Supercharging Network Security w/ SIGMA

Nate Guagenti (@neu5ron), SOC Prime

> (^W^h^Oa^mi /^A^L^I)

- @neu5ron (New-Tron)
- Father
- Employee at SOC Prime
- Author of None, Contributor of Some
  - https://github.com/Neo23x0/sigma
  - https://github.com/Cyb3rWard0g/HELK
  - https://github.com/hunters-forge/OSSEM
- Lego Builder

Agenda

- SIGMA Quick Recap
- Why Zeek or network for that matter
- Use Cases
- Screen sharing

Nate Guagenti
@neu5ron

SIGMA

1 | Common language.
Both for detections and search

600+ | Detection and rule logic.
One can cover many techniques

∞ | Infinite log possibilities

∞ | Infinite community

MISP, HELK, SecurityOnion, ATT&CK...

Nate Guagenti
@neu5ron

NSM Is Dead....

Nate Guagenti
@neu5ron

Endpoint is unable to cover:

Routers, Switches, Firewalls..

Virtualization (ie: ESXi) servers.

Bios/chip level.

SCADA/ICS. etc...

Nate Guagenti
@neu5ron

Nate Guagenti
@neu5ron

The Goldilogs

- conn.log
- **dce_rpc.log**
- dhcp.log
- dnp3.log
- dns.log
- dpd.log
- files.log
- ftp.log
- http.log
- irc.log
- kerberos.log
- known_certs.log
- known_devices.log
- known_hosts.log
- known_modbus.log
- known_services.log
- modbus_register_change.log
- modbus.log
- mysql.log
- notice.log
- ntlm.log
- pe.log
- radius.log
- rdp.log
- rfb.log
- sip.log
- smb_cmd.log
- **smb_files.log**
- **smb_mapping.log**
- smtp.log
- snmp.log
- socks.log
- software.log
- ssh.log
- ssl.log
- **syslog.log**
- traceroute.log
- tunnel.log
- weird.log
- x509.log
- ntp.log
- Lots of community ones
- Scada/ICS from
- MQTT
- Lots of community ones

Zeek Syslog: Logs in Logs

Time	ip_src_addr	ip_dst_addr		port_dst	protocol	severity	facility	message
2018-07-02 22:03:04.603	.170	1	30	514	udp	INFO	USER	
2018-07-02 22:03:00.608	40	1		514	udp	NOTICE	AUTH	
2018-07-02 22:02:57.260	9	1	19	514	udp	NOTICE	LOCAL7	","message":"3013: 003012: Jul 2 22:02:24.026: %DOT1X_SWITCH-5-ERR_VLAN_NOT_FOUND: Attempt to assign non-existent or shutdown VLAN VOICE to 802.1x port GigabitEthernet1/0/1 AuditSessionID 843D041D000000140 6"}
2018-07-02 22:02:57.260	163	1	1	514	udp	ERR	LOCAL2	","message":"Jul 2 22:02:53.466 GMT: F -ADX : %STKUNITO-M:CP %SNMP-3-SNMP_AUTH_FAIL: SNMP Authentication failure for SNMP request from host 1 1-Error:Unknown SNMPv3 Security/User name"}

Nate Guagenti
nate@neu5ron.com

SIGMA: Cisco AAA Crypto to Zeek syslog.log

https://github.com/Neo23x0/sigma/blob/master/rules/network/cisco/aaa/cisco_cli_crypto_actions.yml

CLI command to try yourself in splunk:

python3 tools/sigmac -t splunk -c tools/config/splunk-zeek.yml rules/network/cisco/aaa/cisco_cli_crypto_actions.yml

CLI command to try yourself in es-qs (lucene):

python3 tools/sigmac -t es-qs -c tools/config/logstash-zeek-default-json.yml rules/network/cisco/aaa/cisco_cli_crypto_actions.yml

```yaml
title: Cisco Crypto Commands
id: 1f978c6a-4415-47fb-aca5-736a44d7ca3d
status: experimental
description: Show when private keys are being exported from the device, or when new certi
references:
    - https://attack.mitre.org/techniques/T1145/
    - https://attack.mitre.org/techniques/T1130/
author: Austin Clark
date: 2019/08/12
tags:
    - attack.credential_access
    - attack.defense_evasion
    - attack.t1130
    - attack.t1145
logsource:
    product: cisco
    service: aaa
    category: accounting
fields:
    - src
    - CmdSet
    - User
    - Privilege_Level
    - Remote_Address
detection:
    keywords:
        - 'crypto pki export'
        - 'crypto pki import'
        - 'crypto pki trustpoint'
    condition: keywords
falsepositives:
    - Not commonly run by administrators.  Also whitelist your known good certificates.
level: high
```

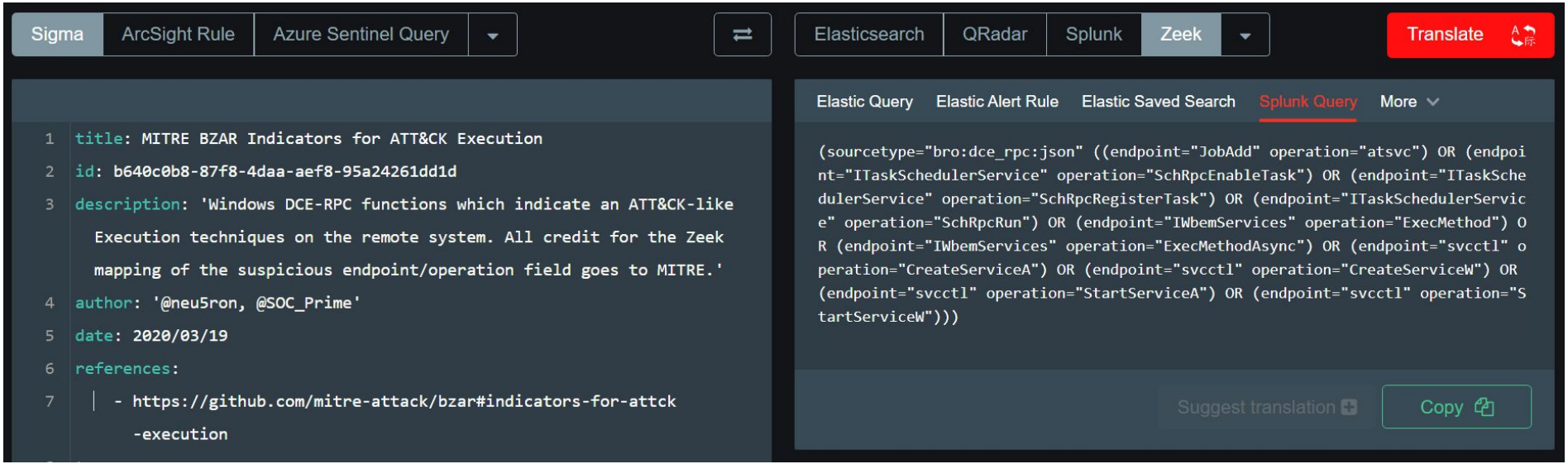
```
## Splunk
(sourcetype="bro:syslog:json" ("crypto pki export" OR "crypto pki import" OR "crypto pki
 trustpoint"))


## Elasticsearch Lucene (would work in Kibana search bar too)
(@stream:"syslog" AND \*.keyword:(*crypto\ pki\ export* OR *crypto\ pki\ import* OR *crypto\
 pki\ trustpoint*))
```

MITRE BZAR Execution SIGMA Rule View

```yaml
title: MITRE BZAR Indicators for ATT&CK Execution
id: b640c0b8-87f8-4daa-aef8-95a24261dd1d
description: 'Windows DCE-RPC functions which indicate an ATT&
CK-like Execution techniques on the remote system. All credit for
the Zeek mapping of the suspicious endpoint/operation field goes to
MITRE.'
author: '@neu5ron, @SOC_Prime'
date: 2020/03/19
references:
    - https://github.com/mitre-attack/
    bzar#indicators-for-attck-execution
tags:
  - attack.execution
  - attack.t1035
  - attack.t1047
  - attack.t1053
logsource:
  product: zeek
  service: dce_rpc
detection:
  op1:
    endpoint: 'JobAdd'
    operation: 'atsvc'
  op2:
    endpoint: 'ITaskSchedulerService'
    operation: 'SchRpcEnableTask'
  op3:
    endpoint: 'ITaskSchedulerService'
    operation: 'SchRpcRegisterTask'
  op4:
    endpoint: 'ITaskSchedulerService'
    operation: 'SchRpcRun'
  op5:
    endpoint: 'IWbemServices'
    operation: 'ExecMethod'
  op6:
    endpoint: 'IWbemServices'
    operation: 'ExecMethodAsync'
  op7:
    endpoint: 'svcctl'
    operation: 'CreateServiceA'
  op8:
    endpoint: 'svcctl'
    operation: 'CreateServiceW'
  op9:
    endpoint: 'svcctl'
    operation: 'StartServiceA'
  op10:
    endpoint: 'svcctl'
    operation: 'StartServiceW'
  condition: 1 of them
falsepositives:
    - 'Windows administrator tasks or troubleshooting'
    - 'Windows management scripts or software'
level: medium
```

Uncoder: MITRE BZAR Execution to Splunk



Uncoder: MITRE BZAR Execution to Elastic Query (Lucene)

Sigma | ArcSight Rule | Azure Sentinel Query | ⇄ | Elasticsearch | QRadar | Splunk | Zeek | Translate

```
1  title: MITRE BZAR Indicators for ATT&CK Execution
2  id: b640c0b8-87f8-4daa-aef8-95a24261dd1d
3  description: 'Windows DCE-RPC functions which indicate an
     ATT&CK-like Execution techniques on the remote system. All
     credit for the Zeek mapping of the suspicious endpoint
     /operation field goes to MITRE.'
4  author: '@neu5ron, @SOC_Prime'
5  date: 2020/03/19
6  references:
7    - https://github.com/mitre-attack/bzar#indicators-for
       -attck-execution
```

Elastic Query | Elastic Alert Rule | Elastic Saved Search | More

```
(@stream:"dce_rpc" AND ((endpoint:"JobAdd" AND operation:"atsvc") OR
(endpoint:"ITaskSchedulerService" AND operation:"SchRpcEnableTask") O
R (endpoint:"ITaskSchedulerService" AND operation:"SchRpcRegisterTas
k") OR (endpoint:"ITaskSchedulerService" AND operation:"SchRpcRun") O
R (endpoint:"IWbemServices" AND operation:"ExecMethod") OR (endpoin
t:"IWbemServices" AND operation:"ExecMethodAsync") OR (endpoint:"svcc
tl" AND operation:"CreateServiceA") OR (endpoint:"svcctl" AND operati
on:"CreateServiceW") OR (endpoint:"svcctl" AND operation:"StartServic
eA") OR (endpoint:"svcctl" AND operation:"StartServiceW")))
```

Suggest translation | Copy

Translating to: Zeek / Elastic Query

Uncoder: Web Server Multiple Error Caused by Single IP

Zeek http.log covers all same scenarios as existing Proxy and Web Server rules \o/

```
title: Multiple Suspicious Resp Codes Caused by Single Client
id: 6fdfc796-06b3-46e8-af08-58f3505318af
description: Detects possible exploitation activity or bugs in a web
  application
author: Thomas Patzke
date: 2017/02/19
modified: 2020/03/14
logsource:
  | category: webserver
detection:
  | selection:
  | | | sc-status:
  | | | | - 400
  | | | | - 401
  | | | | - 403
  | | | | - 500
  | timeframe: 10m
  | condition: selection | count() by src_ip > 10
falsepositives:
  | - Unstable application
  | - Application that misuses the response codes
```

```
curl -s -XPUT -H 'Content-Type: application/json' --data-binary @- localhos
t:9200/_watcher/watch/6fdfc796-06b3-46e8-af08-58f3505318af <<EOF
{
  "metadata": {
    "title": "Multiple Suspicious Resp Codes Caused by Single Client",
    "description": "Detects possible exploitation activity or bugs in a web
application",
    "tags": "",
    "query": "(@stream:\"http\" AND status_code:(\"400\" OR \"401\" OR \"403
\" OR \"500\"))"
  },
  "trigger": {
    "schedule": {
      "interval": "10m"
    }
  },
  "input": {
    "search": {
      "request": {
        "body": {
          "size": 0,
          "query": {
            "bool": {
              "must": [
                {
                  "query_string": {
                    "query": "(@stream:\"http\" AND status_code:(\"400\" OR
```

SIGMA: DCE RPC Enumeration (Elastalert)

https://github.com/Neo23x0/sigma/blob/master/rules/network/zeek/zeek-dce_rpc_domain_user_enumeration.yml

CLI command to try yourself:

python3 tools/sigmac -t elastalert -c tools/config/ecs-zeek-corelight.yml rules/network/zeek/zeek-dce_rpc_domain_user_enumeration.yml

```yaml
title: Domain User Enumeration Network Recon 01
description: Domain user and group enumeration via network reconnaissance. Seen in APT 29 and oth
id: 66a0bdc6-ee04-441a-9125-99d2eb547942
references:
    - "https://github.com/OTRF/detection-hackathon-apt29"
    - "https://github.com/OTRF/detection-hackathon-apt29/issues/37"
author: 'Nate Guagenti (@neu5ron), Open Threat Research (OTR)'
date: 2020/05/03
modified: 2020/05/03
tags:
    - attack.discovery
    - attack.t1087
    - attack.t1082
logsource:
    product: zeek
    service: dce_rpc
detection:
    selection:
        operation:
            #- LsarEnumerateTrustedDomains #potentially too many FPs, removing. caused by netlogo
            #- SamrEnumerateDomainsInSamServer #potentially too many FPs, removing. #method obtai
            - LsarLookupNames3 #method translates a batch of security principal names to their SI
            - LsarLookupSids3 #translates a batch of security principal SIDs to their name forms
            - SamrGetGroupsForUser #obtains a listing of groups that a user is a member of
            - SamrLookupIdsInDomain #method translates a set of RIDs into account names
            - SamrLookupNamesInDomain #method translates a set of account names into a set of RID
            - SamrQuerySecurityObject #method queries the access control on a server, domain, use
            - SamrQueryInformationGroup #obtains attributes from a group object
    timeframe: 30s
    condition: selection | count(operation) by src_ip > 4
falsepositives:
    - Devices that may do authentication like a VPN or a firewall that looksup IPs to username
    - False positives depend on scripts and administrative tools used in the monitored environment
level: medium
status: experimental
```

```yaml
alert:
- debug
buffer_time:
  seconds: 30
description: Domain user and group enumeration via network reconnaissance
  . Seen in APT 29 and other common tactics and actors. Detects a set of
  RPC (remote procedure calls) used to enumerate a domain controller. The
   rule was created based off the datasets and hackathon from
  https://github.com/OTRF/detection-hackathon-apt29
doc_type: doc
filter:
- query:
    query_string:
      query: (event.dataset:"dce_rpc" AND dce_rpc.operation:
  ("LsarLookupNames3" OR "LsarLookupSids3" OR "SamrGetGroupsForUser" OR
  "SamrLookupIdsInDomain" OR "SamrLookupNamesInDomain" OR
  "SamrQuerySecurityObject" OR "SamrQueryInformationGroup"))
index: '*ecs-*'
max_threshold: 4
metric_agg_key: dce_rpc.operation.keyword
metric_agg_type: cardinality
name: 66a0bdc6-ee04-441a-9125-99d2eb547942_0
priority: 3
query_key: source.ip.keyword
realert:
  minutes: 0
type: metric_aggregation
```

SIGMA: Windows Event ID 5145 Rule Converted to Zeek SMB (Elastalert)

https://github.com/Neo23x0/sigma/blob/master/rules/network/zeek/zeek-dce_rpc_domain_user_enumeration.yml

CLI command to try yourself:

python3 tools/sigmac -t elastalert -c tools/config/ecs-zeek-corelight.yml rules/network/zeek/zeek_smb_converted_win_lm_namedpipe.yml

```yaml
title: First Time Seen Remote Named Pipe - Zeek
id: 52d8b0c6-53d6-439a-9e41-52ad442ad9ad
description: This detection excludes known namped pipes accessible remotely and notify on newly observed ones, may help to detect lateral
 movement and remote exec
    using named pipes
author: 'Samir Bousseaden, @neu5ron'
date: 2020/04/02
references:
    - https://github.com/neo23x0/sigma/blob/d42e87edd741dd646db946f30964f331f92f50e6/rules/windows/builtin/win_lm_namedpipe.yml
tags:
    - attack.lateral_movement
    - attack.t1077
logsource:
    product: zeek
    service: smb_files
detection:
    selection1:
        path: \\*\IPC$
    selection2:
        path: \\*\IPC$
        name:
         - 'atsvc'
         - 'samr'
         - 'lsarpc'
         - 'winreg'
         - 'netlogon'
         - 'srvsvc'
         - 'protected_storage'
         - 'wkssvc'
         - 'browser'
         - 'netdfs'
         - 'svcctl'
         - 'spoolss'
         - 'ntsvcs'
         - 'LSM_API_service'
         - 'HydraLsPipe'
         - 'TermSrv_API_service'
         - 'MsFteWds'
    condition: selection1 and not selection2
falsepositives:
    - update the excluded named pipe to filter out any newly observed legit named pipe
```

```yaml
alert:
- debug
description: This detection excludes known namped pipes
 accessible remotely and notify on newly observed ones,
 may help to detect lateral movement and remote exec using
  named pipes
filter:
- query:
    query_string:
      query: (event.dataset:"smb_files" AND file.path
 .keyword:\\*\\IPC$ AND (NOT (file.path.keyword:\\*\\IPC$
 AND file.name:("atsvc" OR "samr" OR "lsarpc" OR "winreg"
 OR "netlogon" OR "srvsvc" OR "protected_storage" OR
 "wkssvc" OR "browser" OR "netdfs" OR "svcctl" OR
 "spoolss" OR "ntsvcs" OR "LSM_API_service" OR
 "HydraLsPipe" OR "TermSrv_API_service" OR "MsFteWds"))))
index: '*ecs-*'
name: 52d8b0c6-53d6-439a-9e41-52ad442ad9ad_0
priority: 2
realert:
  minutes: 0
type: any
```

SIGMAC (SIGMA Config aka Field Mapping)

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

 # Arcsight
tools/config/arcsight-zeek.yml

 # Elasticsearch: Lucene, Kibana, Elastalert, Watcher
tools/config/logstash-zeek-default-json.yml (No field rename ECS)
tools/config/ecs-zeek-corelight.yml (Corelight ECS)
tools/config/ecs-zeek-elastic-beats-implementation.yml (Filebeat ECS)

 # Splunk
tools/config/splunk-zeek.yml

 # If your database does not rename fields, it will work as is
Thus no need to write a SIGMAC

 # More on the way

Nate Guagenti
nate@neu5ron.com
Nate Guagenti
nate@neu5ron.com

Coming soon for test/use APT 29 Hackathon dataset:
https://zeek.neu5ron.com

Github, Twitter, & Interwebs:
@neu5ron

Linkedin
https://linkedin.com/in/NathanGuagenti