own agent** and **ingestion pipeline**!

Security Monitoring is Evolving...

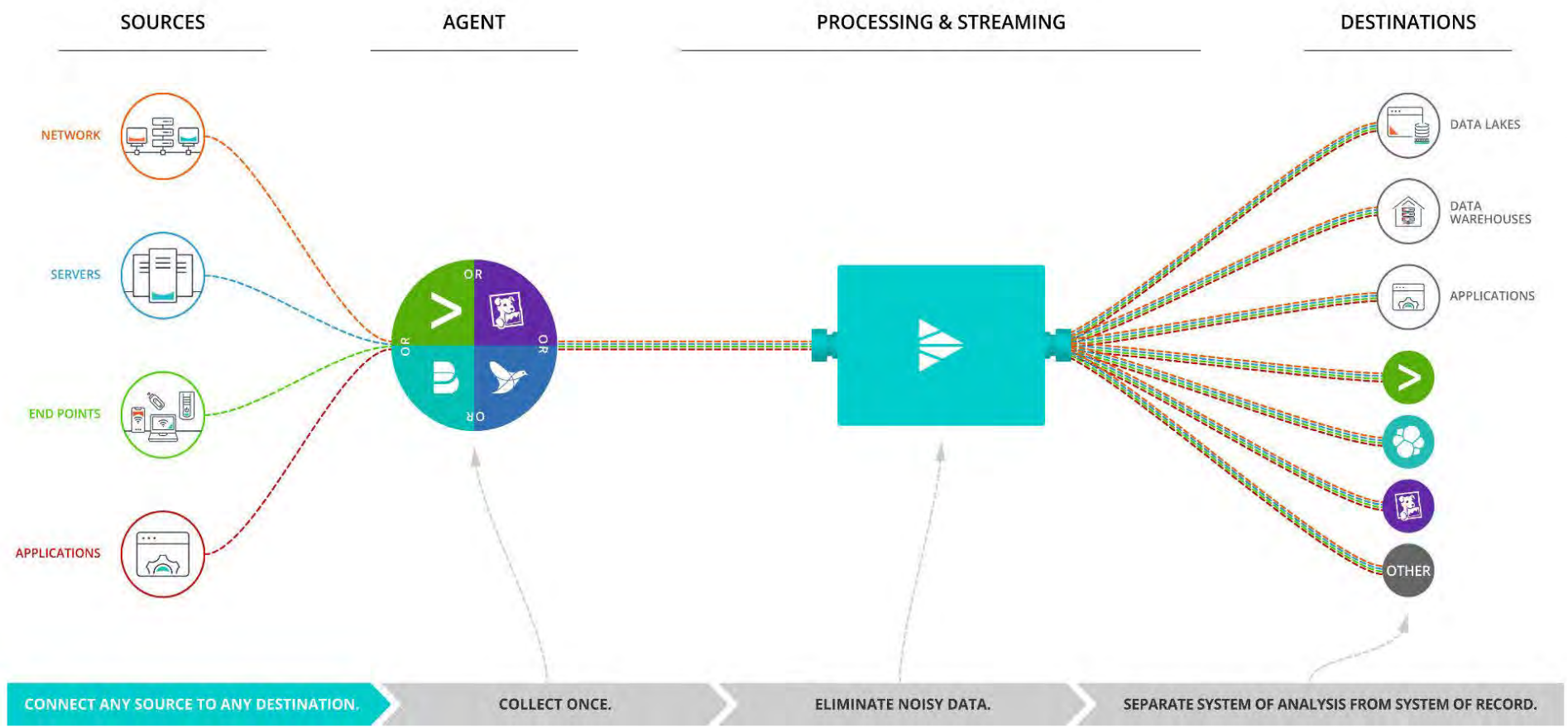
Transform your traditional **SIEM architecture**.

Need to Instrument More While Paying Less

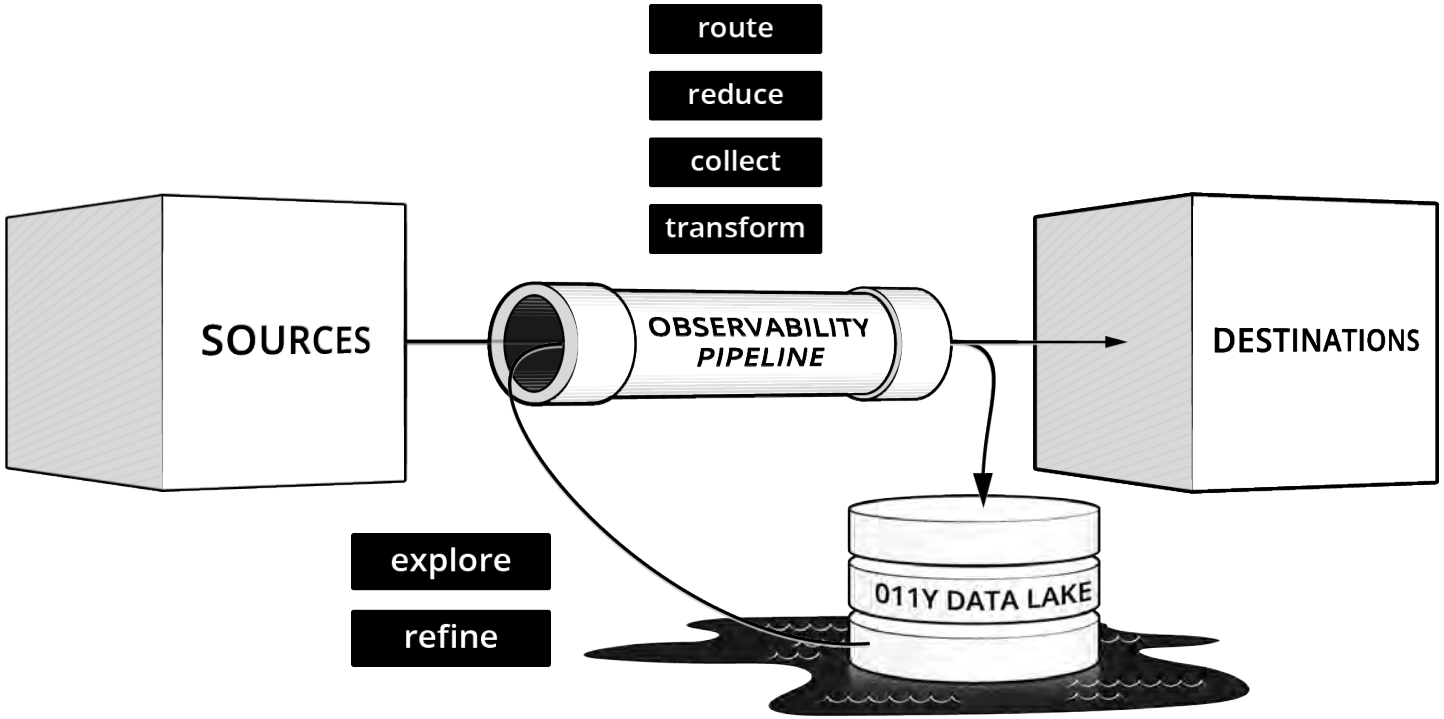
FIND THE MIDDLE GROUND

BETWEEN WHAT YOU REQUIRE AND WHAT YOU CAN AFFORD

Next Generation Pipeline Architecture



The Future of Security Observability



Benefits of an Observability Pipeline

1

Choice and control over your
data and tool selection.

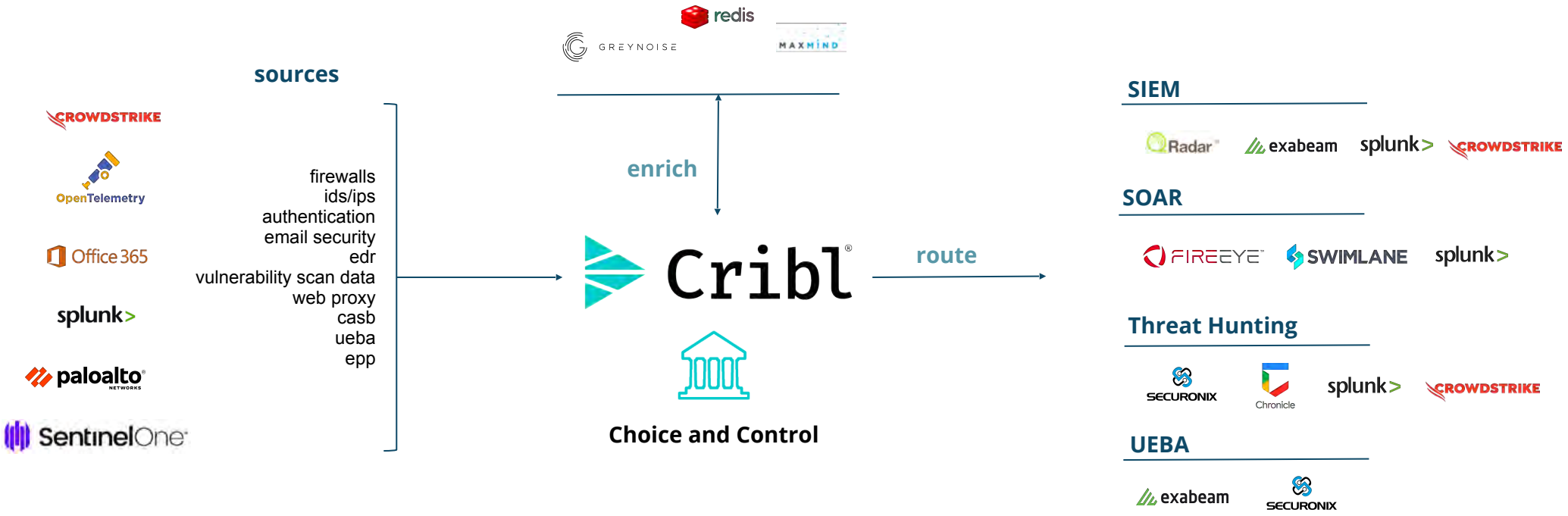
2

Better value from your SIEM
and analysis platforms.

3

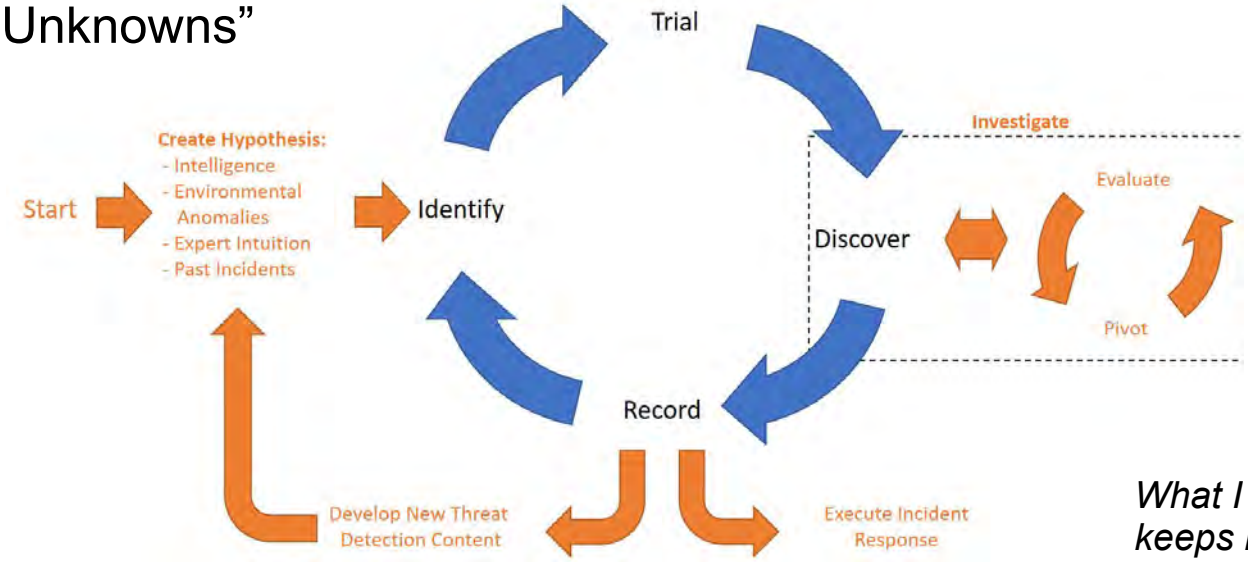
Options to optimize your costs.

Bringing it all together



Threat Hunting Is Observability

Threat Hunters are always looking for "Unknown Unknowns"



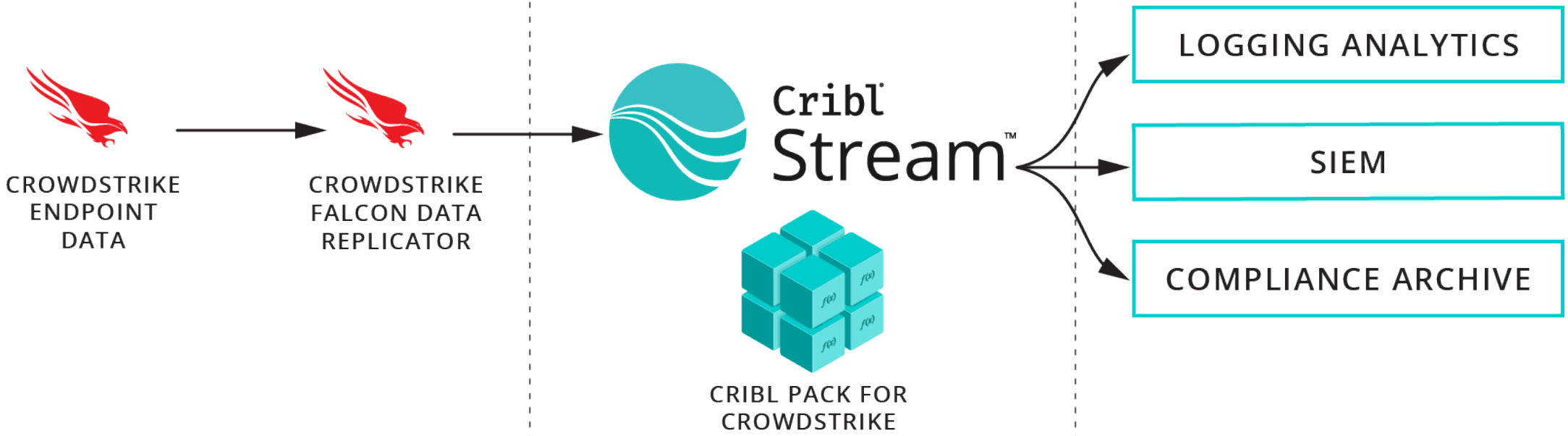
What I don't know about is what keeps me up at night. What are we missing is what scares me. IR Lead Fortune 100 financial

CrowdStrike & Cribl Architecture

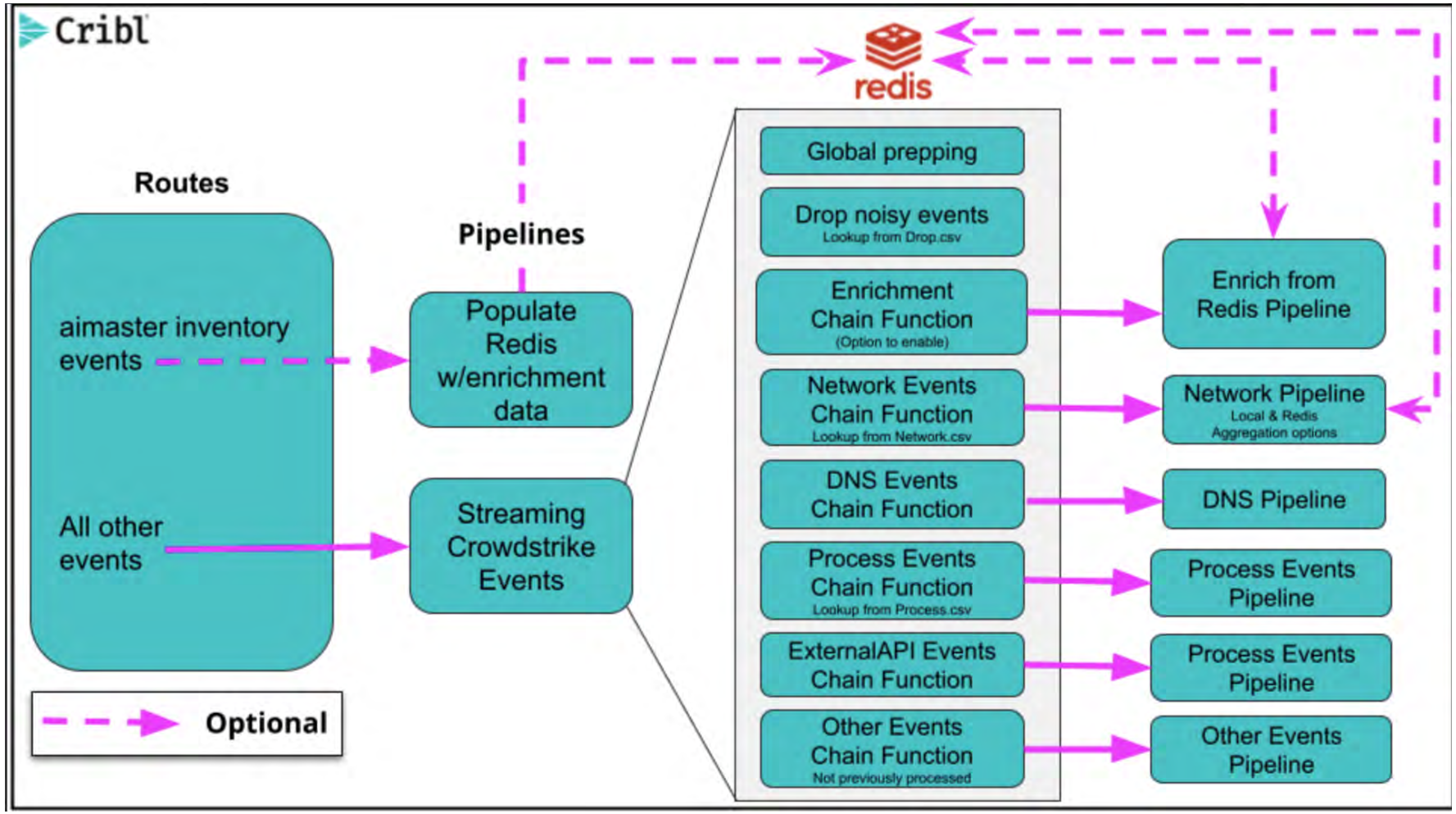
Endpoint data is collected and analyzed in CrowdStrike FDR.

Cribl Stream extracts data from FDR, enriches and redacts it, then routes to your destinations in the right data format.

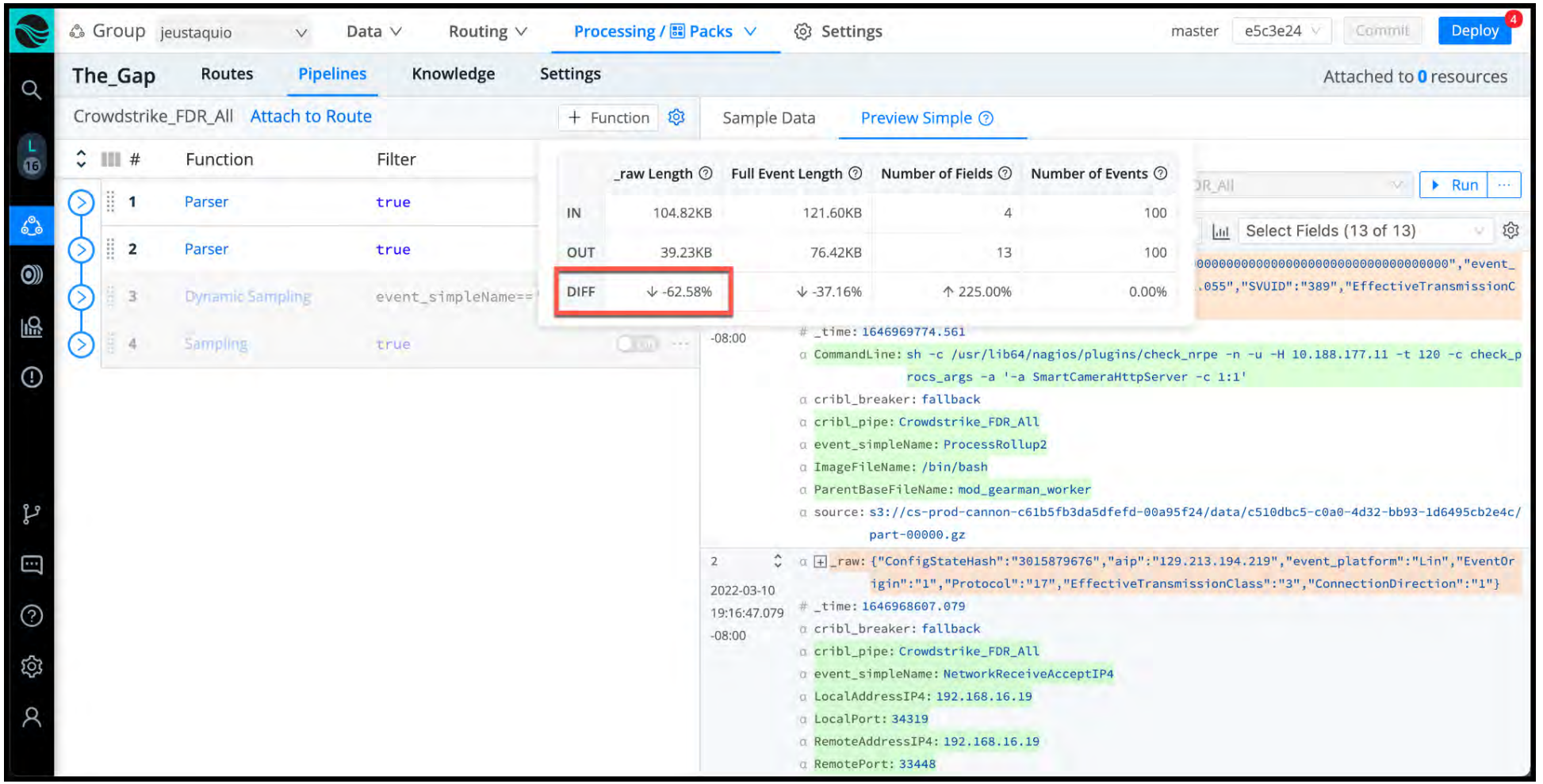
Destinations process, store, and analyze data, giving you a complete security picture.



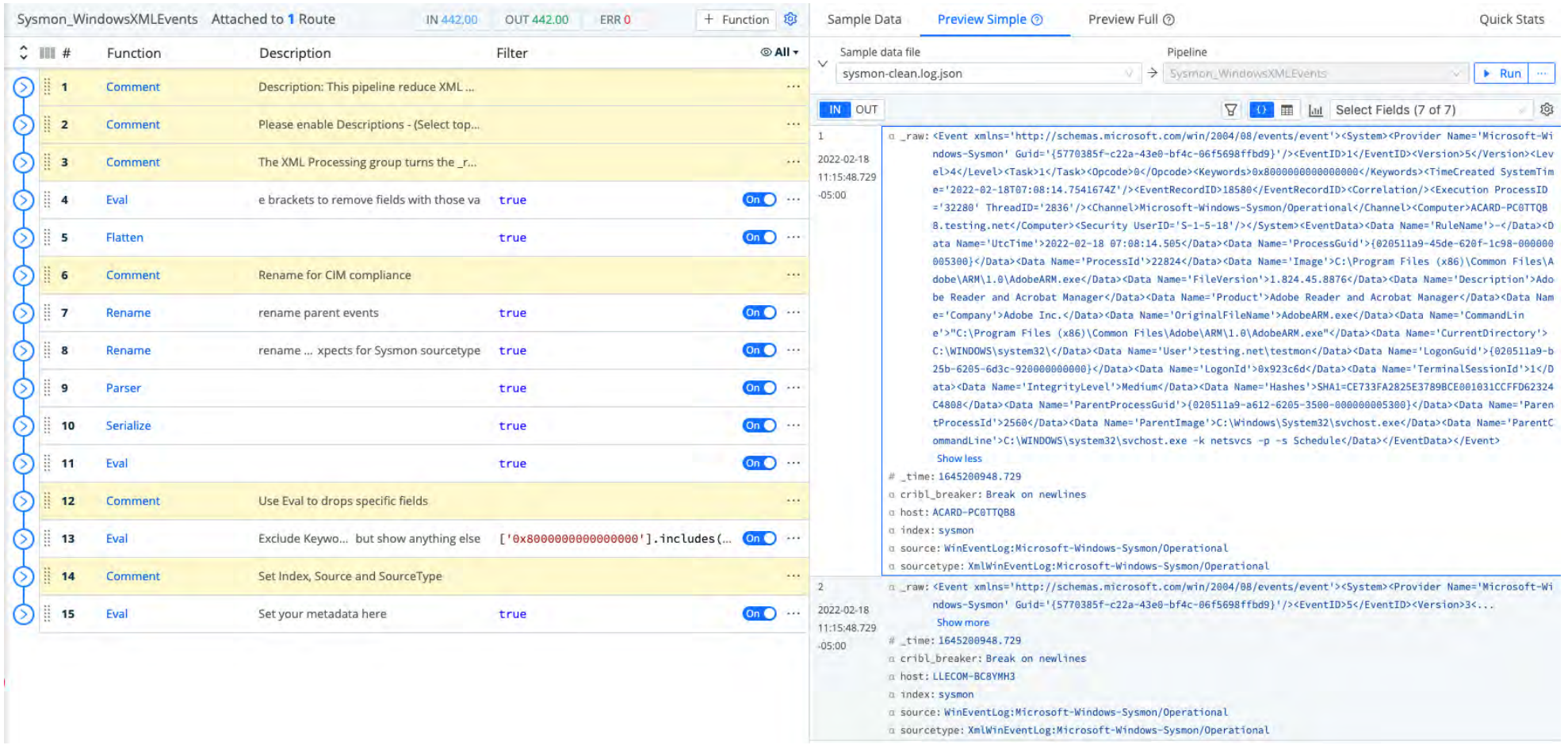
CrowdStrike FDR Cribl Pack Workflow



Less Data – Better Data



Common Security Data Use Case



Bad Data - Difficult Detections

1

2022-02-18
11:15:48.729
-05:00

▫ _raw: <Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2022-02-18T07:08:14.7541674Z'/><EventRecordID>18580</EventRecordID><Correlation/><Execution ProcessID='32280' ThreadID='2836'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>ACARD-PC0TTQB8.testing.net</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2022-02-18 07:08:14.505</Data><Data Name='ProcessGuid'>{020511a9-45de-620f-1c98-000000005300}</Data><Data Name='ProcessId'>22824</Data><Data Name='Image'>C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\AdobeARM.exe</Data><Data Name='FileVersion'>1.824.45.8876</Data><Data Name='Description'>Adobe Reader and Acrobat Manager</Data><Data Name='Product'>Adobe Reader and Acrobat Manager</Data><Data Name='Company'>Adobe Inc.</Data><Data Name='OriginalFileName'>AdobeARM.exe</Data><Data Name='CommandLine'>"C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\AdobeARM.exe"</Data><Data Name='CurrentDirectory'>C:\WINDOWS\system32\</Data><Data Name='User'>testing.net\testmon</Data><Data Name='LogonGuid'>{020511a9-b25b-6205-6d3c-920000000000}</Data><Data Name='LogonId'>0x923c6d</Data><Data Name='TerminalSessionId'>1</Data><Data Name='IntegrityLevel'>Medium</Data><Data Name='Hashes'>SHA1=CE733FA2825E3789BCE001031CCFFD62324C4808</Data><Data Name='ParentProcessGuid'>{020511a9-a612-6205-3500-000000005300}</Data><Data Name='ParentProcessId'>2560</Data><Data Name='ParentImage'>C:\Windows\System32\svchost.exe</Data><Data Name='ParentCommandLine'>C:\WINDOWS\system32\svchost.exe -k netsvcs -p -s Schedule</Data></EventData></Event>

Show less

_time: 1645200948.729
▫ cribl_breaker: Break on newlines
▫ host: ACARD-PC0TTQB8
▫ index: sysmon
▫ source: WinEventLog:Microsoft-Windows-Sysmon/Operational
▫ sourcetype: XmlWinEventLog:Microsoft-Windows-Sysmon/Operational

Better Data – Better Detections

	_raw Length	Full Event Length	Number of Fields	Number of Events
IN	218.04KB	253.39KB	7	154
OUT	146.92KB	183.18KB	7	154
DIFF	↓ -32.62%	↓ -27.71%	0.00%	0.00%

Bringing it all together.

Benefits of an Observability Pipeline

Organize for Success - People and Process still the foundation

Breakdown organizational Silos

Benefits of an Observability Pipeline

Create a foundation of good data

How to Transform your SIEM Archtecture

In the next month

Gap analysis and Research

Define requirements

Over the next 90 days…Build your Plan

Meet with management and EA owner

Look for allies, security, ops, GRC

Within the next six months…Sell your Plan

Present your proposal to leadership

Rinse and Repeat – Don’t give up

Want to See It for Yourself?

Cribl

Demo Stream today in our sandboxes!

https://sandbox.cribl.io

Sign up for a FREE account!

Cribl.Cloud

https://cribl.cloud

Q&A

Thank You

Contact Us

Cribl, Inc. 44 Tehama St. San Francisco, CA 94105
Sales Inquiries hello@cribl.io
Career Opportunities jobs@cribl.io
Join our Community https://cribl.io/community
Visit Us http://www.cribl.io