

13TH ANNUAL LEADERSHIP EVENT



# CYBER SECURITY SUMMIT

[cybersecuritysummit.org](http://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.



**CYBER SECURITY**  
www.cybersecuritysummit.org **SUMMIT**

13th Annual Cyber Security Summit | October 24-26, 2023



#cybersecuritysummit #css13

RESILIENCE  
**UNLOCKED**

A decorative graphic in the bottom right corner featuring a globe with glowing blue data lines and a network-like structure.

**The struggle.**



**CYBER SECURITY**  
www.cybersecuritysummit.org **SUMMIT**

13th Annual Cyber Security Summit | October 24-26, 2023



#cybersecuritysummit #css13

RESILIENCE  
**UNLOCKED**

COPYRIGHT © 2023 CRIBB, INC. ALL RIGHTS RESERVED.

A decorative graphic in the bottom right corner featuring a blue and white globe with glowing data lines and a grid pattern, set against a dark blue background.



# Distributed Systems Driving Evolution

Today – System Performance

– System Performance



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

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



**CYBER SECURITY**  
SUMMIT  
www.cybersecuritysummit.org

13th Annual Cyber Security Summit | October 24-26, 2023

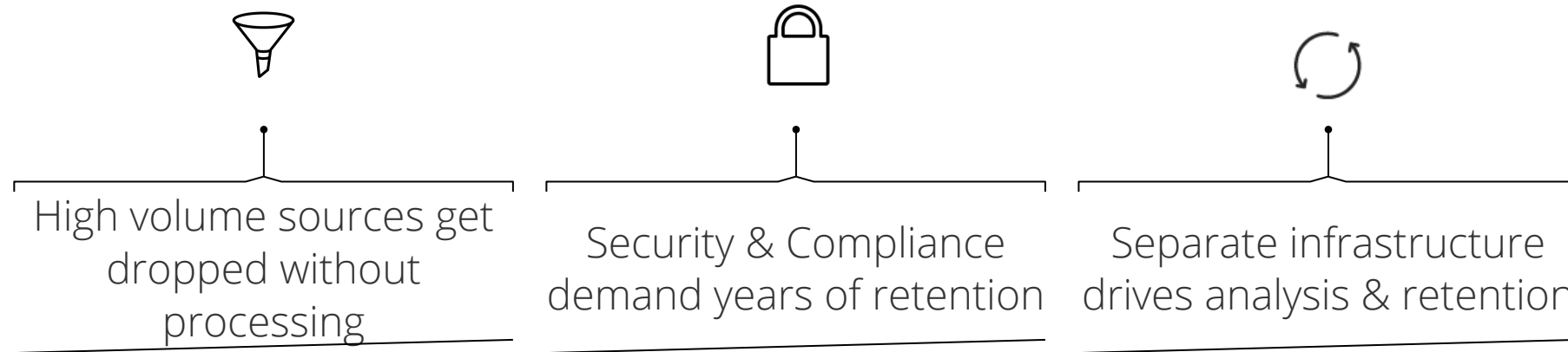


#cybersecuritysummit #css13

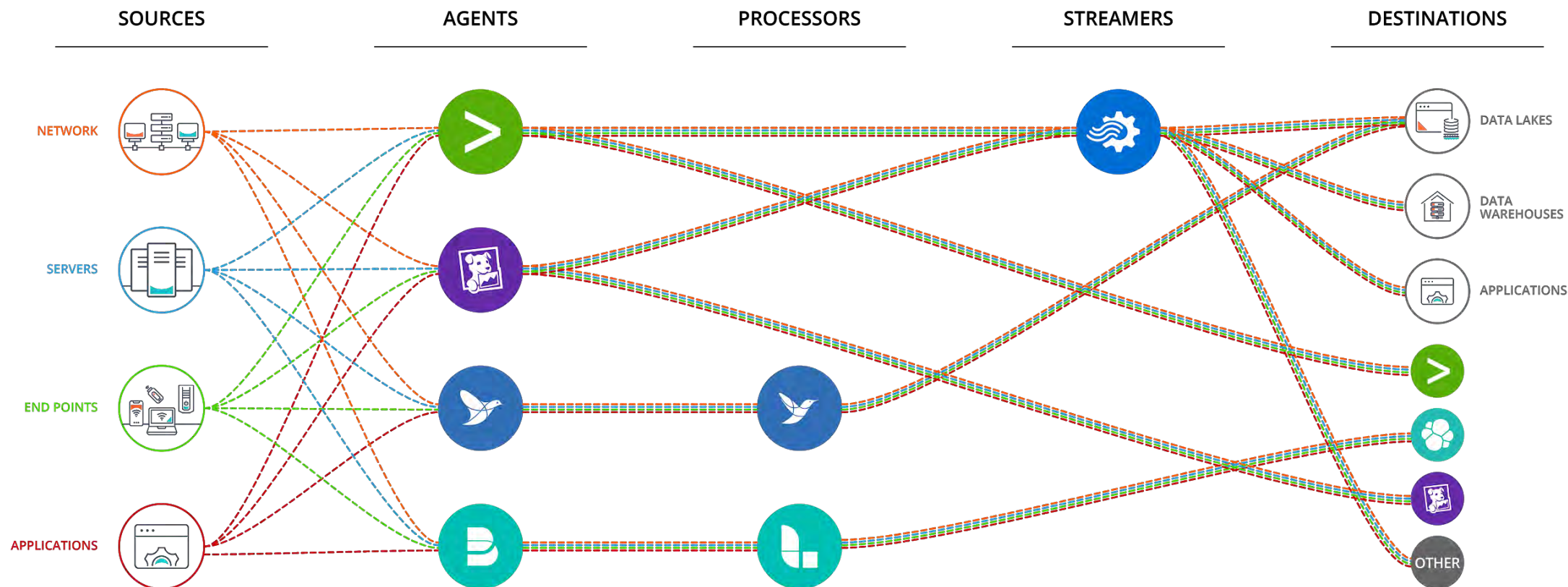
RESILIENCE  
UNLOCKED

# Organizations are Retaining More & Longer

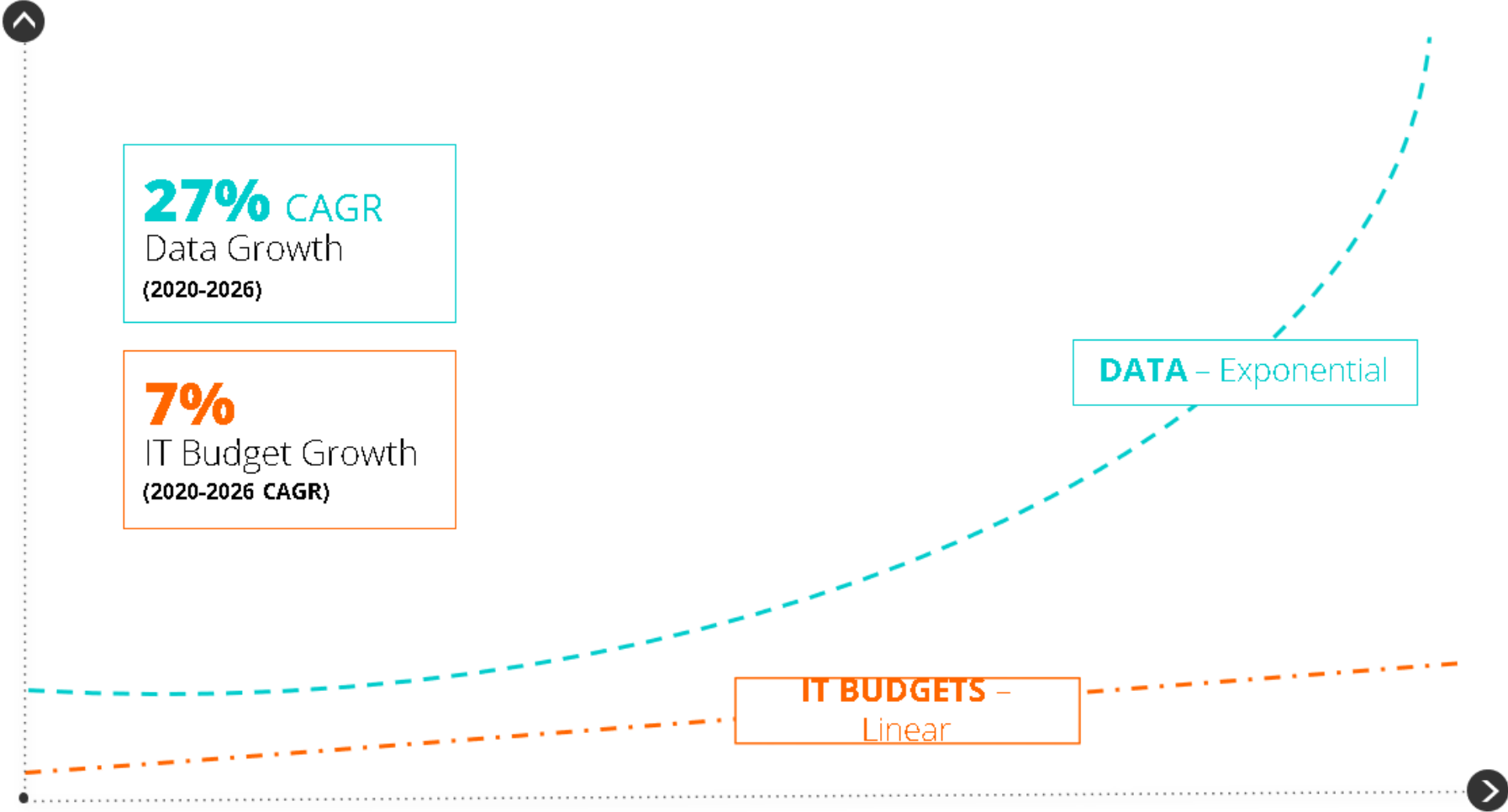
We have a long backlog of data sources to onboard — more than **5 times the capacity** we have!



# Collect Data by Exclusion: Complex & Inflexible

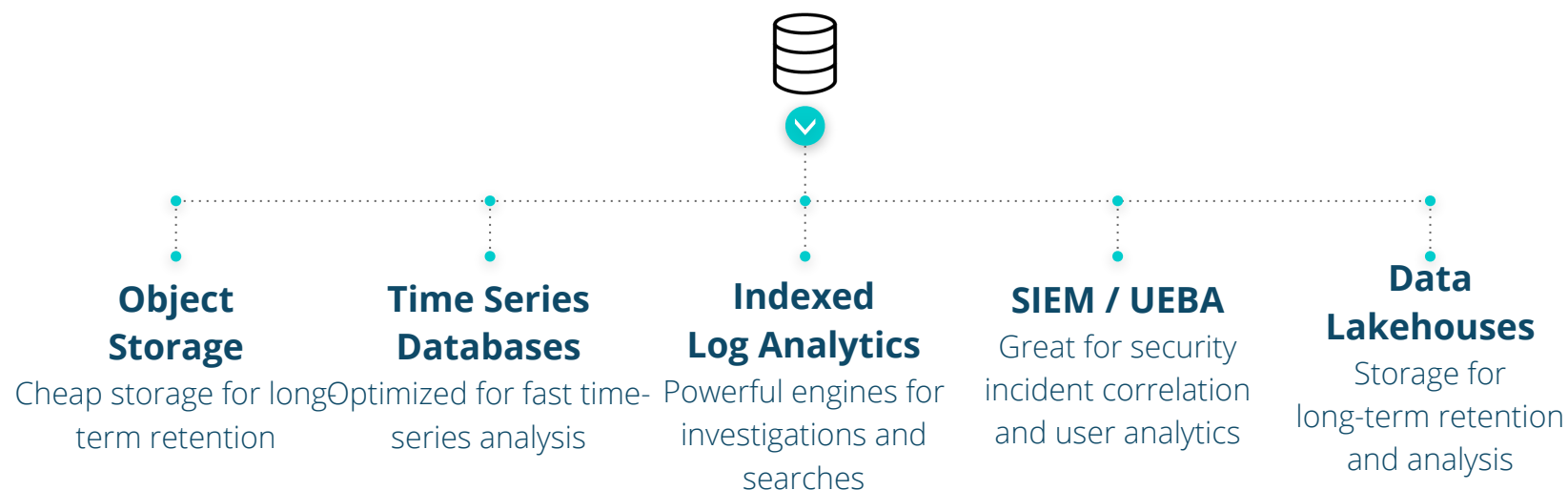


# Budgets Aren't Keeping Up





# So Data Management is Evolving...



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



# Security Monitoring is Evolving...

## MONITORING

Answer questions you know you have

**Exclude** sources by default

Single system performance focus

Reduce data to save storage

Compliance adds complexity

## OBSERVABILITY

Answer questions you didn't expect

Include all sources by default

Distributed systems focused

Keep all data in cold storage

Compliance by default (all data)



Transform your traditional **SIEM architecture.**



**CYBER SECURITY**  
www.cybersecuritysummit.org **SUMMIT**

13th Annual Cyber Security Summit | October 24-26, 2023



#cybersecuritysummit #css13

RESILIENCE  
**UNLOCKED**

COPYRIGHT © 2023 CRIBB, INC. ALL RIGHTS RESERVED.

A decorative graphic in the bottom right corner featuring a globe with glowing data lines and a network-like structure.

# Need to Instrument More While Paying Less



**FIND THE MIDDLE GROUND**



**BETWEEN WHAT YOU REQUIRE  
AND WHAT YOU CAN AFFORD**



**CYBER SECURITY**  
www.cybersecuritysummit.org **SUMMIT**

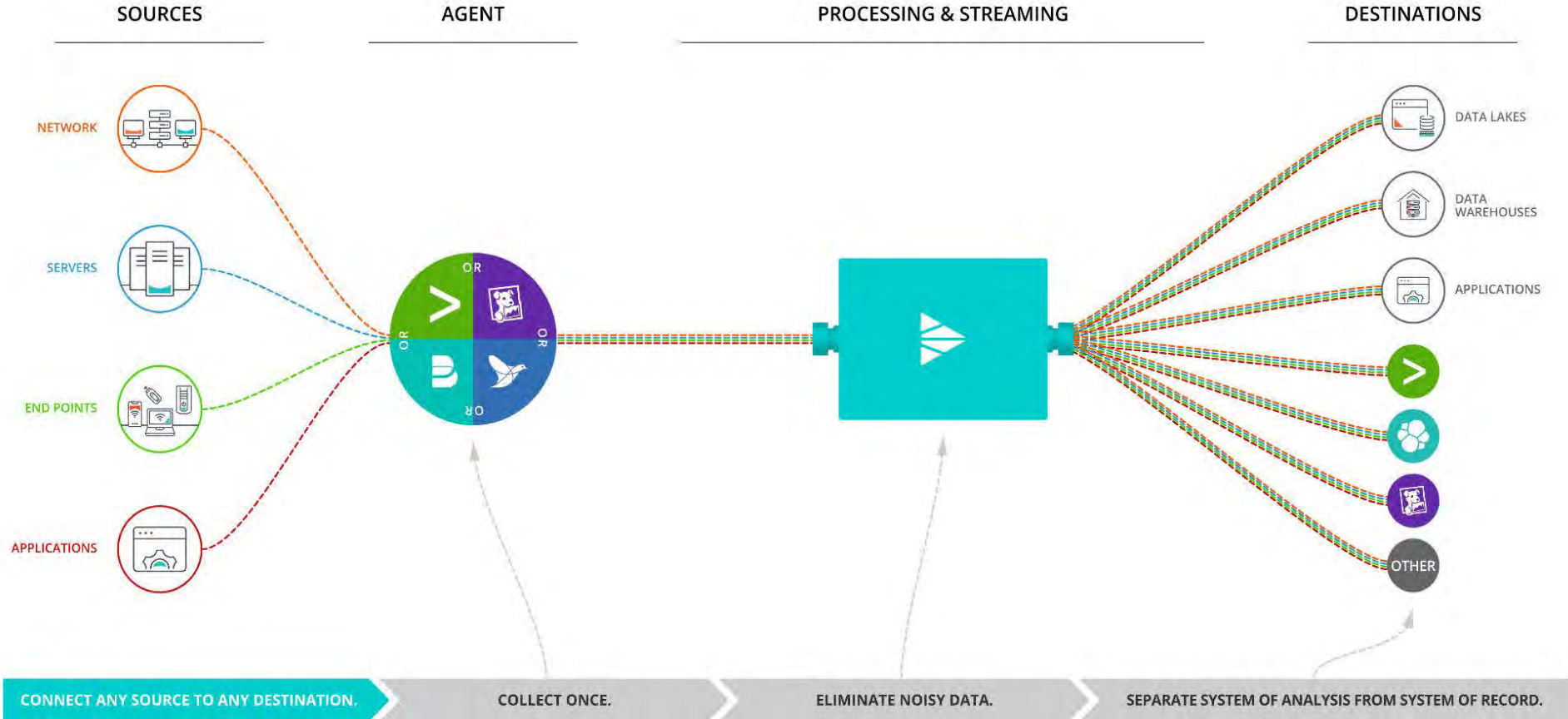
13th Annual Cyber Security Summit | October 24-26, 2023



#cybersecuritysummit #css13

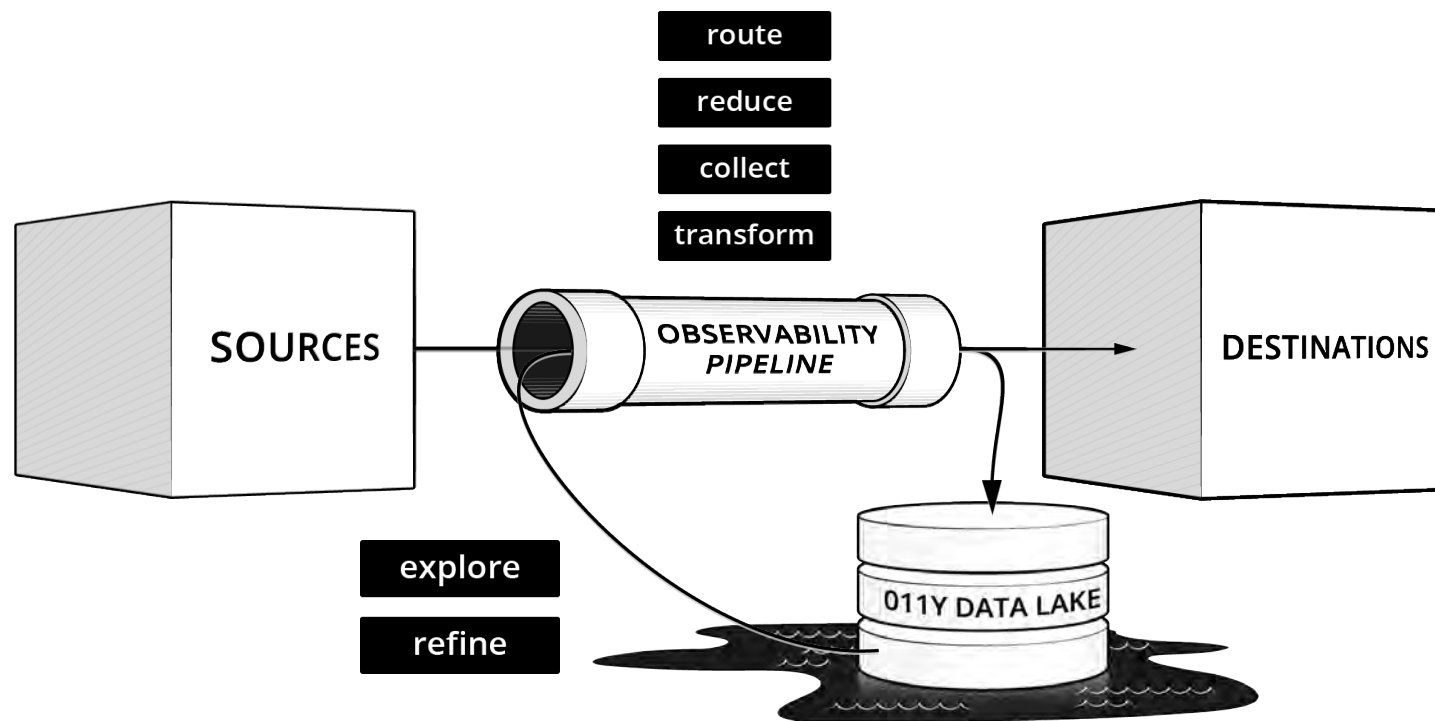
RESILIENCE  
**UNLOCKED**

# 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

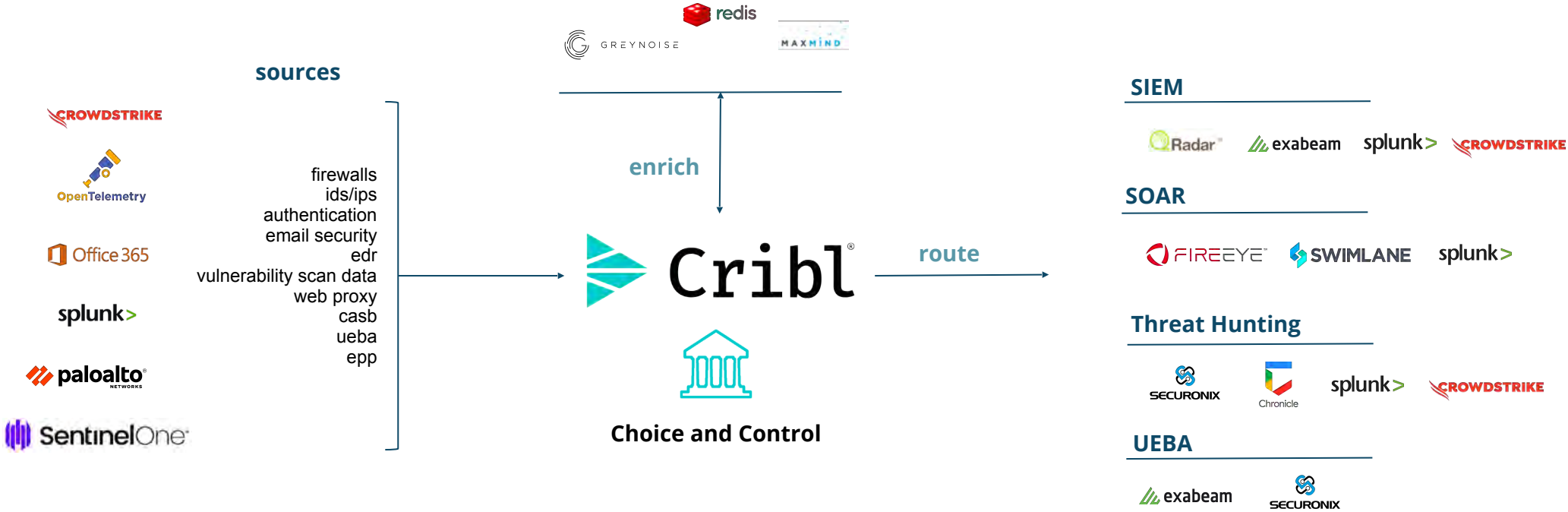
Better value from your SIEM and analysis platforms.

3

Options to optimize your costs.

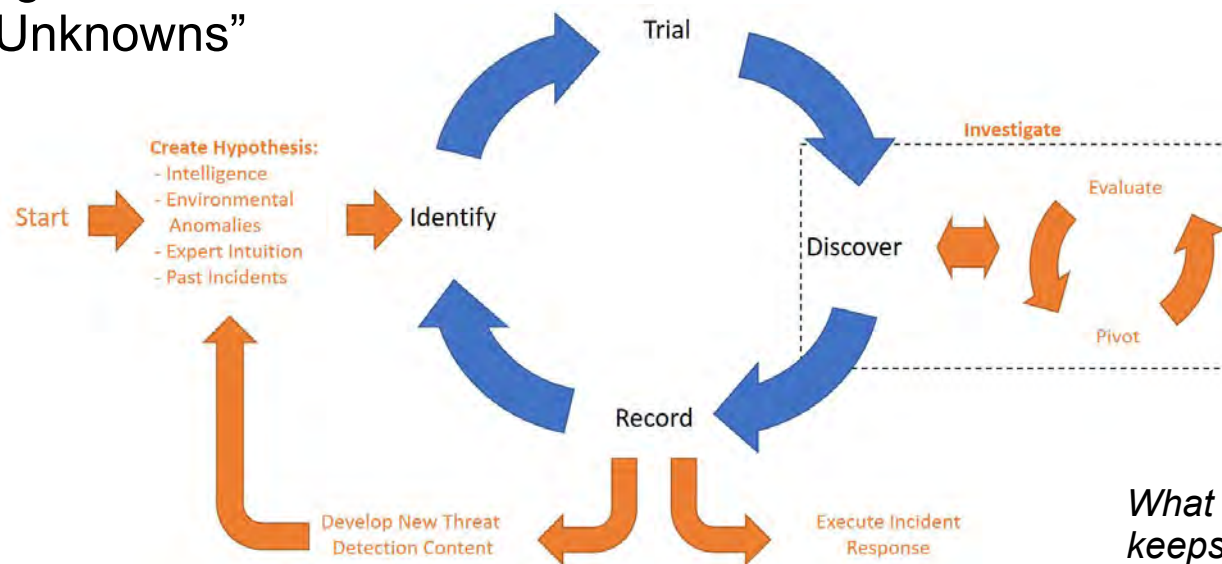


# Bringing it all together



# 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.

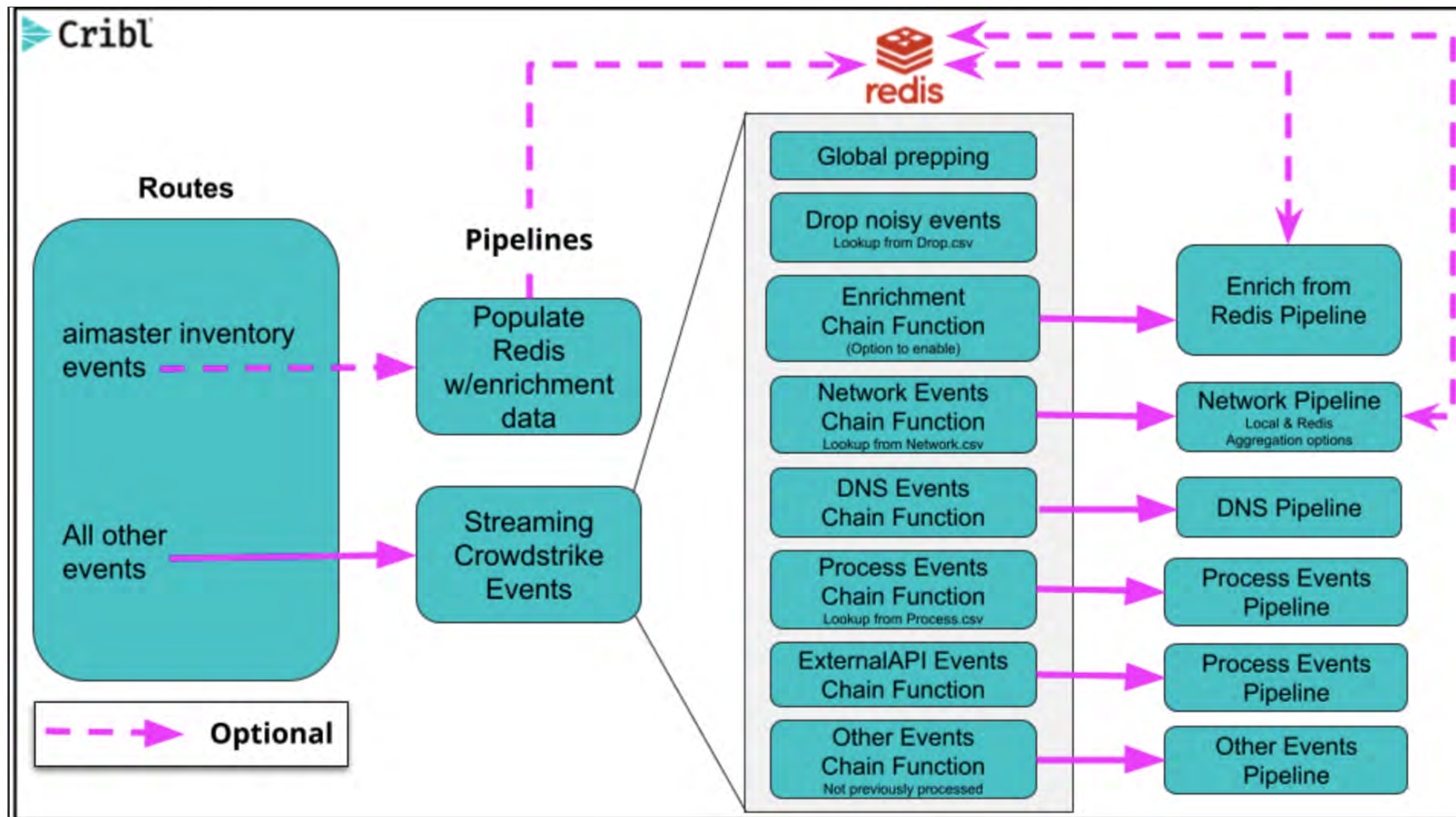
Cribl Stream extracts data from FDR, enriches and redacts it, then routes to your destinations in the right data format.

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





# CrowdStrike FDR Cribl Pack Workflow



# Less Data – Better Data

The screenshot displays the Elastic SIEM interface for configuring a pipeline named 'Crowdstrike\_FDR\_All'. The pipeline consists of four functions: Parser, Parser, Dynamic Sampling, and Sampling. A table provides a comparison of data metrics before and after processing:

	_raw Length	Full Event Length	Number of Fields	Number of Events
IN	104.82KB	121.60KB	4	100
OUT	39.23KB	76.42KB	13	100
DIFF	↓ -62.58%	↓ -37.16%	↑ 225.00%	0.00%

The 'DIFF' row is highlighted with a red border, indicating the significant data reduction achieved. The interface also shows a list of pipeline functions and a preview of event data, including fields like 'event\_platform', 'event\_origin', and 'event\_type'.





# Common Security Data Use Case

Sysmon\_WindowsXMLEvents Attached to 1 Route IN 442.00 OUT 442.00 ERR 0 + Function

#	Function	Description	Filter	Filter
1	Comment	Description: This pipeline reduce XML ...		
2	Comment	Please enable Descriptions - (Select top...		
3	Comment	The XML Processing group turns the _r...		
4	Eval	e brackets to remove fields with those va	true	On
5	Flatten		true	On
6	Comment	Rename for CIM compliance		
7	Rename	rename parent events	true	On
8	Rename	rename ... xpects for Sysmon sourcetype	true	On
9	Parser		true	On
10	Serialize		true	On
11	Eval		true	On
12	Comment	Use Eval to drops specific fields		
13	Eval	Exclude Keywo... but show anything else	['0x8000000000000000'], includes (...	On
14	Comment	Set Index, Source and SourceType		
15	Eval	Set your metadata here	true	On

Sample Data Preview Simple Preview Full Quick Stats

Sample data file sysmon-clean.log.json Pipeline Sysmon\_WindowsXMLEvents Run

IN OUT Select Fields (7 of 7)

```

1
2022-02-18
11:15:48.729
-05:00
#_time: 1645200948.729
#_cribl_breaker: Break on newLines
#_host: ACARD-PC8TTQ88
#_index: sysmon
#_source: WinEventLog:Microsoft-Windows-Sysmon/Operational
#_sourcetype: XmlWinEventLog:Microsoft-Windows-Sysmon/Operational

2
2022-02-18
11:15:48.729
-05:00
#_time: 1645200948.729
#_cribl_breaker: Break on newLines
#_host: LLECOM-BCBYMH3
#_index: sysmon
#_source: WinEventLog:Microsoft-Windows-Sysmon/Operational
#_sourcetype: XmlWinEventLog:Microsoft-Windows-Sysmon/Operational
    
```



# 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><Lev
el>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTim
e='2022-02-18T07:08:14.7541674Z' /><EventRecordID>18580</EventRecordID><Correlation/><Execution ProcessID
='32280' ThreadID='2836' /><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>ACARD-PC0TTQB
8.testing.net</Computer><Security UserID='S-1-5-18' /></System><EventData><Data Name='RuleName'>-</Data><D
ata Name='UtcTime'>2022-02-18 07:08:14.505</Data><Data Name='ProcessGuid'>{020511a9-45de-620f-1c98-000000
005300}</Data><Data Name='ProcessId'>22824</Data><Data Name='Image'>C:\Program Files (x86)\Common Files\A
dobe\ARM\1.0\AdobeARM.exe</Data><Data Name='FileVersion'>1.824.45.8876</Data><Data Name='Description'>Ado
be Reader and Acrobat Manager</Data><Data Name='Product'>Adobe Reader and Acrobat Manager</Data><Data Nam
e='Company'>Adobe Inc.</Data><Data Name='OriginalFileName'>AdobeARM.exe</Data><Data Name='CommandLin
e'>"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-b
25b-6205-6d3c-920000000000}</Data><Data Name='LogonId'>0x923c6d</Data><Data Name='TerminalSessionId'>1</D
ata><Data Name='IntegrityLevel'>Medium</Data><Data Name='Hashes'>SHA1=CE733FA2825E3789BCE001031CCFFD62324
C4808</Data><Data Name='ParentProcessGuid'>{020511a9-a612-6205-3500-000000005300}</Data><Data Name='Paren
tProcessId'>2560</Data><Data Name='ParentImage'>C:\Windows\System32\svchost.exe</Data><Data Name='ParentC
ommandLine'>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

```

1
2022-02-18
11:15:48.729
-05:00
_raw:
  app: C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\AdobeARM.exe
  Channel: Microsoft-Windows-Sysmon/Operational
  cmdline: "C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\AdobeARM.exe"
  Company: Adobe Inc.
  Description: Adobe Reader and Acrobat Manager
  dvc: ACARD-PC0TTQB8.testing.net
  EventID: 1
  EventRecordID: 18580
  FileVersion: 1.824.45.8876
  Guid: {5770385f-c22a-43e0-bf4c-06f5698ffbd9}
  Level: 4
  LogonGuid: {028511a9-b25b-6205-6d3c-920000000000}
  LogonId: 0x923c6d
  Name: Microsoft-Windows-Sysmon
  Opcode: 0
  OriginalFileName: AdobeARM.exe
  parent_process: C:\WINDOWS\system32\svchost.exe -k netsvcs -p -s Schedule
  parent_process_guid: {020511a9-a612-6205-3500-000000005300}
  parent_process_id: 2560
  ParentImage: C:\Windows\System32\svchost.exe
  process_current_directory: C:\WINDOWS\system32\
  process_hash: SHA1=CE733FA2825E3789BCE001031CCFFD62324C4808
  process_id: 22824
  process_integrity_level: Medium
  ProcessID: 32280
  Product: Adobe Reader and Acrobat Manager
  session_id: {020511a9-45de-620f-1c98-000000005300}
  SystemTime: 2022-02-18T07:08:14.7541674Z
  Task: 1
  TerminalSessionId: 1
  ThreadID: 2836
  User: testing.net\testmon
  user_id: S-1-5-18
  UtcTime: 2022-02-18 07:08:14.505
  Version: 5
#_time: 1645200948.729
  cribl_breaker: Break-on-newlines
  cribl_pipe: Sysmon_WindowsXMLEvents
  host: ACARD-PC0TTQB8
  index: sysmon
  source: XmlWinEventLog:Microsoft-Windows-Sysmon/Operational
  sourcetype: XmlWinEventLog:Microsoft-Windows-Sysmon/Operational

```

	_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.



**CYBER SECURITY**  
www.cybersecuritysummit.org **SUMMIT**

13th Annual Cyber Security Summit | October 24-26, 2023



#cybersecuritysummit #css13

RESILIENCE  
**UNLOCKED**

COPYRIGHT © 2023 CRIBB, INC. ALL RIGHTS RESERVED.

# Benefits of an Observability Pipeline

**Organize for Success - People and Process still the foundation**

Breakdown organizational Silos



**CYBER SECURITY**  
www.cybersecuritysummit.org **SUMMIT**

13th Annual Cyber Security Summit | October 24-26, 2023



#cybersecuritysummit #css13

RESILIENCE  
**UNLOCKED**  
COPYRIGHT © 2023 CRIBL, INC. ALL RIGHTS RESERVED.

# Benefits of an Observability Pipeline

## Create a foundation of good data

Quality data standards and enforcement are



How to Transform your SIEM Architecture

## 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



**CYBER SECURITY**  
www.cybersecuritysummit.org **SUMMIT**

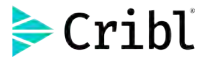
13th Annual Cyber Security Summit | October 24-26, 2023



#cybersecuritysummit #css13

RESILIENCE  
**UNLOCKED**  
COPYRIGHT © 2023 CRIBL, INC. ALL RIGHTS RESERVED

# Want to See It for Yourself?



Demo Stream today in our sandboxes!

Sign up for a FREE account!



# Cribl<sup>®</sup>.Cloud

<https://sandbox.cribl.io>

<https://cribl.cloud>



**CYBER SECURITY**  
www.cybersecuritysummit.org **SUMMIT**

13th Annual Cyber Security Summit | October 24-26, 2023



#cybersecuritysummit #css13

RESILIENCE  
**UNLOCKED**  
COPYRIGHT © 2023 CRIBL, INC. ALL RIGHTS RESERVED.



# Q&A



**CYBER SECURITY**  
www.cybersecuritysummit.org **SUMMIT**

13th Annual Cyber Security Summit | October 24-26, 2023



#cybersecuritysummit #css13

RESILIENCE  
**UNLOCKED**

COPYRIGHT © 2023 CRIBB, INC. ALL RIGHTS RESERVED.

# Thank You

## Contact Us

**Cribl, Inc.** 44 Tehama St. San Francisco, CA 94105

**Sales Inquiries** [hello@cribl.io](mailto:hello@cribl.io)

**Career Opportunities** [jobs@cribl.io](mailto:jobs@cribl.io)

**Join our Community** <https://cribl.io/community>

**Visit Us** <http://www.cribl.io>



**CYBER SECURITY**  
www.cybersecuritysummit.org **SUMMIT**

13th Annual Cyber Security Summit | October 24-26, 2023



#cybersecuritysummit #css13

RESILIENCE  
**UNLOCKED**