RSAConference2022
San Francisco & Digital | June 6 – 9

TRANSFORM

SESSION ID: PART4-R03

Extend EDR Visibility by Logging Everything: Demo with Free Integrations

Adam Hogan

SE Director for Humio, CrowdStrike
CrowdStrike
@adamwhogan

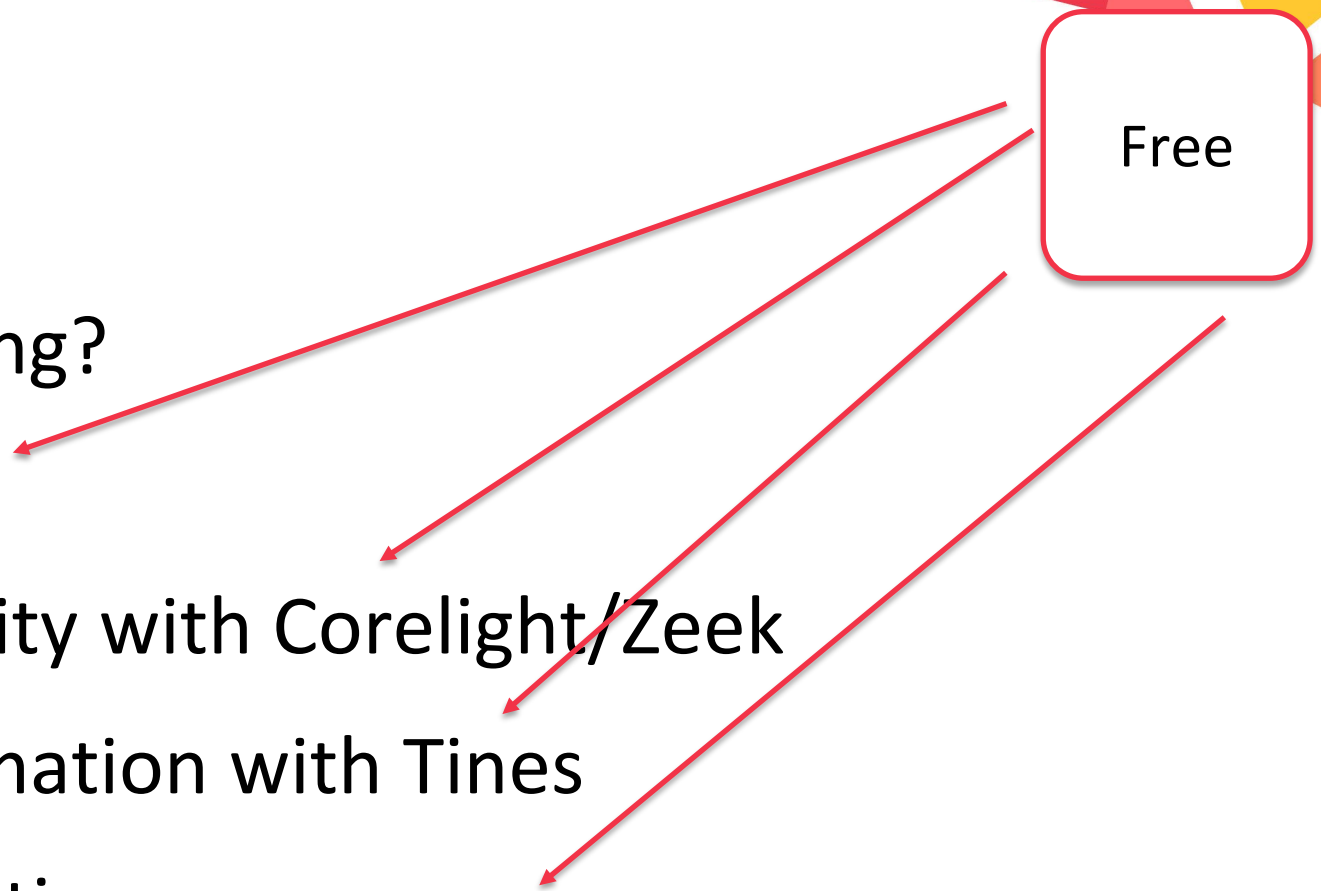
Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

Agenda

- What is XDR?
- What data is worth logging?
- Logging data in Humio
- Extending Falcon's visibility with Corelight/Zeek
- Extending Humio's automation with Tines
- Close the Loop with ticketing



Why?

- Environment for
  - Demo
  - Education
  - Show off Humio Community Edition

Free

Get Started With Humio

Humio Community Edition

Unleash the power of streaming observability at no cost.

- Ingest up to 16GB per day
- 7-day retention
- Ongoing usage with no trial period and no credit card required

Access Free Now

RSAConference2022

XDR


Congratulations! Your
EDR
evolved into
XDR!

Sine qua non of Detection & Response

All the data you might need in your next investigation

CROWDSTRIKE

Sine qua non of Detection & Response

All the data you might need in your next investigation to have the context and confidence to

Sine qua non of Detection & Response

All the data you might need in your next investigation to have the context and confidence to assess a false positive

Sine qua non of Detection & Response

All the data you might need in your next investigation to have the context and confidence to identify a breach

Sine qua non of Detection & Response

All the data you might need in your next investigation to have the context and confidence to discover the root cause

RSAConference2022

Extending EDR Visibility

Into the Network

Zeek & Corelight

- Open Source: Zeek
- Free: Corelight @ Home!
- Visibility
  - Devices not running EDR
  - Great network traffic detail
- Correlation
  - Community ID

CROWDSTRIKE

Logging Problem

- A more general lesson: How do you calculate TCO for a set of logs?
- How to cut costs of logging?
  - Don’t log it
  - Reduce retention
  - Sample (e.g. metrics)
  - Assessment (e.g. alerts)

Logging Problem

- A more general lesson: How do you calculate TCO for a set of logs?
- How to increase benefit of logging
  - Log more
  - Share more
  - Reduce search time

Community ID

- Hash a network connection
  - Protocol, Source IP, Destination IP, Source Port, Destination IP, ICMP Type, ICMP Code, Seed
- #type = “CrowdStrike”
  AND #event_simpleName=NetworkConnectIP4
  | join({#type=“Zeek”}, field=_community_id)
- Done!

CROWDSTRIKE

CommunityID in Humio

Talon3FDR | Search | Dashboards | Alerts | Parsers | Files | Settings

Auto (Table) | Queries | Language syntax | Table widget | Last 24h (Static) | Run

```
1 #event_simpleName=Network* |
2 communityId(proto=Protocol, sourceip=LocalAddressIP4, sourceport=LocalPort, destinationip=RemoteAddressIP4, destinationport=RemotePort)
3 | table([@timestamp, _community_id, LocalAddressIP4, LocalPort, RemoteAddressIP4, RemotePort, Protocol, aid], limit=20)
```

Results | Events

Fields | Hits: 766 | Speed: 0.05 GB/s | EPS: 65.58k | Work: 0 | Completion: 100% | Status: Done | Save as...

Fields	#
@timestamp	18
LocalAddressIP4	5
LocalPort	20
Protocol	1
RemoteAddressIP4	17
RemotePort	2
_community_id	20
aid	7

@timestamp	_community_id	LocalAddressIP4	LocalPort	RemoteAddressIP4	RemotePort	Protocol	aid
2021-12-11 14:12:59	1:IMacrYLP1Am/NGJ7PcwA5B9Q5sc=	172.17.0.29	64520	13.69.239.72	443	6	edbd072bd70e415290d713231e46df69
2021-12-11 14:12:41	1:BqMHjTKNez/NpGEbILmE77/6xcM=	172.17.0.26	51424	13.69.239.72	443	6	94c9add4a3364b1d9dbaac86d7c1073a
2021-12-11 14:03:42	1:2Mgd0Fy+Bax/U9MTWZhsOausPiw=	172.17.0.22	40908	169.254.169.254	80	6	ee2289b9f4664677ae37172f1dbbb09d
2021-12-11 14:03:42	1:NoqbErYHwY6vA0dSlCn1qtyomlk=	172.17.0.22	40906	169.254.169.254	80	6	ee2289b9f4664677ae37172f1dbbb09d
2021-12-11 14:01:08	1:ew82WjuxptigU3ZDoJTO8llTyio=	172.17.0.29	55327	13.89.179.9	443	6	f4c6840e31654f42aa28ff5dbb1d36cd
2021-12-11 14:01:07	1:SVlJINEBfo5bgsjDZ9tu99ESMXM=	172.17.0.26	56861	13.89.179.9	443	6	24638d3e587f47e9929b162b92b375e9
2021-12-11 13:59:11	1:qZvv5DFXNgya7N5q8GFc9DcJRaQ=	172.17.0.26	56851	52.179.216.235	443	6	24638d3e587f47e9929b162b92b375e9
2021-12-11 13:59:11	1:TqIbZZuRk5cIUryPAFws11yt/II=	172.17.0.26	56850	52.184.216.174	443	6	24638d3e587f47e9929b162b92b375e9
2021-12-11 13:57:46	1:NJ1wS/uIBizYndRFCNLy60dbJKo=	172.17.0.29	55302	40.83.247.108	443	6	f4c6840e31654f42aa28ff5dbb1d36cd
2021-12-11 13:56:44	1:CrzpLvbWgba5cU3So5qlOJrQfpg=	172.17.0.26	56826	20.72.205.209	443	6	24638d3e587f47e9929b162b92b375e9
2021-12-11 13:56:44	1:04iykULjc7WheNsGrcgChPj156E=	172.17.0.26	56828	20.190.151.6	443	6	24638d3e587f47e9929b162b92b375e9
2021-12-11 13:55:08	1:4SiEWIhFe4ImWL/w52LjDj69SQU=	172.17.0.26	56811	142.250.69.195	443	6	24638d3e587f47e9929b162b92b375e9

CommunityID in Falcon

Talon3FDR | Search | Dashboards | Alerts | Parsers | Files | Settings

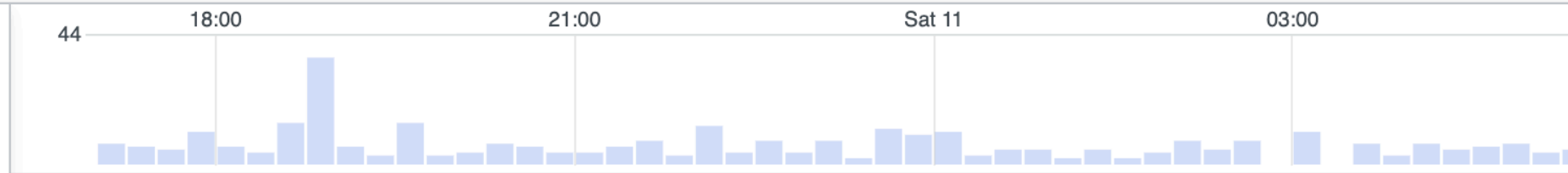
Auto (Table) | Queries | Language syntax | Table widget

```
1 #event_simpleName=Network* |
2 communityId(proto=Protocol, sourceip=LocalAddressIP4, sourceport=LocalPort, destinationip=RemoteAddressIP4, destinationport=RemotePort)
3 | table([@timestamp, _community_id, LocalAddressIP4, LocalPort, RemoteAddressIP4, RemotePort, Protocol, aid], limit=20)
```

Results | Events

Fields

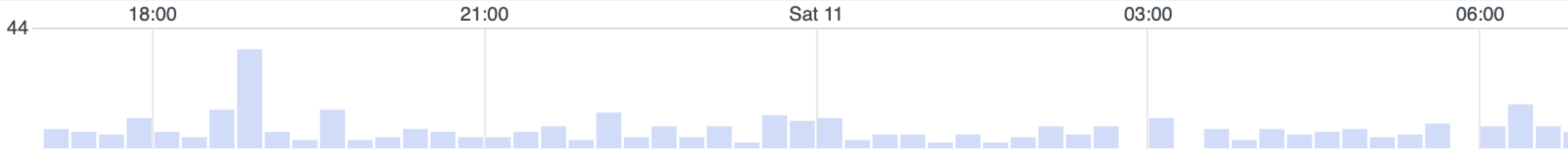
Hits: 766 | Speed: 0.05 GB/s | EPS: 65.58k | Work: 0 | Completion: 100%



Fields	#
@timestamp	18
LocalAddressIP4	5
LocalPort	20
Protocol	1

@timestamp	_community_id	LocalAddressIP4	LocalPort	Remote

Hits: 766 | Speed: 0.05 GB/s | EPS: 65.58k | Work: 0 | Completion: 100% | Status: Done



@timestamp	_community_id	LocalAddressIP4	LocalPort	RemoteAddressIP4
2021-12-11 14:12:59	1:IMacrYLP1Am/NGJ7PcwA5B9Q5sc=	172.17.0.29	64520	13.69.239.72
2021-12-11 14:12:41	1:BqMHjTKNez/NpGEbILmE77/6xcM=	172.17.0.26	51424	13.69.239.72
2021-12-11 14:03:42	1:2Mgd0Fy+Bax/U9MTWZhsOausPiw=	172.17.0.22	40908	169.254.169.254
2021-12-11 14:03:42	1:NoqbErYHwY6vA0dSlCn1qtyomlk=	172.17.0.22	40906	169.254.169.254
2021-12-11 14:01:08	1:ew82WjuxptigU3ZDoJTO8llTyio=	172.17.0.29	55327	13.89.179.9
2021-12-11 14:01:07	1:SVlJINEBfo5bgsjDZ9tu99ESMXM=	172.17.0.26	56861	13.89.179.9
2021-12-11 13:59:11	1:qZvv5DFXNgya7N5q8GFc9DcJRaQ=	172.17.0.26	56851	52.179.216.235
2021-12-11 13:59:11	1:TqIbZZuRk5cIUryPAFws11yt/II=	172.17.0.26	56850	52.184.216.174
2021-12-11 13:57:46	1:NJ1wS/uIBizYndRFCNLy60dbJKo=	172.17.0.29	55302	40.83.247.108
2021-12-11 13:56:44	1:CrzpLvbWgba5cU3So5qlOJrQfpg=	172.17.0.26	56826	20.72.205.209
2021-12-11 13:56:44	1:04iykULjc7WheNsGrcgChPj156E=	172.17.0.26	56828	20.190.151.6
2021-12-11 13:55:08	1:4SiEWIhFe4ImWL/w52LjDj69SQU=	172.17.0.26	56811	142.250.69.195

RSAConference2022

Demo!

Apply

- What data sets do you need more of?
- What extends visibility beyond EDR?

RSAConference2022

Extending EDR Visibility

Application Logs

Extending EDR Visibility

- Application Logs
  - They’re just sitting there, let’s go get them.
- Send Logs to Humio
  - Real Time Response
  - Humio Log Collector

CROWDSTRIKE

RSAConference2022

Demo!

RSAConference2022

Close the Loop

Close the Loop

- Hypothesis -> ad hoc searching
- Theory -> Automated alerting
- High confidence theory -> Priority Alerting
- Proven Theory -> Automated remediation

Tines

- Tines Community Edition!
  - if you're familiar with the APIs you use, Tines will dramatically speed up developing automated alerts and remediation.
- Caveats
  - SOAR presents a lot of organizational challenges.
  - It's own learning curve
    - Power tool

RSAConference2022

Demo!

Apply What You Have Learned Today

- Next week you should:
  - Sign up for Humio Community Edition!
  - Sign up for Corelight @ Home!
  - Sign up for Tines Community Edition!
- In the first three months following this presentation you should:
  - Review your TCO calculations for which logs you might need to investigate in the future.
    - If you have low confidence in these decisions, experiment.
  - Consider more raw telemetry
    - coalitions with other teams to share costs.

CROWDSTRIKE

RSAConference2022

Thank you!

@adamwhogan