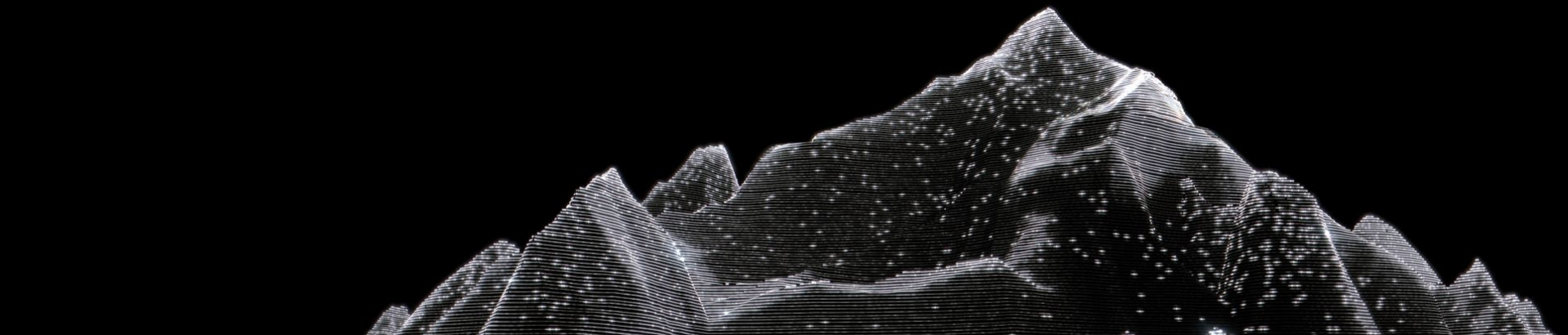
corelight

How to hunt with Zeek + Sigma



Today’s speakers

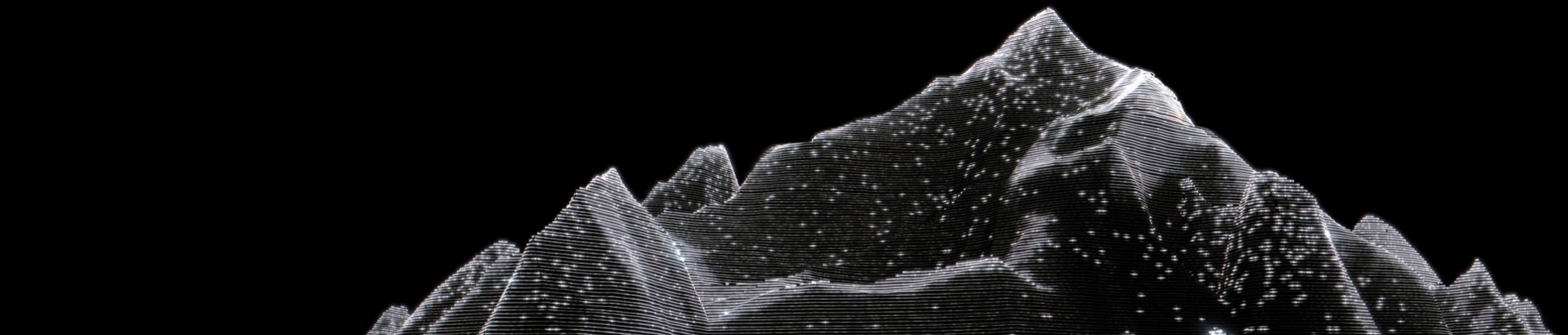
Vince Stoffer
Sr. Director of Product Management

Mark Overholser
Sales Engineer

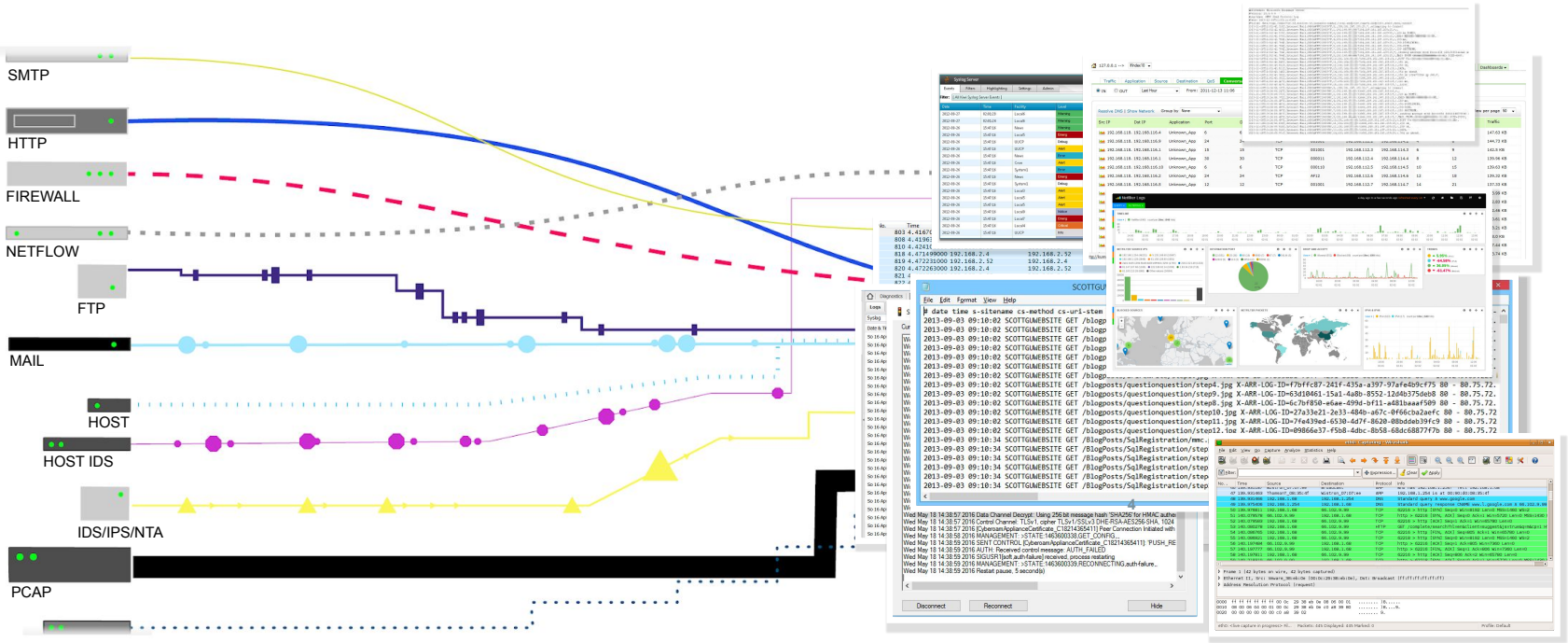
Edward Smith
Sr. Product Marketing Manager

corelight

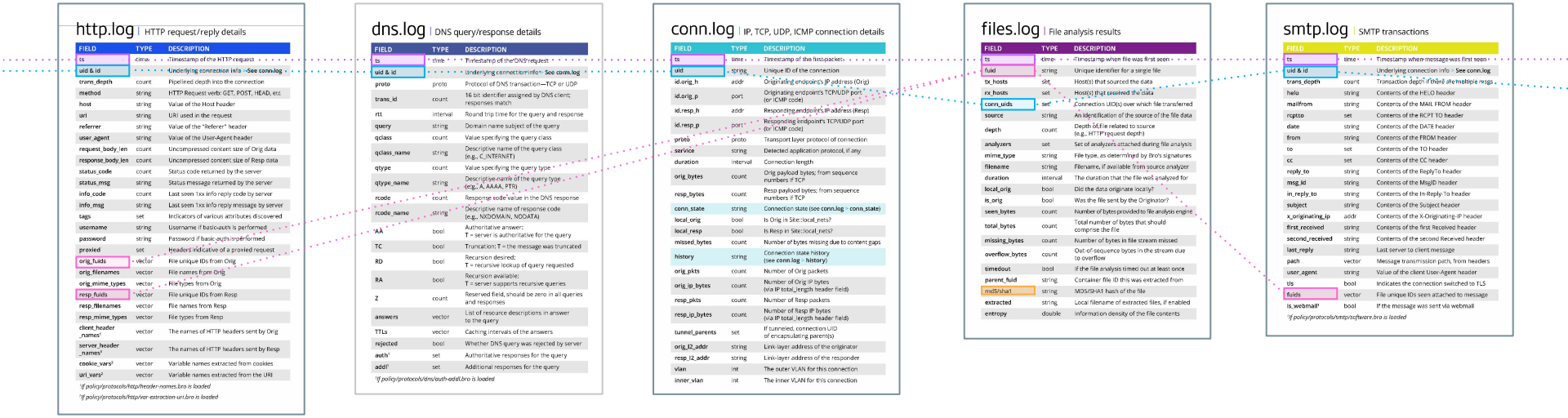
What is Zeek?



Network data wasn’t made for security.



Zeek transforms raw traffic into rich security stories



http.log | HTTP request/reply details

FIELD	TYPE	DESCRIPTION
ts	time	Timestamp of the HTTP request
uid & id		Underlying connection info > See conn.log
trans_depth	count	Pipelined depth into the connection
method	string	HTTP Request verb: GET, POST, HEAD, etc
host	string	Value of the Host header
uri	string	URI used in the request
referrer	string	Value of the "Referer" header
user_agent	string	Value of the User-Agent header
request_body_len	count	Uncompressed content size of Orig data
response_body_len	count	Uncompressed content size of Resp data
status_code	count	Status code returned by the server
status_msg	string	Status message returned by the server
info_code	count	Last seen 1xx info reply code by server
info_msg	string	Last seen 1xx info reply message by server
tags	set	Indicators of various attributes discovered
username	string	Username if basic-auth is performed
password	string	Password if basic-auth is performed
proxied	set	Headers indicative of a proxied request
orig_fuids	vector	File unique IDs from Orig
orig_filenames	vector	File names from Orig
orig_mime_types	vector	File types from Orig
resp_fuids	vector	File unique IDs from Resp
resp_filenames	vector	File names from Resp
resp_mime_types	vector	File types from Resp
client_header_names[1]	vector	The names of HTTP headers sent by Orig
server_header_names[1]	vector	The names of HTTP headers sent by Resp
cookie_vars[2]	vector	Variable names extracted from cookies
uri_vars[2]	vector	Variable names extracted from the URI

[1] If policy/protocols/http/header-names.bro is loaded
[2] If policy/protocols/http/var-extraction-uri.bro is loaded

dns.log | DNS query/response details

FIELD	TYPE	DESCRIPTION
ts	time	Timestamp of the DNS request
uid & id		Underlying connection info > See conn.log
proto	proto	Protocol of DNS transaction—TCP or UDP
trans_id	count	16 bit identifier assigned by DNS client; responses match
rtt	interval	Round trip time for the query and response
query	string	Domain name subject of the query
qclass	count	Value specifying the query class
qclass_name	string	Descriptive name of the query class (e.g., C_INTERNET)
qtype	count	Value specifying the query type
qtype_name	string	Descriptive name of the query type (e.g., A, AAAA, PTR)
rcode	count	Response code value in the DNS response
rcode_name	string	Descriptive name of response code (e.g., NXDOMAIN, NODATA)
AA	bool	Authoritative answer: T = server is authoritative for the query
TC	bool	Truncation: T = the message was truncated
RD	bool	Recursion desired: T = recursive lookup of query requested
RA	bool	Recursion available: T = server supports recursive queries
Z	count	Reserved field, should be zero in all queries and responses
answers	vector	List of resource descriptions in answer to the query
TTLs	vector	Caching intervals of the answers
rejected	bool	Whether DNS query was rejected by server
auth[1]	set	Authoritative responses for the query
addl[1]	set	Additional responses for the query

[1] If policy/protocols/dns/auth-addl.bro is loaded

conn.log | IP, TCP, UDP, ICMP connection details

FIELD	TYPE	DESCRIPTION
ts	time	Timestamp of the first packet
uid	string	Unique ID of the connection
id.orig_h	addr	Originating endpoint's IP address (Orig)
id.orig_p	port	Originating endpoint's TCP/UDP port (or ICMP code)
id.resp_h	addr	Responding endpoint's IP address (Resp)
id.resp_p	port	Responding endpoint's TCP/UDP port (or ICMP code)
proto	proto	Transport layer protocol of connection
service	string	Detected application protocol, if any
duration	interval	Connection length
orig_bytes	count	Orig payload bytes; from sequence numbers if TCP
resp_bytes	count	Resp payload bytes; from sequence numbers if TCP
conn_state	string	Connection state (see conn.log > conn_state)
local_orig	bool	Is Orig in Site::local_nets?
local_resp	bool	Is Resp in Site::local_nets?
missed_bytes	count	Number of bytes missing due to content gaps
history	string	Connection state history (see conn.log > history)
orig_pkts	count	Number of Orig packets
orig_ip_bytes	count	Number of Orig IP bytes (via IP total_length header field)
resp_pkts	count	Number of Resp packets
resp_ip_bytes	count	Number of Resp IP bytes (via IP total_length header field)
tunnel_parents	set	If tunneled, connection UID of encapsulating parent(s)
orig_l2_addr	string	Link-layer address of the originator
resp_l2_addr	string	Link-layer address of the responder
vlan	int	The outer VLAN for this connection
inner_vlan	int	The inner VLAN for this connection

files.log | File analysis results

FIELD	TYPE	DESCRIPTION
ts	time	Timestamp when file was first seen
fuid	string	Unique identifier for a single file
tx_hosts	set	Host(s) that sourced the data
rx_hosts	set	Host(s) that received the data
conn_uids	set	Connection UID(s) over which file transferred
source	string	An identification of the source of the file data
depth	count	Depth of file related to source (e.g., HTTP request depth)
analyzers	set	Set of analyzers attached during file analysis
mime_type	string	File type, as determined by Bro's signatures
filename	string	Filename, if available from source analyzer
duration	interval	The duration that the file was analyzed for
local_orig	bool	Did the data originate locally?
is_orig	bool	Was the file sent by the Originator?
seen_bytes	count	Number of bytes provided to file analysis engine
total_bytes	count	Total number of bytes that should comprise the file
missing_bytes	count	Number of bytes in file stream missed
overflow_bytes	count	Out-of-sequence bytes in the stream due to overflow
timedout	bool	If the file analysis timed out at least once
parent_fuid	string	Container file ID this was extracted from
md5/sha1	string	MD5/SHA1 hash of the file
extracted	string	Local filename of extracted files, if enabled
entropy	double	Information density of the file contents

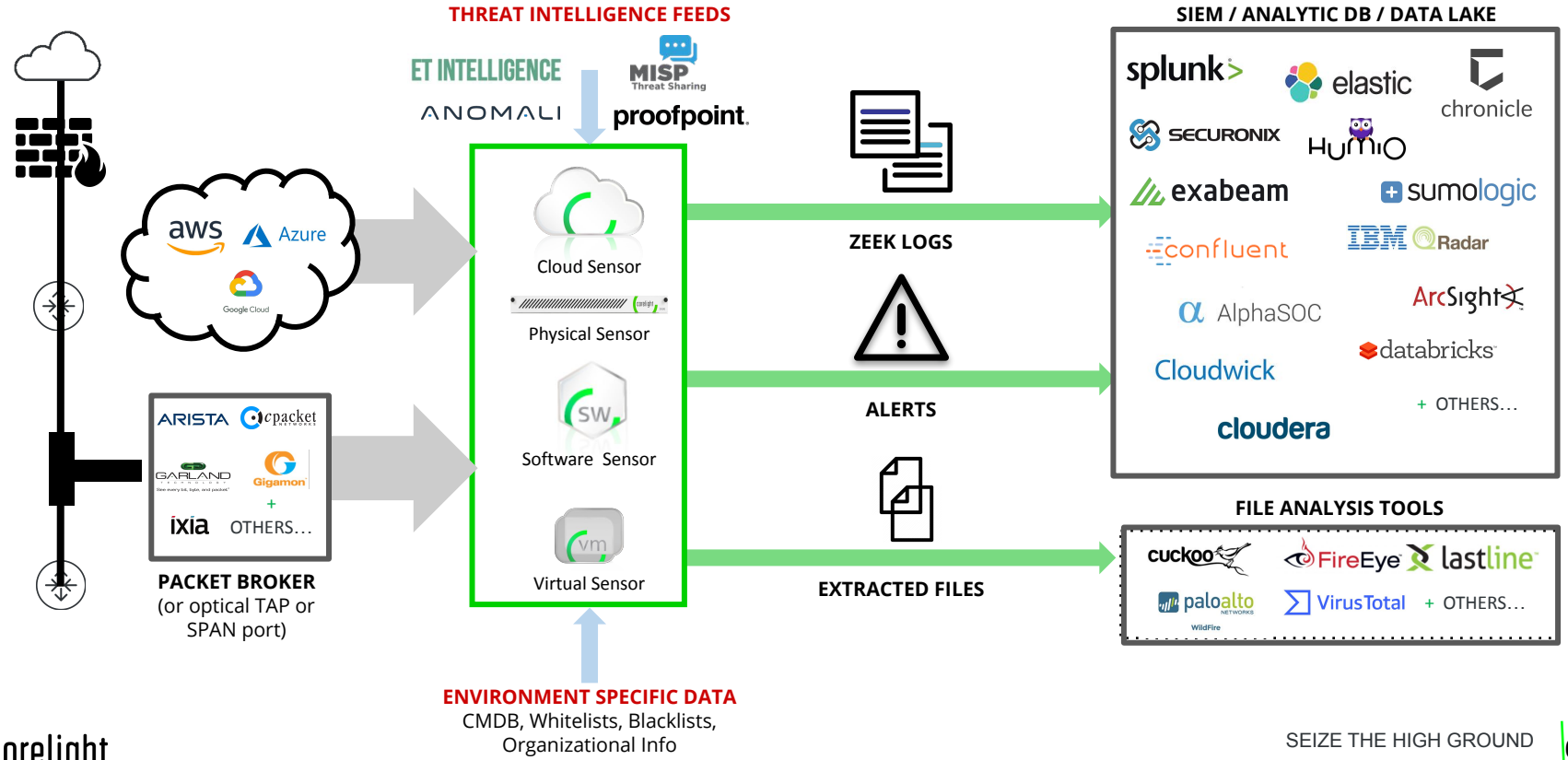
smtp.log | SMTP transactions

FIELD	TYPE	DESCRIPTION
ts	time	Timestamp when message was first seen
uid & id		Underlying connection info > See conn.log
trans_depth	count	Transaction depth if there are multiple msgs
helo	string	Contents of the HELO header
mailfrom	string	Contents of the MAIL FROM header
rcptto	set	Contents of the RCPT TO header
date	string	Contents of the DATE header
from	string	Contents of the FROM header
to	set	Contents of the TO header
cc	set	Contents of the CC header
reply_to	string	Contents of the ReplyTo header
msg_id	string	Contents of the MsgID header
in_reply_to	string	Contents of the In-Reply-To header
subject	string	Contents of the Subject header
x_originating_ip	addr	Contents of the X-Originating-IP header
first_received	string	Contents of the first Received header
second_received	string	Contents of the second Received header
last_reply	string	Last server to client message
path	vector	Message transmission path, from headers
user_agent	string	Value of the client User-Agent header
tls	bool	Indicates the connection switched to TLS
fuids	vector	File unique IDs seen attached to message
is_webmail[1]	bool	If the message was sent via webmail

[1] If policy/protocols/smtp/software.bro is loaded

ts	Timestamps with microsecond accuracy, synchronized across logs
uid	Unique ID for every connection
md5/sha1	File hash of every file
fuid	Unique ID for every instance of every file seen on the network

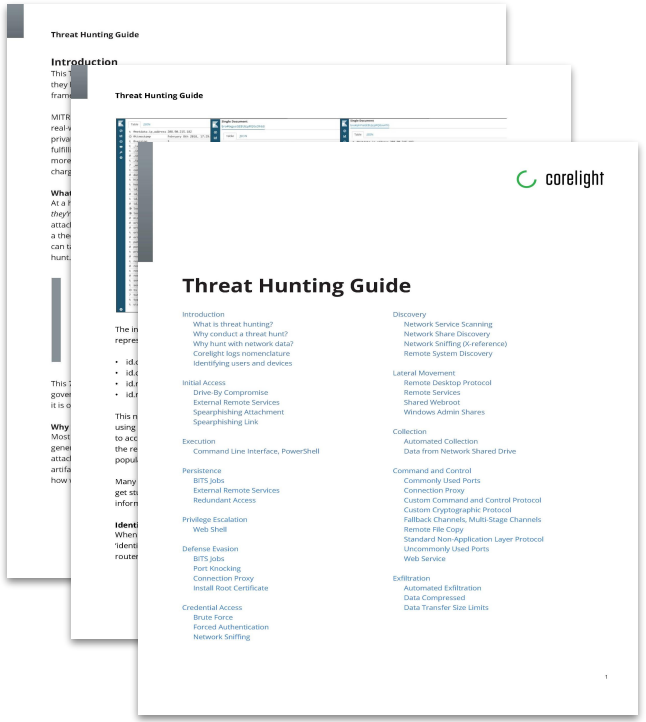
Typical Deployment



Corelight's Threat Hunting Guide

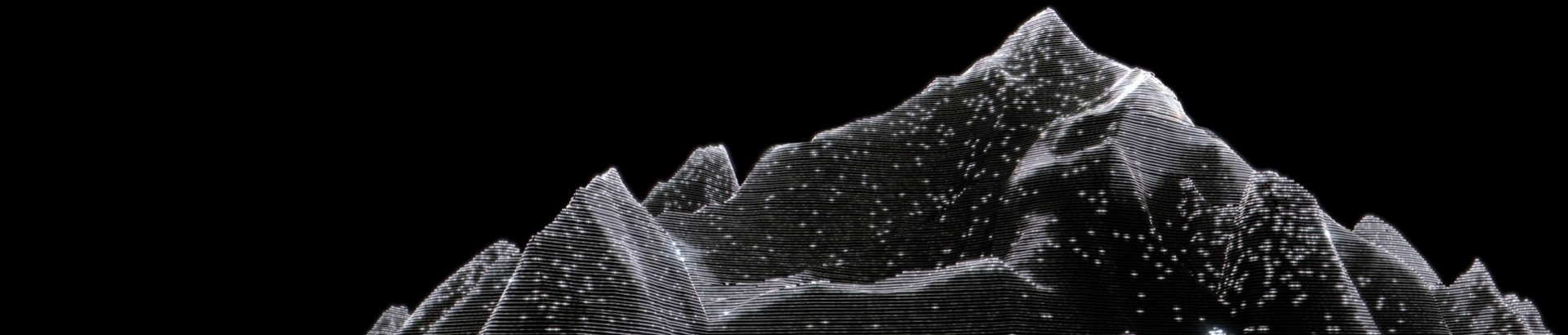
Your free guide to the essentials of network-based threat hunting

- In-depth guide to deepen your knowledge of threat hunting
- Demonstrates the benefits of a data-centric approach
- Great companion for our free Sigma rules



corelight

What is SIGMA?



What is SIGMA?

- An open source project which provides generic signature format for SIEMs
- “Sigma is for log files what Snort is for network traffic and YARA is for files.”
- Think of it like a “Rosetta Stone” of SIEM queries

SIGMA and Zeek

- Corelight contracted with SOC Prime (Nate Guagenti - @neu5ron) to create Zeek data mappings for SIGMA, which we published in 2020

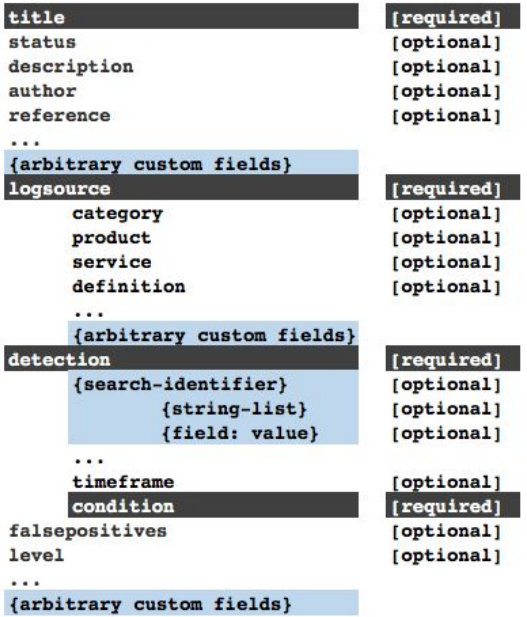
https://github.com/Neo23x0/sigma/tree/master/tools/config

Quick Demo: https://twitter.com/i/status/1256558461292339200

- SIGMA is pretty heavily endpoint based, but Zeek is helping to change this!

Schema and example SIGMA query

```
title: Suspicious PsExec Execution - Zeek
description: detects execution of psexec or paexec with renamed service name, this rule helps to filter out the noise if psexec is used for legit purposes or if attacker uses a different psexec client other than sysinternal one
author: 'Samir Bousseaden, @neu5ron'
date: 2020/04/02
references:
    - https://github.com/neo23x0/sigma/blob/d42e87edd741dd646db946f30964f331f92f50e6/rules/windows/builtin/win_susp_psexec.yml
tags:
    - attack.lateral_movement
    - attack.t1077
logsource:
    product: zeek
    service: smb_files
detection:
    selection1:
        name: '*\IPC$'
        path:
         - '*-stdin'
         - '*-stdout'
         - '*-stderr'
    selection2:
        name: '*\IPC$'
        path: 'PSEXESVC*'
    condition: selection1 and not selection2
falsepositives:
    - nothing observed so far
level: high
```



corelight

Example output from query

Elastic:
```
(event.dataset:smb_files AND (file.name:*\\IPC$ AND file.path:(*\-stdin OR *\-stdout OR *\-stderr)) AND (NOT (file.name:*\\IPC$ AND file.path:PSEXESVC*)))
```

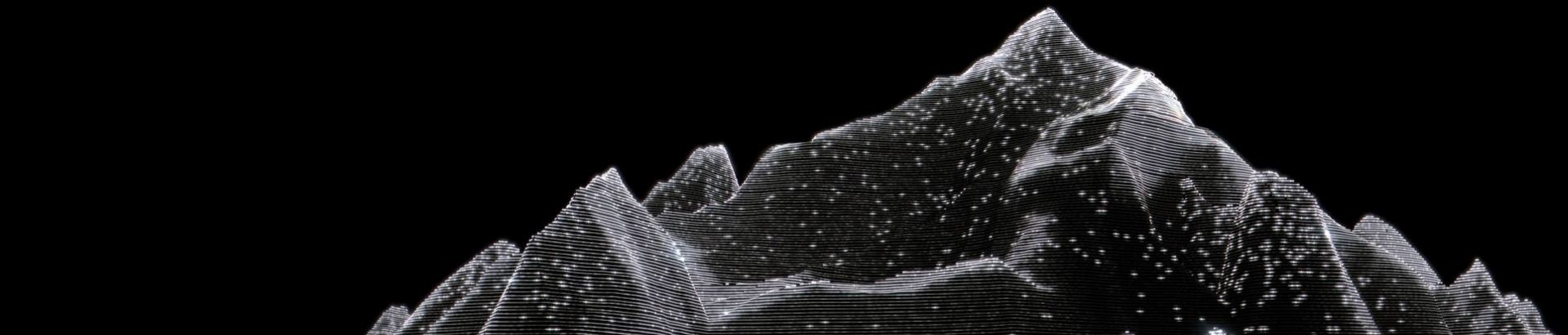
Splunk:
```
(sourcetype="bro:smb_files:json" (name="*\\IPC$" (path="*-stdin" OR path="*-stdout" OR path="*-stderr")) NOT (name="*\\IPC$" path="PSEXESVC*"))
```

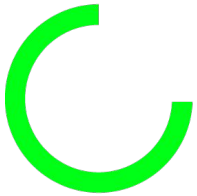
Uncoder.io and TDM

- TDM - Threat Detection Marketplace from SOC Prime
  - tdm.socprime.com
  - free and paid rules plus bounty program
- Uncoder - Translator app created by SOC Prime
- Includes 15+ SIEM and data formats including:
  - Splunk
  - Kibana
  - Humio
  - Arcsight
  - Sentinel
  - and more!

corelight

The Corelight Threat Hunting Sigma Rules



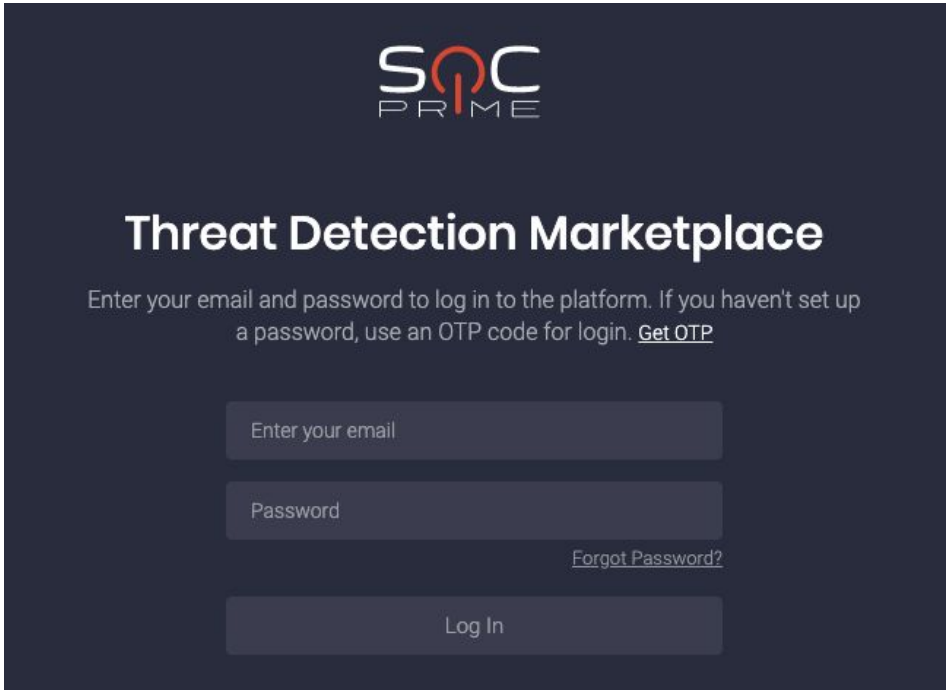


corelight + SIGMA

- Over 70 new Sigma rules released by Corelight
  - (authored by SOC Prime)
- Mapped to MITRE ATT&CK TTPs
  - 26 techniques (16 unique top level)
  - 10 categories
- Designed around our Corelight Threat Hunting Guide v2
- Free and open to contributions and improvements
- Currently hosted on SOC Prime's Threat Detection Marketplace (TDM)

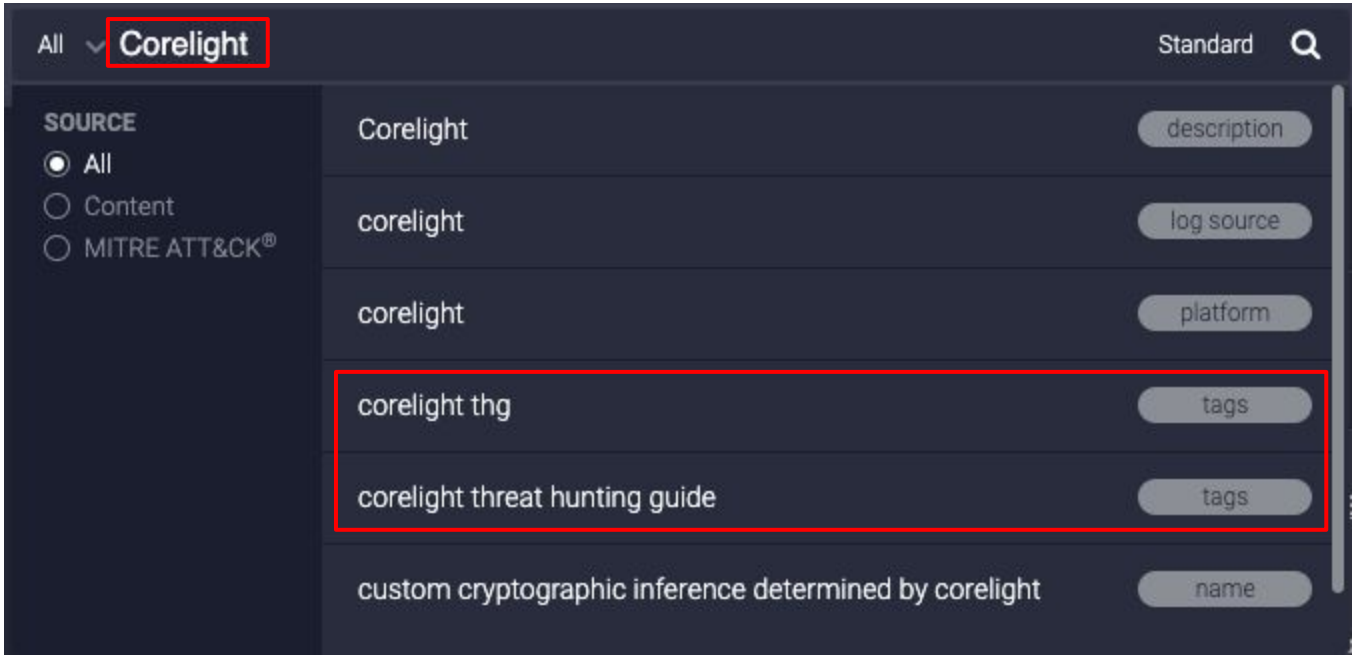
How do I get these rules?

Visit https://tdm.socprime.com to log in or **create a free account**

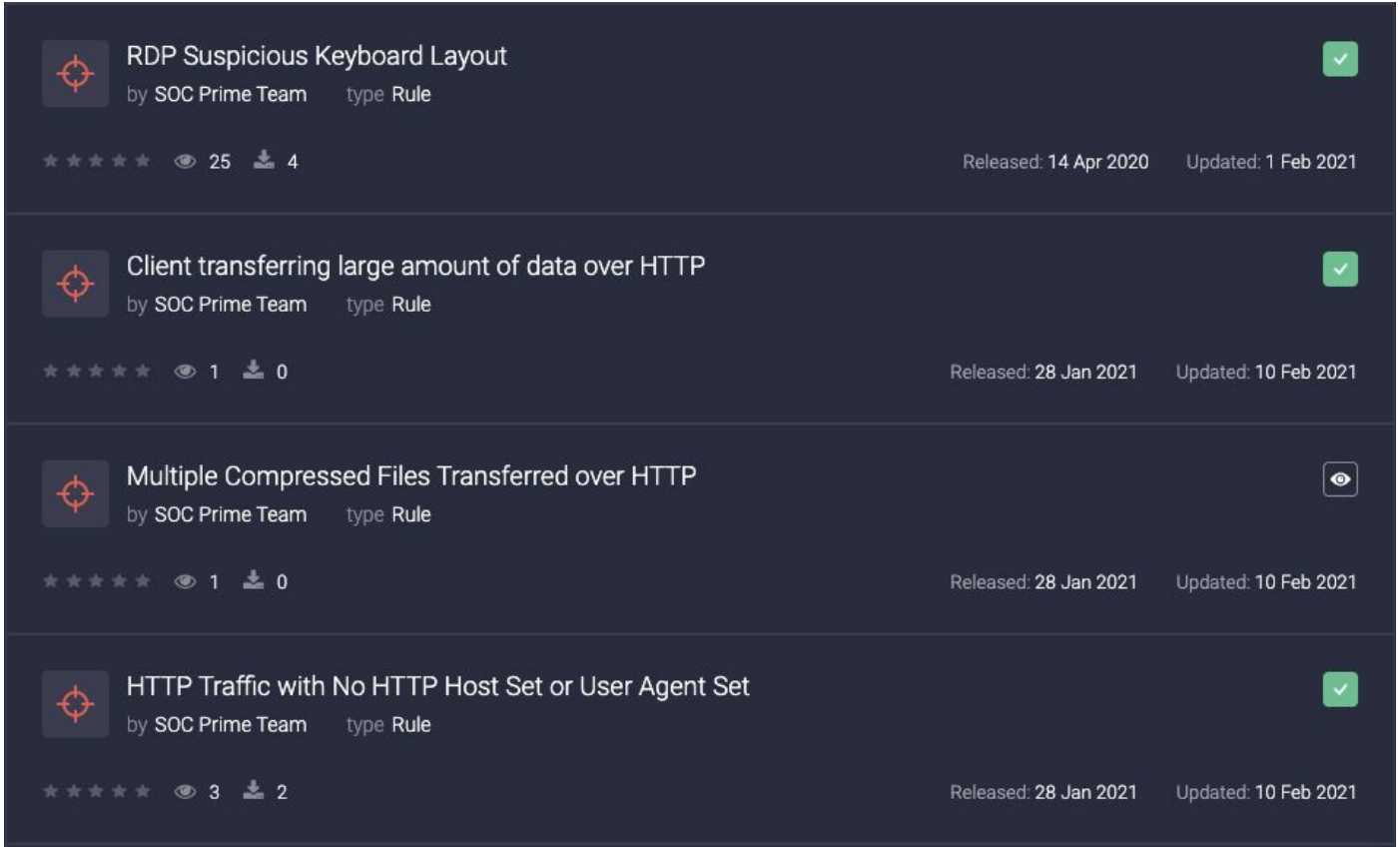


How do I get these rules?

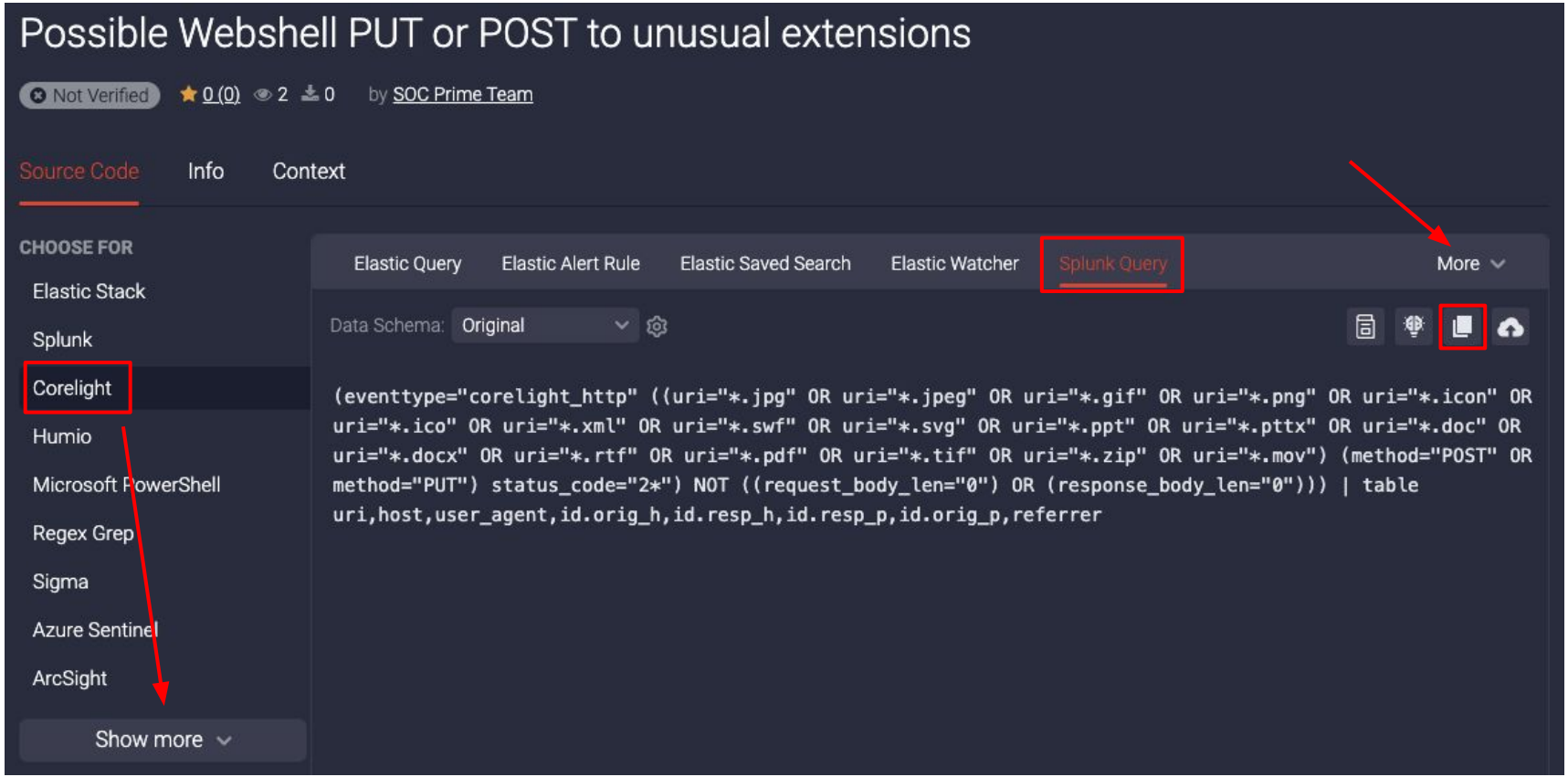
Search for “Corelight” in the search bar; select one of the relevant tags



How do I get these rules?



How do I use these rules?



Rule: Possible Webshell PUT or POST to unusual extensions

New Search

Save As ▾ New Table Close

```
(eventtype="corelight_http" ((uri="*.jpg" OR uri="*.jpeg" OR uri="*.gif" OR uri="*.png" OR uri="*.icon" OR uri="*.ico" OR uri="*.xml" OR uri="*.swf" OR uri="*.svg" OR uri="
    *.ppt" OR uri="*.pttx" OR uri="*.doc" OR uri="*.docx" OR uri="*.rtf" OR uri="*.pdf" OR uri="*.tif" OR uri="*.zip" OR uri="*.mov") (method="POST" OR method="PUT")
    status_code="2*") NOT ((request_body_len="0") OR (response_body_len="0"))) | table uri,host,user_agent,id.orig_h,id.resp_h,id.resp_p,id.orig_p,referrer
```

Last 200 days ▾

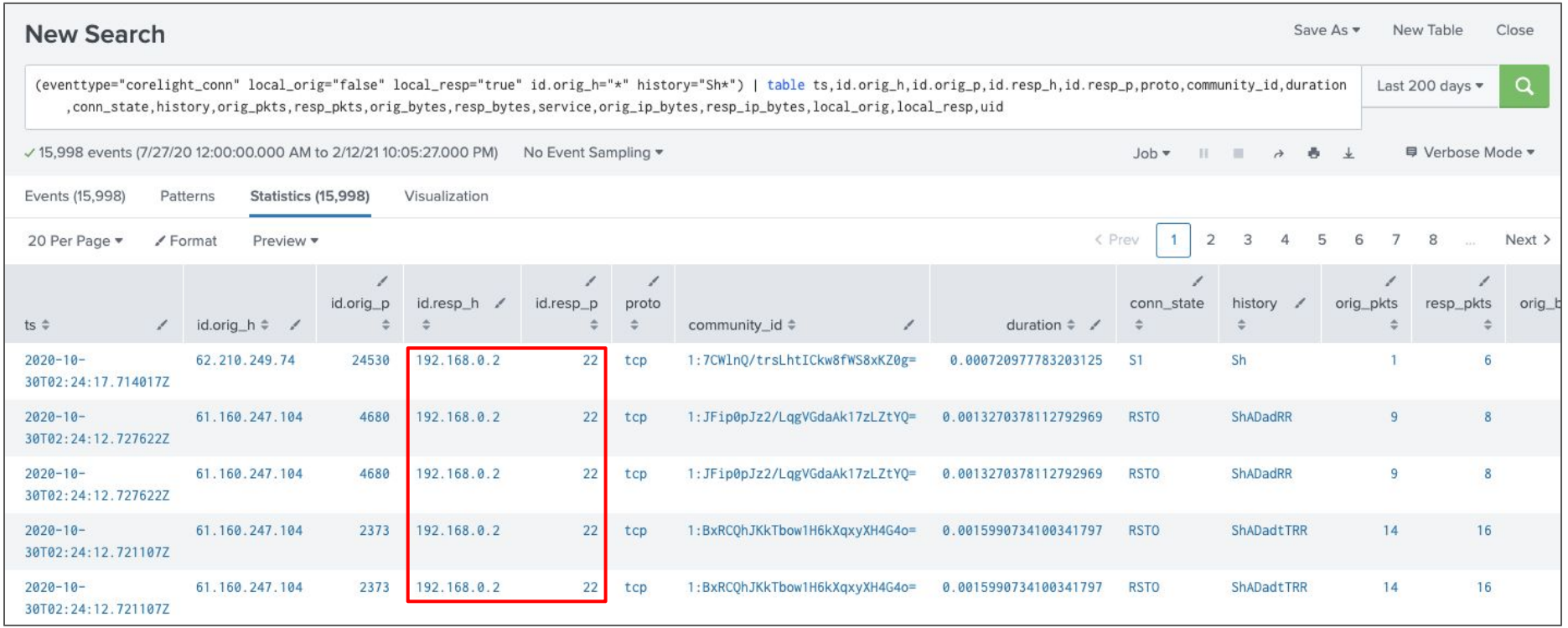
✓ 8 events (7/27/20 12:00:00.000 AM to 2/12/21 9:22:23.000 PM) No Event Sampling ▾ Job ▾ Verbose Mode ▾

Events (8) Patterns **Statistics (8)** Visualization

20 Per Page ▾ Format Preview ▾

uri	host	user_agent	id.orig_h	id.resp_h	id.resp_p	id.orig_p	referrer
/pixel.gif	3c22c4fa.static.spillpalletonline.com	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)	10.4.5.101	188.165.62.40	80	49192	
/pixel.gif	3c22c4fa.static.spillpalletonline.com	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)	10.4.5.101	188.165.62.40	80	49192	
/pixel.gif	3c22c4fa.static.spillpalletonline.com	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)	10.4.5.101	188.165.62.40	80	49192	
/pixel.gif	3c22c4fa.static.spillpalletonline.com	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)	10.4.5.101	188.165.62.40	80	49192	

Rule: Response from External Facing Service (Overview Query)



New Search

Save As ▾ New Table Close

```
(eventtype="corelight_conn" local_orig="false" local_resp="true" id.orig_h="*" history="Sh*") | table ts,id.orig_h,id.orig_p,id.resp_h,id.resp_p,proto,community_id,duration
    ,conn_state,history,orig_pkts,resp_pkts,orig_bytes,resp_bytes,service,orig_ip_bytes,resp_ip_bytes,local_orig,local_resp,uid
```

Last 200 days ▾

✓ 15,998 events (7/27/20 12:00:00.000 AM to 2/12/21 10:05:27.000 PM) No Event Sampling ▾ Job ▾ Verbose Mode ▾

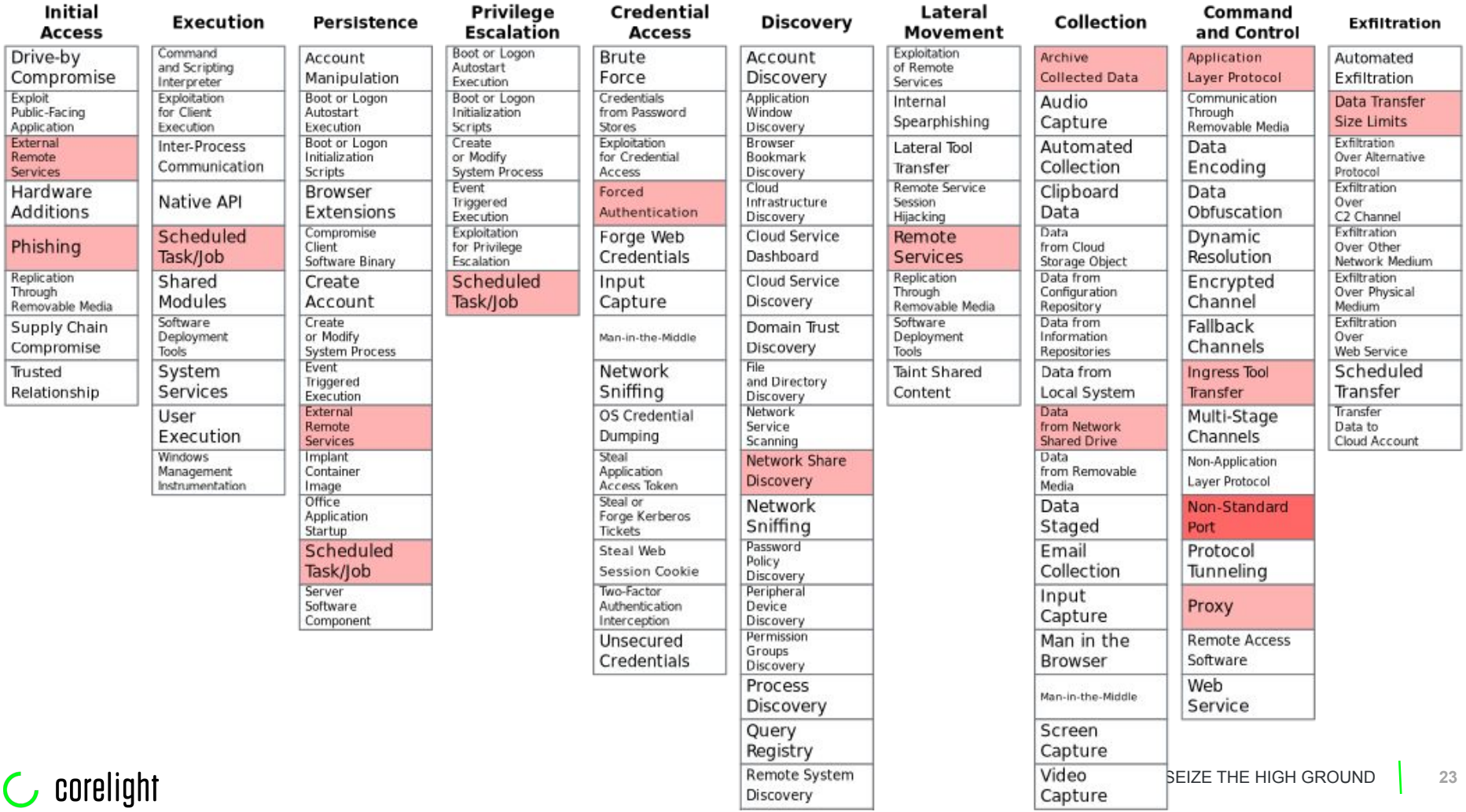
Events (15,998) Patterns **Statistics (15,998)** Visualization

20 Per Page ▾ Format Preview ▾ < Prev 1 2 3 4 5 6 7 8 ... Next >

ts	id.orig_h	id.orig_p	id.resp_h	id.resp_p	proto	community_id	duration	conn_state	history	orig_pkts	resp_pkts	orig_b
2020-10-30T02:24:17.714017Z	62.210.249.74	24530	192.168.0.2	22	tcp	1:7CWlnQ/trsLhtICkw8fWS8xKZ0g=	0.000720977783203125	S1	Sh	1	6	
2020-10-30T02:24:12.727622Z	61.160.247.104	4680	192.168.0.2	22	tcp	1:JFip0pJz2/LqgVGdaAk17zLZtYQ=	0.0013270378112792969	RSTO	ShADadRR	9	8	
2020-10-30T02:24:12.727622Z	61.160.247.104	4680	192.168.0.2	22	tcp	1:JFip0pJz2/LqgVGdaAk17zLZtYQ=	0.0013270378112792969	RSTO	ShADadRR	9	8	
2020-10-30T02:24:12.721107Z	61.160.247.104	2373	192.168.0.2	22	tcp	1:BxRCQhJKkTbow1H6kXqxyXH4G4o=	0.0015990734100341797	RSTO	ShADadtTRR	14	16	
2020-10-30T02:24:12.721107Z	61.160.247.104	2373	192.168.0.2	22	tcp	1:BxRCQhJKkTbow1H6kXqxyXH4G4o=	0.0015990734100341797	RSTO	ShADadtTRR	14	16	

Rule: C2 DGA Detected Via Repetitive Failures

ts	id.orig_h	id.orig_p	id.resp_h	id.resp_p	proto	qtype_name	qtype	query	answers	rcode	rcode_name
2020-10-30T02:57:53.984168Z	192.168.204.141	63243	192.168.204.2	53	udp	A	1	oaeyopqpwmctvstgrv.com		3	NXDOMAIN
2020-10-30T02:57:53.983981Z	192.168.204.141	63437	192.168.204.2	53	udp	A	1	kqvohmvyfjbwsjrcpx.com		3	NXDOMAIN
2020-10-30T02:57:53.983834Z	192.168.204.141	62667	192.168.204.2	53	udp	A	1	gnrsypvuwbisjzxya.com		3	NXDOMAIN
2020-10-30T02:57:53.983448Z	192.168.204.141	56175	192.168.204.2	53	udp	A	1	idiexymtmrcxvg.com		3	NXDOMAIN
2020-10-30T02:57:53.983217Z	192.168.204.141	51474	192.168.204.2	53	udp	A	1	adisgbbajbjokvr.com		3	NXDOMAIN
2020-10-30T02:57:53.982760Z	192.168.204.141	55659	192.168.204.2	53	udp	A	1	xwrobptfqcdzpxp8.com		3	NXDOMAIN
2020-10-30T02:57:53.982203Z	192.168.204.141	61305	192.168.204.2	53	udp	A	1	xevumdeninsk1.com		3	NXDOMAIN
2020-10-30T02:57:53.981762Z	192.168.204.141	53297	192.168.204.2	53	udp	A	1	zeyepwsksqepmxmgt6.com		3	NXDOMAIN
2020-10-30T02:57:53.981635Z	192.168.204.141	52684	192.168.204.2	53	udp	A	1	nafreasaozpckabb2.com		3	NXDOMAIN


Initial Access
Drive-by Compromise
Exploit Public-Facing Application
External Remote Services
Hardware Additions
Phishing
Replication Through Removable Media
Supply Chain Compromise
Trusted Relationship
Execution
Command and Scripting Interpreter
Exploitation for Client Execution
Inter-Process Communication
Native API
Scheduled Task/Job
Shared Modules
Software Deployment Tools
System Services
User Execution
Windows Management Instrumentation
Persistence
Account Manipulation
Boot or Logon Autostart Execution
Boot or Logon Initialization Scripts
Browser Extensions
Compromise Client Software Binary
Create Account
Create or Modify System Process
Event Triggered Execution
External Remote Services
Implant Container Image
Office Application Startup
Scheduled Task/Job
Server Software Component
Privilege Escalation
Boot or Logon Autostart Execution
Boot or Logon Initialization Scripts
Create or Modify System Process
Event Triggered Execution
Exploitation for Privilege Escalation
Scheduled Task/Job
Credential Access
Brute Force
Credentials from Password Stores
Exploitation for Credential Access
Forced Authentication
Forge Web Credentials
Input Capture
Man-in-the-Middle
Network Sniffing
OS Credential Dumping
Steal Application Access Token
Steal or Forge Kerberos Tickets
Steal Web Session Cookie
Two-Factor Authentication Interception
Unsecured Credentials
Discovery
Account Discovery
Application Window Discovery
Browser Bookmark Discovery
Cloud Infrastructure Discovery
Cloud Service Dashboard
Cloud Service Discovery
Domain Trust Discovery
File and Directory Discovery
Network Service Scanning
Network Share Discovery
Network Sniffing
Password Policy Discovery
Peripheral Device Discovery
Permission Groups Discovery
Process Discovery
Query Registry
Remote System Discovery
Lateral Movement
Exploitation of Remote Services
Internal Spearphishing
Lateral Tool Transfer
Remote Service Session Hijacking
Remote Services
Replication Through Removable Media
Software Deployment Tools
Taint Shared Content
Collection
Archive Collected Data
Audio Capture
Automated Collection
Clipboard Data
Data from Cloud Storage Object
Data from Configuration Repository
Data from Information Repositories
Data from Local System
Data from Network Shared Drive
Data from Removable Media
Data Staged
Email Collection
Input Capture
Man in the Browser
Man-in-the-Middle
Screen Capture
Video Capture
Command and Control
Application Layer Protocol
Communication Through Removable Media
Data Encoding
Data Obfuscation
Dynamic Resolution
Encrypted Channel
Fallback Channels
Ingress Tool Transfer
Multi-Stage Channels
Non-Application Layer Protocol
Non-Standard Port
Protocol Tunneling
Proxy
Remote Access Software
Web Service
Exfiltration
Automated Exfiltration
Data Transfer Size Limits
Exfiltration Over Alternative Protocol
Exfiltration Over C2 Channel
Exfiltration Over Other Network Medium
Exfiltration Over Physical Medium
Exfiltration Over Web Service
Scheduled Transfer
Transfer Data to Cloud Account

Summary - Q&A

1. **Download the Threat Hunting Guide**

   www3.corelight.com/corelights-introductory-guide-to-threat-hunting-with-zeek-bro-logs

2. **Sign up for a free Threat Detection Marketplace account**

   tdm.socprime.com

3. **Get for your free Sigma rules**

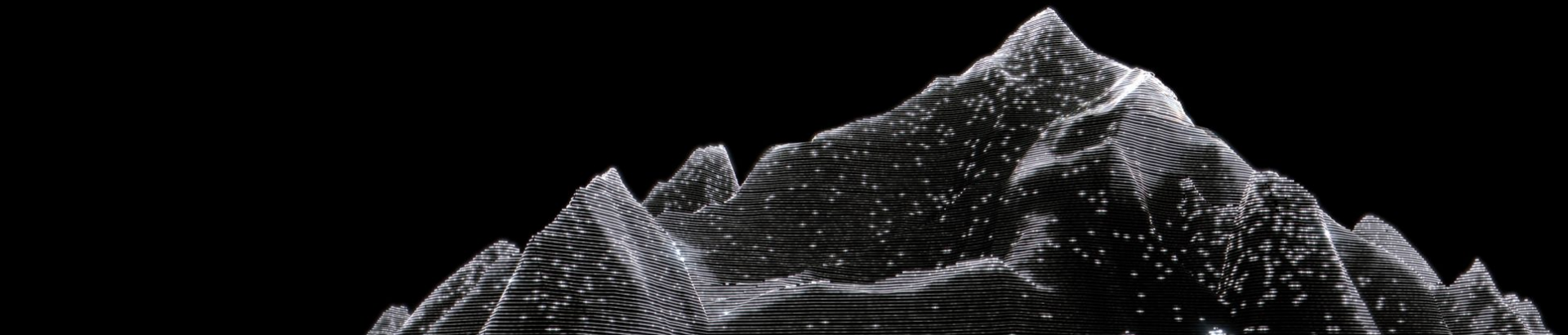
   Search for “Corelight” in the Threat Detection Marketplace

SIGMA resources

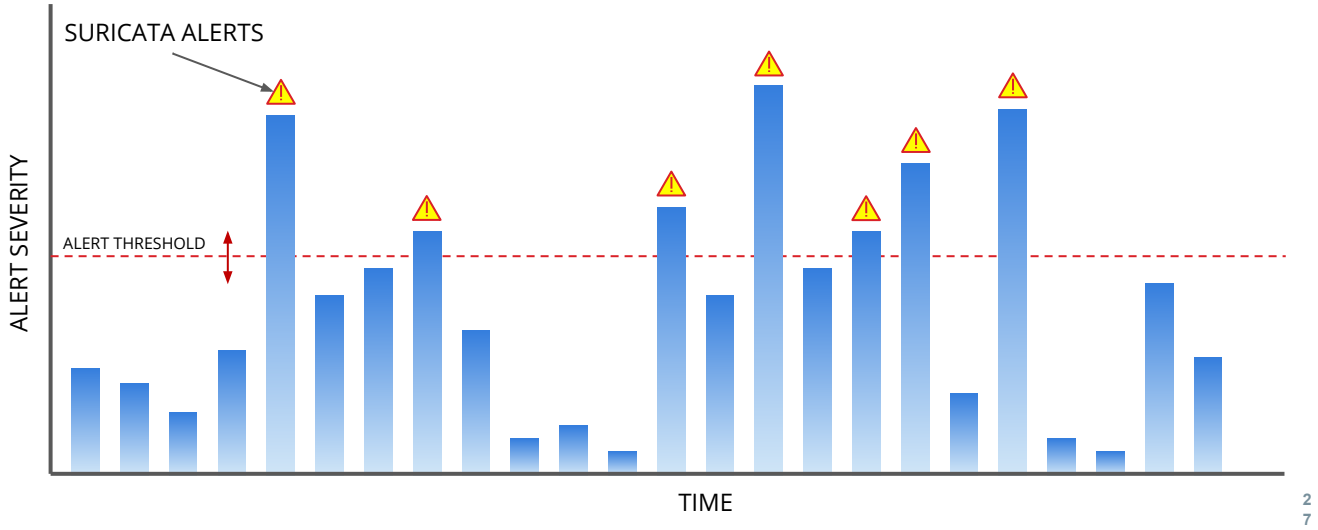
- Main Sigma page: https://github.com/Neo23x0/sigma
- A overview video from SANS (free registration required, starts at 39m)
  - https://www.sans.org/webcasts/mitre-att-ck-sigma-alerting-110010
- A how-to for writing Sigma rules by Florian Roth (one of the authors of SIGMA)
  - https://www.nextron-systems.com/2018/02/10/write-sigma-rules/
- Zeek Sigma pull request
  - https://github.com/Neo23x0/sigma/pull/723

corelight

Thank You



Suricata and Zeek are often used together



SURICATA - SIGNATURE-BASED DETECTIONS

Use best in class signature feeds like ET Pro

CPUs shared by Zeek & Suricata for better performance

Native UID linkage with Zeek for faster joint investigations

“The flashing red light”

ZEEK - POLICY-NEUTRAL METADATA COLLECTION

Collects data for everything

“The security camera”

We go where your traffic goes

Cloud Sensor

Up to 8 Gbps

AWS, Azure, GCP

Ingests traffic directly via native traffic mirroring or via packet brokers

Virtual Sensor

Up to 8 Gbps / instance

Requires VMware ESXi 6.5 or above or Hyper-V on Windows Server 2016

Software Sensor

Container or OS Native deployment

Lightweight (<60 MB)

Seamless scale out

Core Collection & Encrypted Traffic Collection

AP 200

2 Gbps

1U half-depth

Supports Suricata

AP 1001

10 Gbps

1U rack-mounted

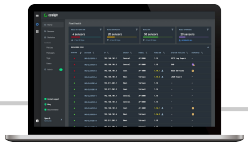
Supports Suricata

AP 3000

25 Gbps+

1U rack-mounted

Supports Suricata



Fleet Manager | VM, Manage up to 250 Sensors

Suricata + Zeek