

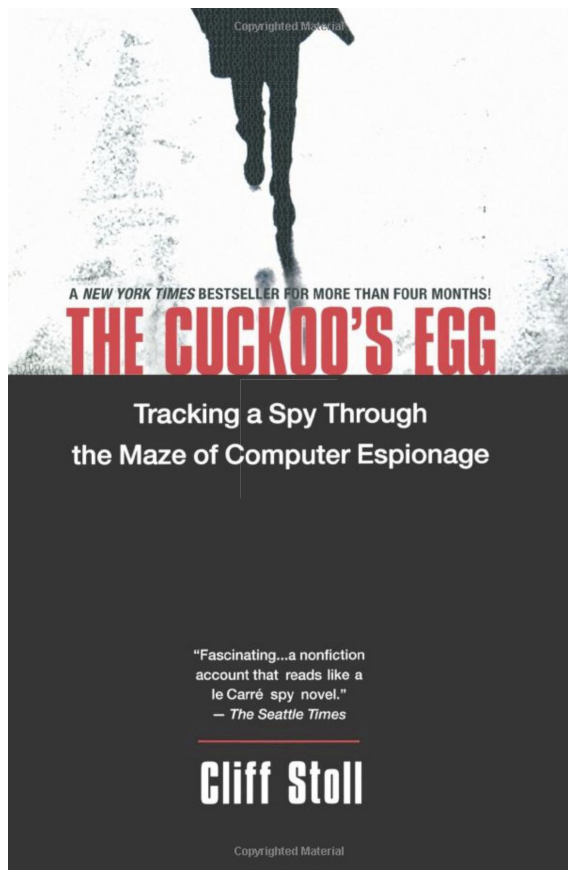
Driving Rapid Incident Response: Specialized Tooling on top of Zeek

Pete Buffon

September 10 2026

Lawrence Berkeley National Laboratory

- **"Bringing Science Solutions to the World"**
- **Hundreds of University staff also LBNL staff**
- **Rich history of scientific discovery**
 - **17 Nobel Prizes**
 - **63 members of the National Academy of Sciences (~3% of the Academy)**



Network utilities from LBNL

- Traceroute
- Libpcap
- Tcpdump

Zeek Network Security Monitor



LAWRENCE BERKELEY NATIONAL LABORATORY NOBEL LAUREATES



Founder,
Ernest Orlando
Lawrence
Physics, 1939

*Honoring men and women from all corners of the globe for outstanding
achievements in physics, chemistry, medicine, literature and peace...*



Glenn T. Seaborg
Chemistry, 1951



Edwin M. McMillan
Chemistry, 1951



Owen Chamberlain
Physics, 1959



Emilio G. Segrè
Physics, 1959



Donald A. Glaser
Physics, 1962



Melvin Calvin
Chemistry, 1961



Luis W. Alvarez
Physics, 1968



Yuan T. Lee
Chemistry, 1986



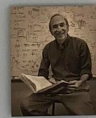
Steven Chu
Physics, 1997



George
F. Smoot III
Physics, 2006



Intergovernmental Panel on
Climate Change
Peace, 2007



Saul Perlmutter
Physics, 2011



Jennifer Doudna
2020



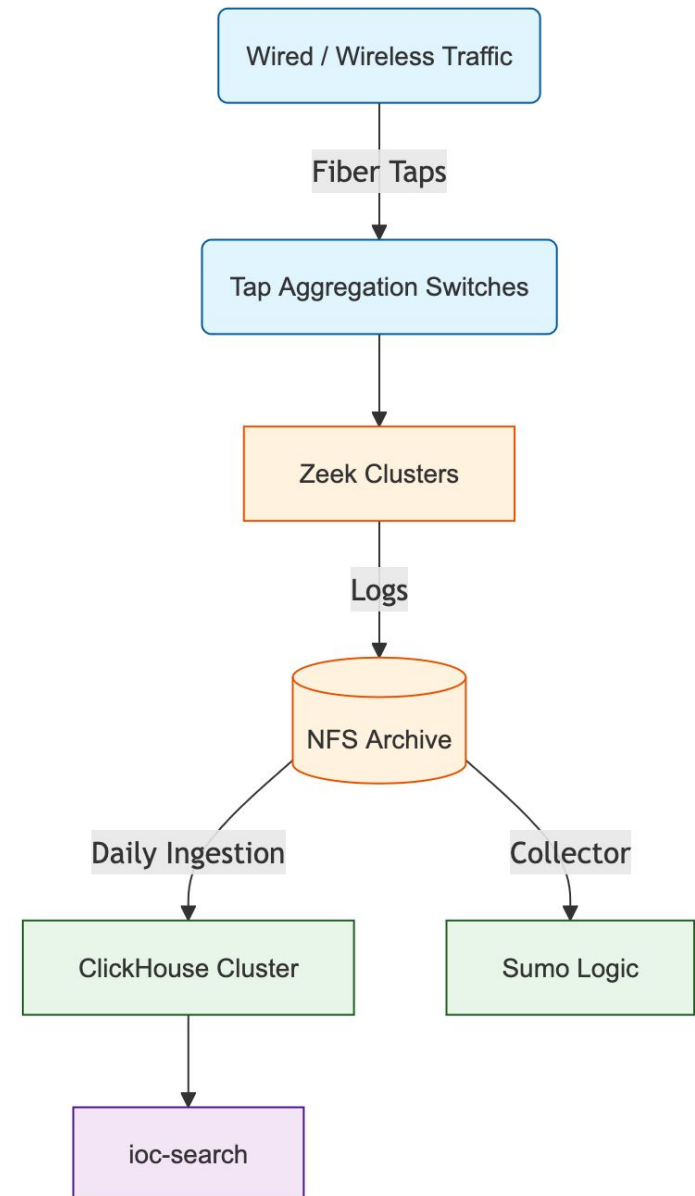
Agenda

- LBNL Zeek Pipeline
- Zeek + Clickhouse
- Why do we need ioc-search?
- Investigation #1
- Sumo Logic Overview
- Why do we need Sumo Logic?
- Investigation #2
- Key Takeaways
- Q&A

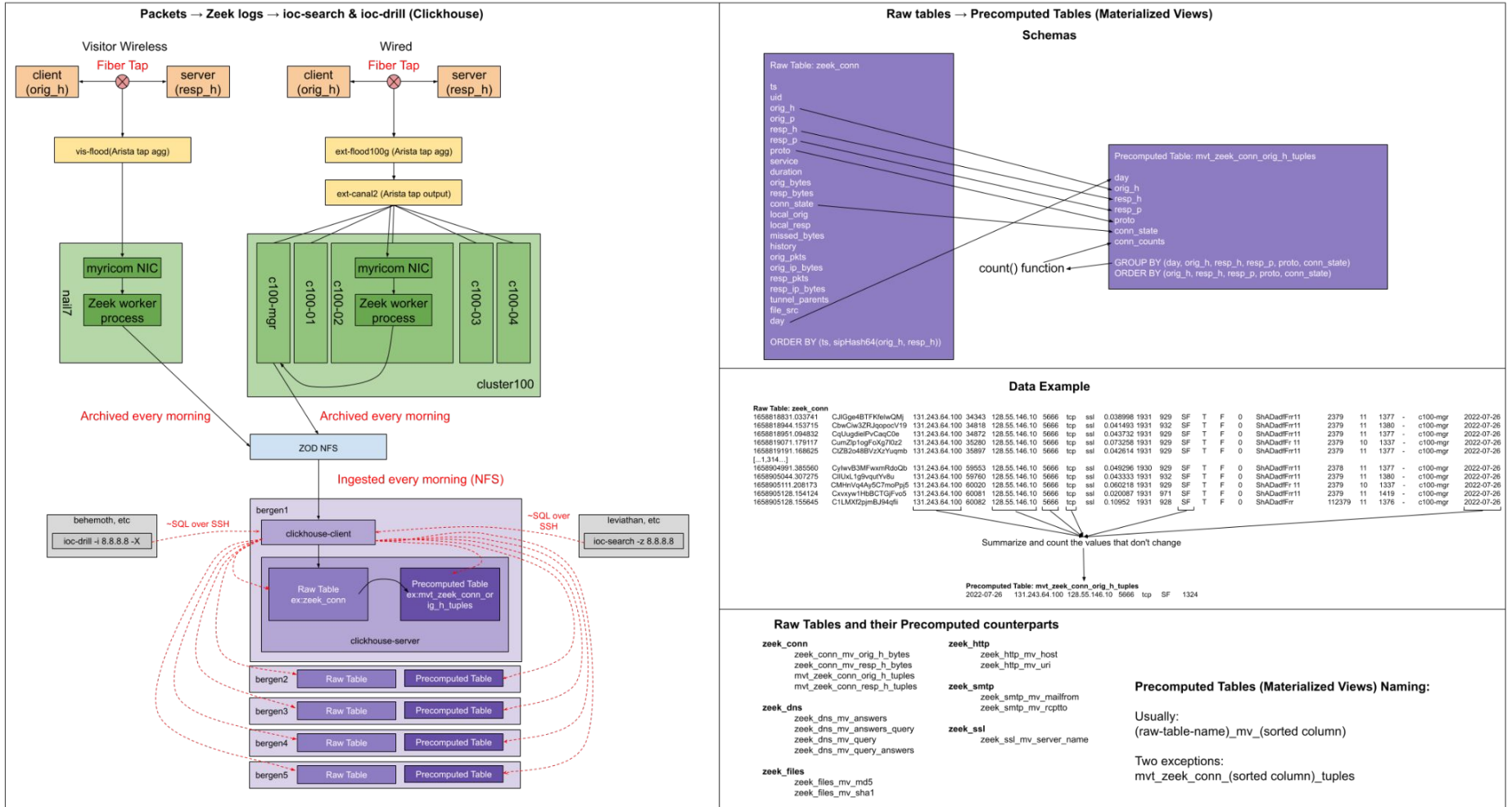
LBNL Zeek Pipeline

LBNL Context

- Intrusion detection
- Real-time blocking of attacks
- In 2025:
 - 55.7 PB of total network traffic
 - 8,700,000 network attacks blocked by Zeek



Zeek + Clickhouse



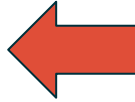
Why do we need ioc-search?

If we search fast, so will search more

lots of cores

```
[pbuffon@crunchbox ~]$ time find
/YURT/bro-NFS/WIRED/logs/ -mtime -7 -type f -name
"conn.log*" | parallel 'zfgrep 192.168.5.1 {}'
```

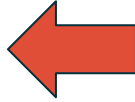
#types	time	string	addr	port	addr	port
enum	string	interval		count	count	string
bool	bool	count	string	count	count	count
count	set[string]		count	string	string	string
...						
real	25m13.458s					
user	80m40.989s					
sys	11m22.258s					



```
[pbuffon@crunchbox ~]$ time ioc-search -i 192.168.5.1 -d
7
```

#day	ip	orig_h_hits	resp_h_hits
2026-08-27	192.168.5.1	39	36052415
2026-08-28	192.168.5.1	33	30548354
2026-08-29	192.168.5.1	27	11095119
2026-08-30	192.168.5.1	36	10497658
2026-08-31	192.168.5.1	32	33831338
2026-09-01	192.168.5.1	41	36746885
2026-09-02	192.168.5.1	36	37033912
2026-09-03	192.168.5.1	33	11375712

real	0m0.561s
user	0m0.040s
sys	0m0.012s



Investigation #1

A recent FBI affidavit identified DOE labs being attacked

<https://www.justice.gov/opa/media/1459096/dl?inline>

...The FBI has been investigating a group of malicious cyber threat actors located in Republic of... They use the acronyms QTFY, QT, and QTCYBER for themselves and their tools, and will hereafter be referred to as "QTFY actors."

These types of events happen every day

Proxy Platform Management: This product manages a botnet of compromised devices, including IoT devices. Its primary function is to manage botnet nodes and to configure SOCKS proxy software on those devices.

Following is infrastructure attributed to this botnet:

	First Seen	Last Seen
23.95.220[.]192	2026-03-12	2026-05-12
103.201.131[.]121	2026-03-16	2026-05-16
109.236.48[.]121	2026-03-09	2026-03-11
install.anticonstitutionally[.]sbs	2026-03-03	Active
mail.fastsecurey[.]info	2026-03-30	Active
www.fastsecurey[.]info	2026-03-30	Active

Investigation #1

```
[pbuffon@crunchbox ~]$ ioc-search -i 23.95.220.192 -d 365
```

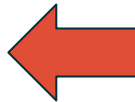
#day	ip	orig_h_hits	resp_h_hits
2026-06-30	23.95.220.192	1	0

```
[pbuffon@crunchbox ~]$ ioc-search -i 103.201.131.121 -d 365
```

#day	ip	orig_h_hits	resp_h_hits
2026-08-05	103.201.131.121	0	1

```
[pbuffon@crunchbox ~]$ ioc-search -i 109.236.48.121 -d 365
```

#day	ip	orig_h_hits	resp_h_hits
2026-03-08	109.236.48.121	1	0
2026-03-09	109.236.48.121	30	4
2026-03-10	109.236.48.121	2	0



Investigation #1

*IP Addresses changed

```
[pbuffon@crunchbox ~]$ ioc-search -z 109.236.48.121 -d 365
```

#day	orig_h	resp_h	resp_p	proto	conn_state	conn_counts
...						
2026-03-09	109.236.48.121	10.0.211.53	8080	tcp	S0	1
2026-03-09	109.236.48.121	10.0.119.43	8080	tcp	S0	1
2026-03-09	109.236.48.121	10.0.182.190	8080	tcp	S0	1
2026-03-09	109.236.48.121	10.0.9.45	8080	tcp	S0	1
2026-03-09	109.236.48.121	10.0.87.19	8080	tcp	S0	1
2026-03-09	109.236.48.121	10.0.64.102	23	tcp	S0	1
2026-03-09	109.236.48.121	192.168.99.250	8080	tcp	S0	1
2026-03-09	109.236.48.121	192.168.77.201	23	tcp	S0	1
2026-03-09	109.236.48.121	192.168.29.161	8080	tcp	S0	1
2026-03-09	109.236.48.121	192.168.122.251	8080	tcp	S0	1
2026-03-09	109.236.48.121	192.168.28.91	8080	tcp	S0	1
2026-03-09	109.236.48.121	192.168.144.222	8080	tcp	S0	1
2026-03-09	109.236.48.121	192.168.226.141	23	tcp	S0	1
2026-03-09	109.236.48.121	192.168.216.201	8080	tcp	S0	1
2026-03-09	109.236.48.121	192.168.19.108	8080	tcp	S0	1
2026-03-09	109.236.48.121	192.168.78.46	23	tcp	S0	1
2026-03-09	109.236.48.121	192.168.97.244	23	tcp	S0	1
2026-03-09	109.236.48.121	172.16.177.255	8080	tcp	S0	1
2026-03-09	109.236.48.121	172.16.41.55	8080	tcp	S0	1
2026-03-09	109.236.48.121	172.16.87.222	23	tcp	S0	1
2026-03-09	109.236.48.121	172.16.17.117	23	tcp	S0	1
2026-03-09	198.129.78.73	109.236.48.121	0	icmp	OTH	4
2026-03-10	109.236.48.121	172.16.12.229	23	tcp	S0	1
2026-03-10	109.236.48.121	172.16.21.35	23	tcp	S0	1

Investigation #1

```
[pbuffon@crunchbox ~]$ ioc-search -h
No arg for -h option
```

Usage:

```
-d [days to look back]  number of days back to search (default: 180, max: 2457)
-f [filename]           file containing IOCs to search
-o [name]               Output directory name within /YURT/tmp
-Q                     Custom query, write whatever SQL-like query you want
-M [memory]             Max memory per query in GB
-n                     noop; show SQL query and exit
```

Table-dependent options (table is set automatically based on option):

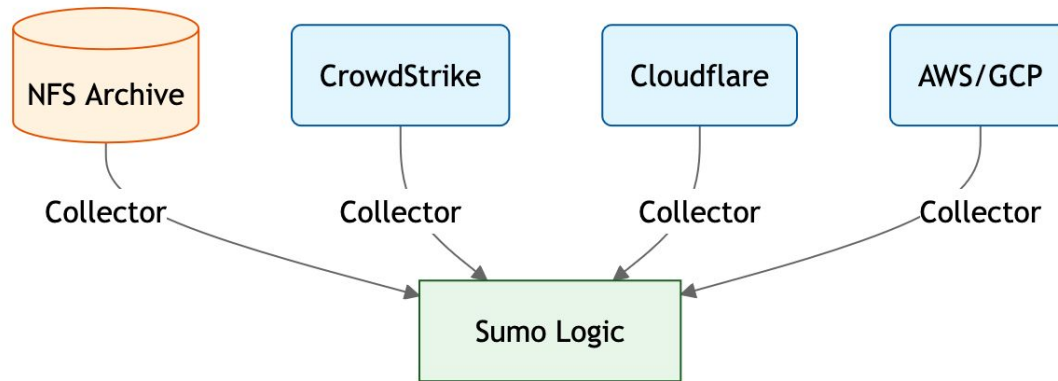
Zeek conn.log

```
-i [ip_address]         same as 'orig_h OR resp_h' (added together)
-O [orig_ip_address]
-R [resp_ip_address]
-D [dst_port]
-P [ip_address]         counts of different protos for this IP address
-C [ip_address]         counts of different conn_states for this IP address
-B [ip_address]         total orig_ip_bytes and resp_ip_bytes for this IP address
                        NOTE: reports orig_ip_bytes where IP is orig_h and resp_ip_bytes where IP is resp_h.
                        However, it is not resp_ip_bytes where the IP is orig_h or vice-versa.
-z [ip_address]         search orig_h or resp_h and return orig_h, resp_h, resp_p, proto, conn_state
-t [ip_address]         return timestamps, tuples, and bytes of when this IP address was seen (SLOW ON DENSE
```

HITS!)

Sumo Logic overview

Cloud aggregation/SIEM platform



- Other platforms in this space: Splunk, Datadog etc.
- Integrates with on-prem or cloud log sources

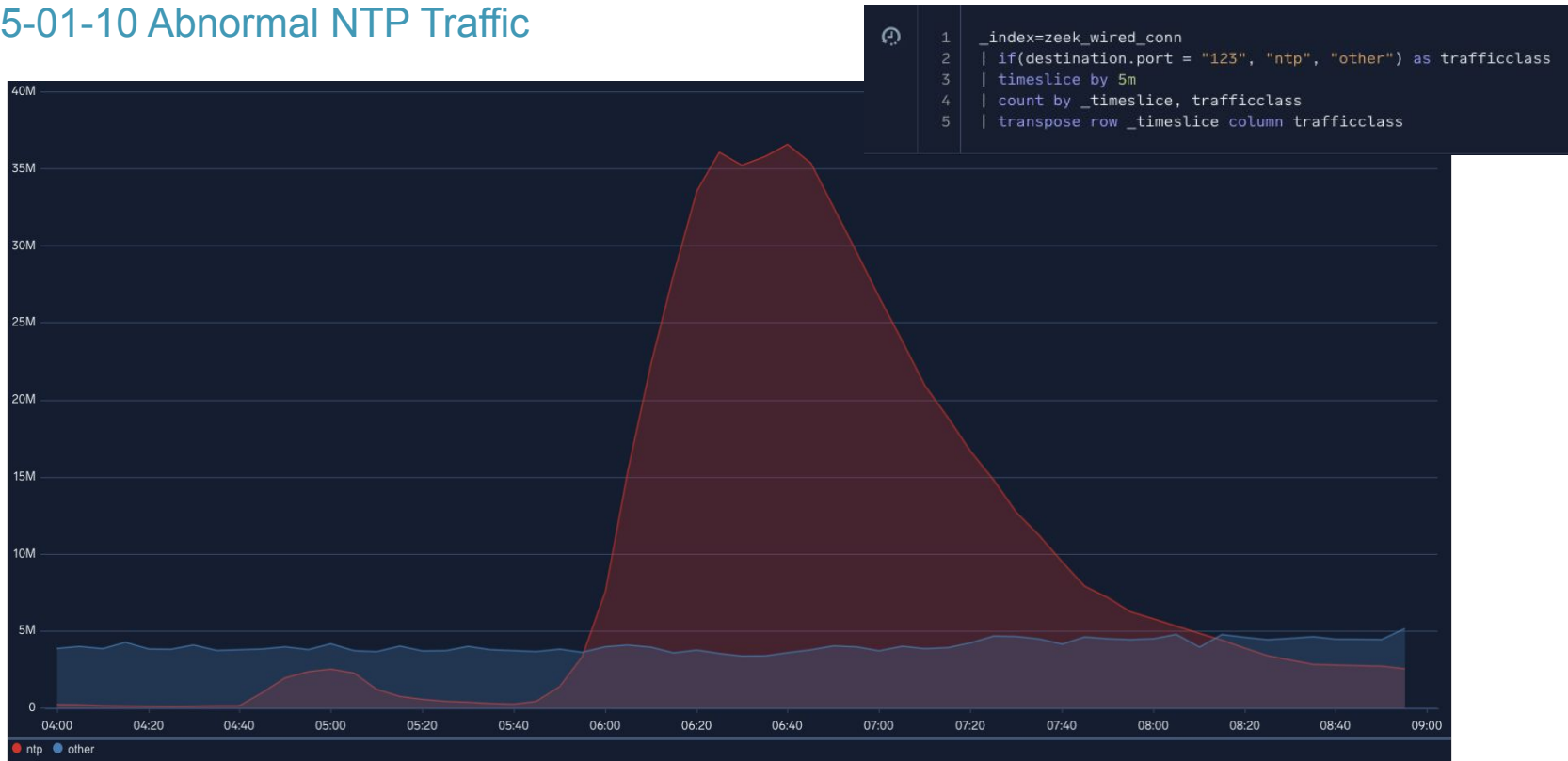
Why do we need Sumo Logic?

Data enrichment and visualization

- Additional functionality over the logs we already have
- Fine grained queries over large datasets
- Data enrichment with other log sources
- Data visualization with customizable graphs

Investigation #2

2025-01-10 Abnormal NTP Traffic



- 500 million connections flooded the network within a brief 4-to-5-hour window.
- Traffic reached a massive peak rate of more than 300,000 connections per second.

Investigation #2

AS4766 (Korea Telecom)



```
1 _index=zeek_wired_conn
2 | where destination.port = "123"
3 | lookup organization from asn://default on ip=source.ip
4 | timeslice by 5m
5 | count by organization
6 | sort by _count
7 | limit 5
```

#	zeek.connection.state	_count
1	S0	514,394,702
2	SF	206
3	OTH	6

Key Takeaways

Zeek as building block

- While Zeek provides invaluable raw network data, it requires specialized, real-time query and analysis platforms to drive actionable incident response.
- Building specialized tools on top of Zeek enables security teams to correlate massive datasets, isolate threats, and execute rapid mitigations

Thank You

Q&A