elastic

Cracking the Beacon

Automating the collection of indicators from Malware

Derek Ditch & Jessica David

Howdy!

Derek Ditch | Principal Security Research Eng
(he/him/his)
@dcode | @dcode

Derek is part of a team of threat researchers at Elastic that works to track threat actors, analyze malware, and build systems to do it at scale.

- Background in network forensics, malware analysis
- Former intrusion analyst at NSA
- Worked in banking & power grid cybersecurity
- Lives in TX between Austin and San Antonio
- 22 year veteran in MOCYBER*

*MOCYBER has brought the community such projects as RockNSM, CAPES, Elastic Container Project, as well as the word “Thrunting” (Threat Hunting)

elastic

Bonjour hi!

Jessica David | Senior Data Engineer

(she/her/hers)

@jeska | @jeska28

Jessica is part of a team of software engineers at Elastic that build the cloud services, data systems, and product experiences that help Elastic's users find and understand the threats facing their organizations.

- Career data pusher
  - Microsoft SQL, IBM Netezza, Hadoop...
- Wearer of many hats
  - Automation, scripting, data fixing...
- Devoted cat mom & amateur woodworker
- First SANS Summit!

elastic

Agenda

Background

Quacking the Code

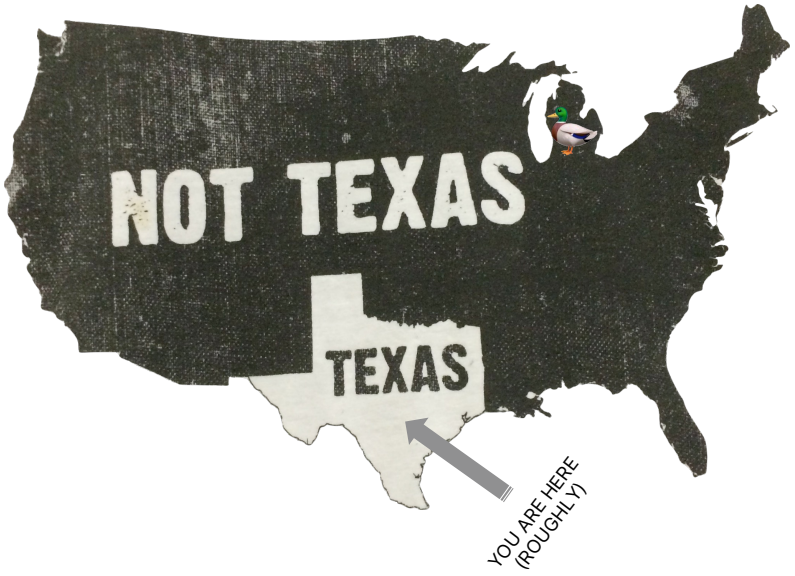
Demo & Future Work

elastic

Why are we here?

Better visibility of threats

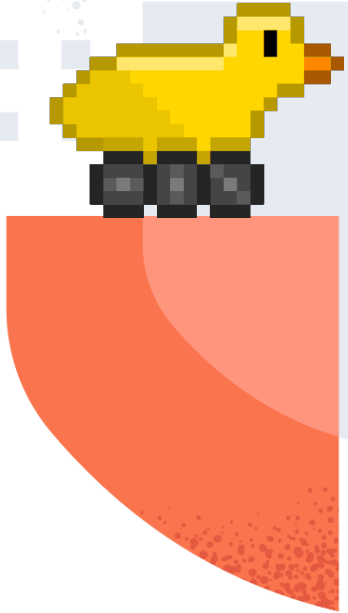
- Detecting known things is easy
- Tools like CobaltStrike and others make building new payloads easy
- Analyzing malware on endpoints to get C2 is tedious



elastic

🦆 Enter Malduck 🦆

- Malduck is a powerful static malware analysis tool created by CERT Polska*
- Provides powerful config extraction of malware features using YARA rules + Python
- So, find malware, dump it into a processing pipeline, find C2 and other information much faster than the manual process



* For interactive use, you can check out mwcfg, a 3rd party tool that lets your run against a single binary or directory with output to stdout

Extraction Workflow (IcedID)

Identify key functions in malware (encryption/decryption)

```
30  wcscpy(v9, L"%016IX");
31  ((void (__fastcall *)(char *, wchar_t *, unsigned __int64))*(&fp_Globals +
32
33  for ( i = 0i64; i < 32; ++i )
34    v12[i - 4] = encrypted_config[i] ^ encrypted_config[i + 64];
35
36  v4 = cookie_gen1(v11, 1u, (__int64)v10);
37
38  if ( v4 && (unsigned int)http_request_params((__int64)v12, (__int64)v4, (_
39  {
40    sub_1800014B4((__int64)lpMem, v14);
41    v5 = lpMem;
42    if ( lpMem )
43    {
```

elastic

Extraction Workflow (IcedID)

Generate YARA rule to pull in offset address of function and registers/values nearby

```
rule icedid {
    strings:
        $a1 = "loader_dll_64.dll" ascii fullword
        $config_decryption = {00 42 8A 44 01 ?? 42 32 04 01 88 44 0D ?? 48 FF C1
    condition:
        all of them
}
```

```
hit = p.uint32v(addr - 3)
config_location = hit + addr + 1

config_blob = p.readv(config_location,250)

key = config_blob[:32]
data = config_blob[64:96]

decrypted_config = xor(key,data)
```

elastic

Extraction Workflow (IcedID)

Write some Python to capture critical data


```
"campaign_id": 429479428,
"domains": "arelyevennot.top",
"family": "IcedID",
"key": "ea99698795276f8bd91533ee4106bf2a672b72030d1458338829c34124d37d49"
```


elastic

Hold Up.

What are we doing here?

elastic

We need samples

We've got some options:

- We can analyze malware statically on disk (if it's written to disk)
- We can analyze memory captures (don't worry, it won't hurt)
- We can leverage Elastic Security Endpoint

Demo

elastic

Setup Elastic Security

elastic

Find apps, content, and more. Ex: Discover ⌘/

D Integrations > Endpoint and Cloud ... > Add integration

Send feedback

Cancel

Add Endpoint and Cloud Security integration

Configure an integration for the selected agent policy.

1 Configure integration

Integration settings

Choose a name and description to help identify how this integration will be used.

Integration name

Name is required

Description Optional

Advanced options

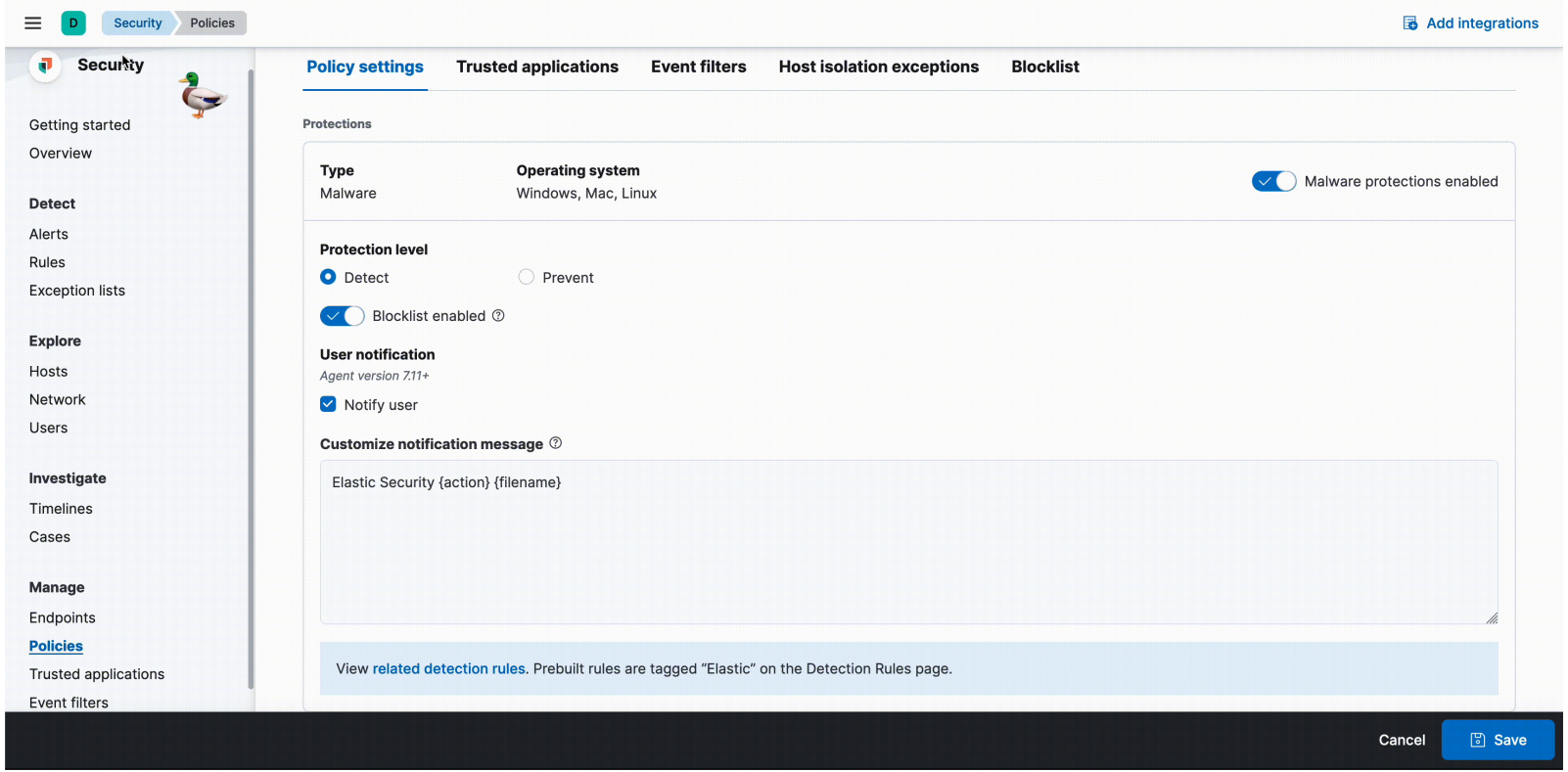
We'll save your integration with our recommended defaults. You can change this later by editing the Endpoint and Cloud Security integration within your agent policy.

2 Where to add this integration?

Your integration policy has errors. Please fix them before saving.

Cancel Save and continue

Configure Endpoint Policy



Enroll Agents & detonate something!

- Set up a sandbox VM (see our demo repo: https://ela.st/sans-dfir-2022)
  - Uses a Vagrantfile
  - Tested on VMWare
  - Follow instructions in README
- Create an Elastic cluster
  - Spin up locally
  - Use Elastic Cloud!
- Find a Cobaltstrike exe and cause trouble!

Check that alerts fired

Discover

Options New Open Share Inspect Save

Search KQL Last 1 day Refresh

+ Add filter

logs-endpoint.alerts-default

Search field names

Filter by type 0

Available fields 141

Popular

_id

agent.id

event.category

event.code

event.id

file.hash.sha256

message

process.entity_id

process.Ext.memory_region.bytes_compressed_present

rule.name

_index

_score

@timestamp

agent.build.original

4 hits

Documents Field statistics BETA

Aug 3, 2022 @ 14:51:20.581 - Aug 4, 2022 @ 14:51:20.581

1 field sorted

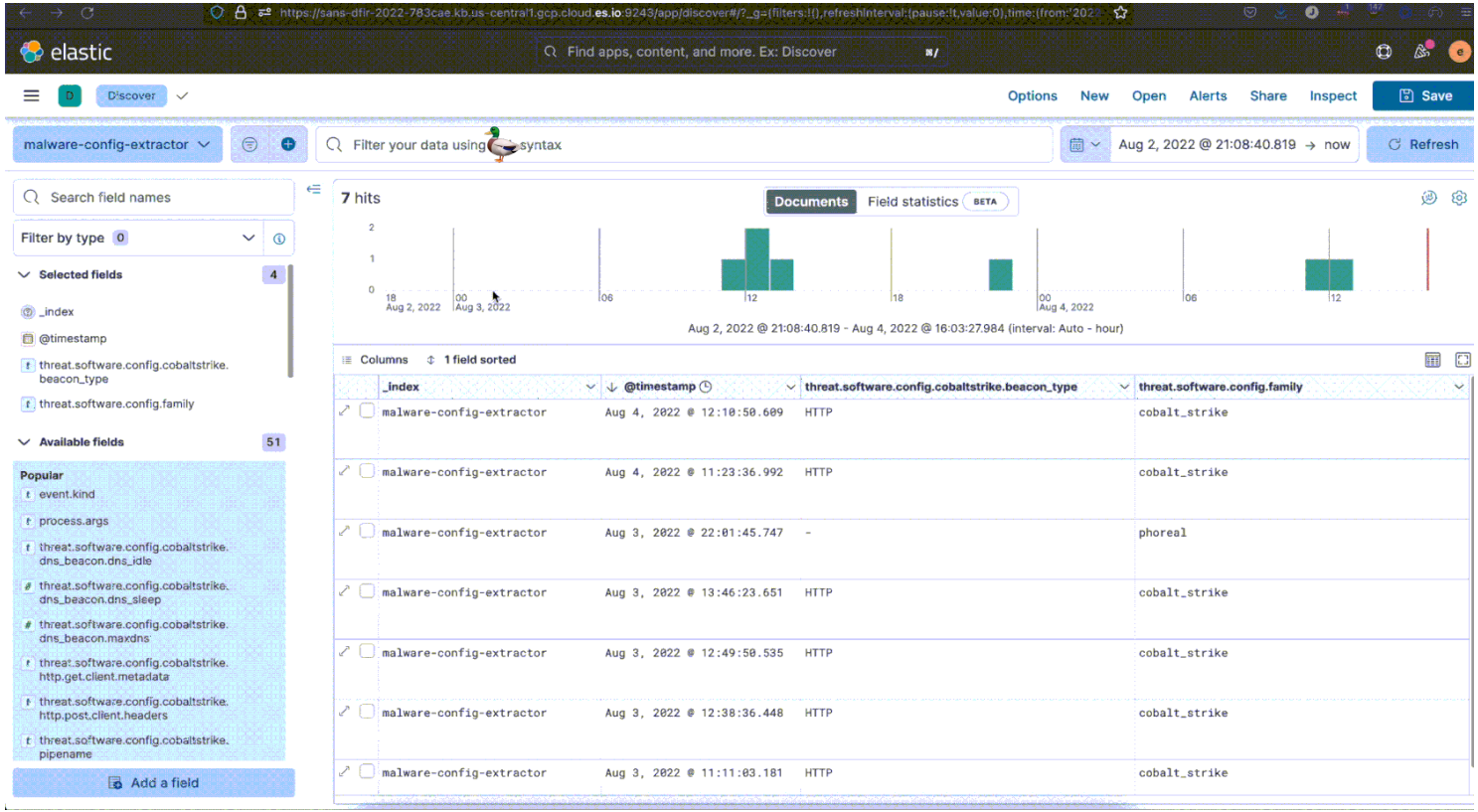
@timestamp	Document
Aug 4, 2022 @ 13:50:29.692	@timestamp Aug 4, 2022 @ 13:50:29.692 agent.build.original version: 8.2.2, compiled: Tue May 24 19:00:00 2022, branch: 8.2, commit: 4cea50c0c15c11a5b15f25 { "sha256": ["17d8695f22d3817c426a0e08a477b88ecdb6088bc253dfbccc760224600afcfd"], "name": ["diagnostic-endpointpe-v4-blocklist"] }, { "sha256": ["32d8 "92ec3c0262dd3acff20ff74f971b601e66c404267db3572ba50dc23d6cdb48e5"], "name": ["diagnostic-ransomware-v1-windows"] }, { "sha256": ["5def544b81f11a
Aug 4, 2022 @ 13:50:23.617	@timestamp Aug 4, 2022 @ 13:50:23.617 agent.build.original version: 8.2.2, compiled: Tue May 24 19:00:00 2022, branch: 8.2, commit: 4cea50c0c15c11a5b15f25223ff9e02324d212c5 agent.id 98ae5a29-62cd-4417-b181-378b91ee73dc agent.type endpoint agent.version 8.2.2 data_stream.dataset endpoint.alerts data_stream.namespace default data_stream.type logs e...
Aug 4, 2022 @ 10:30:37.818	@timestamp Aug 4, 2022 @ 10:30:37.818 agent.build.original version: 8.2.2, compiled: Tue May 24 19:00:00 2022, branch: 8.2, commit: 4cea50c0c15c11a5b15f25223ff9e02324d212c5 agent.id 790f88cc-517f-4759-be25-f7afe1b3c99f agent.type endpoint agent.version 8.2.2 data_stream.dataset endpoint.alerts data_stream.namespace default data_stream.type logs ecs.versi...
Aug 4, 2022 @ 09:32:12.656	@timestamp Aug 4, 2022 @ 09:32:12.656 agent.build.original version: 8.2.2, compiled: Tue May 24 19:00:00 2022, branch: 8.2, commit: 4cea50c0c15c11a5b15f25223ff9e02324d212c5 agent.id 2d1c51c2-1a17-4ca6-b085-c7dea003a251 agent.type endpoint agent.version 8.2.2 data_stream.dataset endpoint.alerts data_stream.namespace default data_stream.type logs ecs.vers...

Hash: a2d546749333d57f7370f528e63ab3b688f72b2b33fb33bdbcab494efc766bd1

Let’s process our alerts!

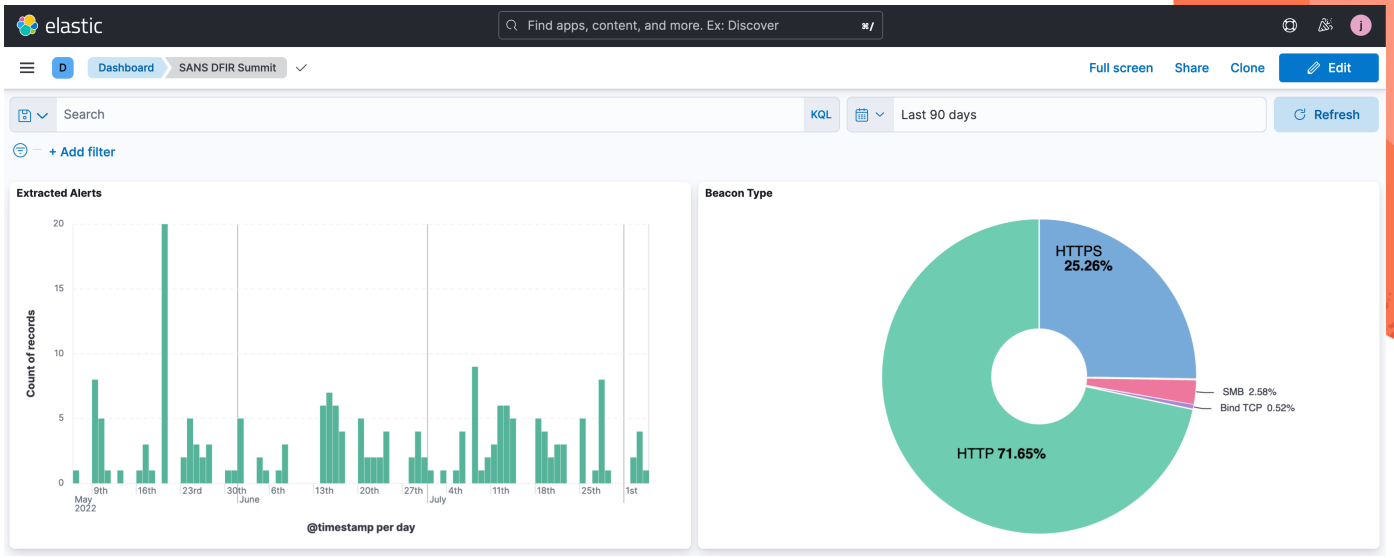
```
❯ docker exec malware-exquacker_malware-exquacker_1 poetry run malware-exquacker --since now-1d/d -v
```

Et voila ✨


elastic
Find apps, content, and more. Ex: Discover
Discover
Options
New
Open
Alerts
Share
Inspect
Save
malware-config-extractor
Filter your data using syntax
Aug 2, 2022 @ 21:08:40.819 → now
Refresh
Search field names
Filter by type 0
Selected fields 4
_index
@timestamp
threat.software.config.cobaltstrike.beacon_type
threat.software.config.family
Available fields 51
Popular
event.kind
process.args
threat.software.config.cobaltstrike.dns_beacon.dns_idle
threat.software.config.cobaltstrike.dns_beacon.dns_sleep
threat.software.config.cobaltstrike.dns_beacon.maxdns
threat.software.config.cobaltstrike.http.get.client.metadata
threat.software.config.cobaltstrike.http.post.client.headers
threat.software.config.cobaltstrike.pipename
Add a field
7 hits
Documents
Field statistics BETA
Aug 2, 2022 @ 21:08:40.819 - Aug 4, 2022 @ 16:03:27.984 (interval: Auto - hour)
Columns
1 field sorted
_index
@timestamp
threat.software.config.cobaltstrike.beacon_type
threat.software.config.family
malware-config-extractor Aug 4, 2022 @ 12:10:50.609 HTTP cobalt_strike
malware-config-extractor Aug 4, 2022 @ 11:23:36.992 HTTP cobalt_strike
malware-config-extractor Aug 3, 2022 @ 22:01:45.747 - phoreal
malware-config-extractor Aug 3, 2022 @ 13:46:23.651 HTTP cobalt_strike
malware-config-extractor Aug 3, 2022 @ 12:49:50.535 HTTP cobalt_strike
malware-config-extractor Aug 3, 2022 @ 12:38:36.448 HTTP cobalt_strike
malware-config-extractor Aug 3, 2022 @ 11:11:03.181 HTTP cobalt_strike

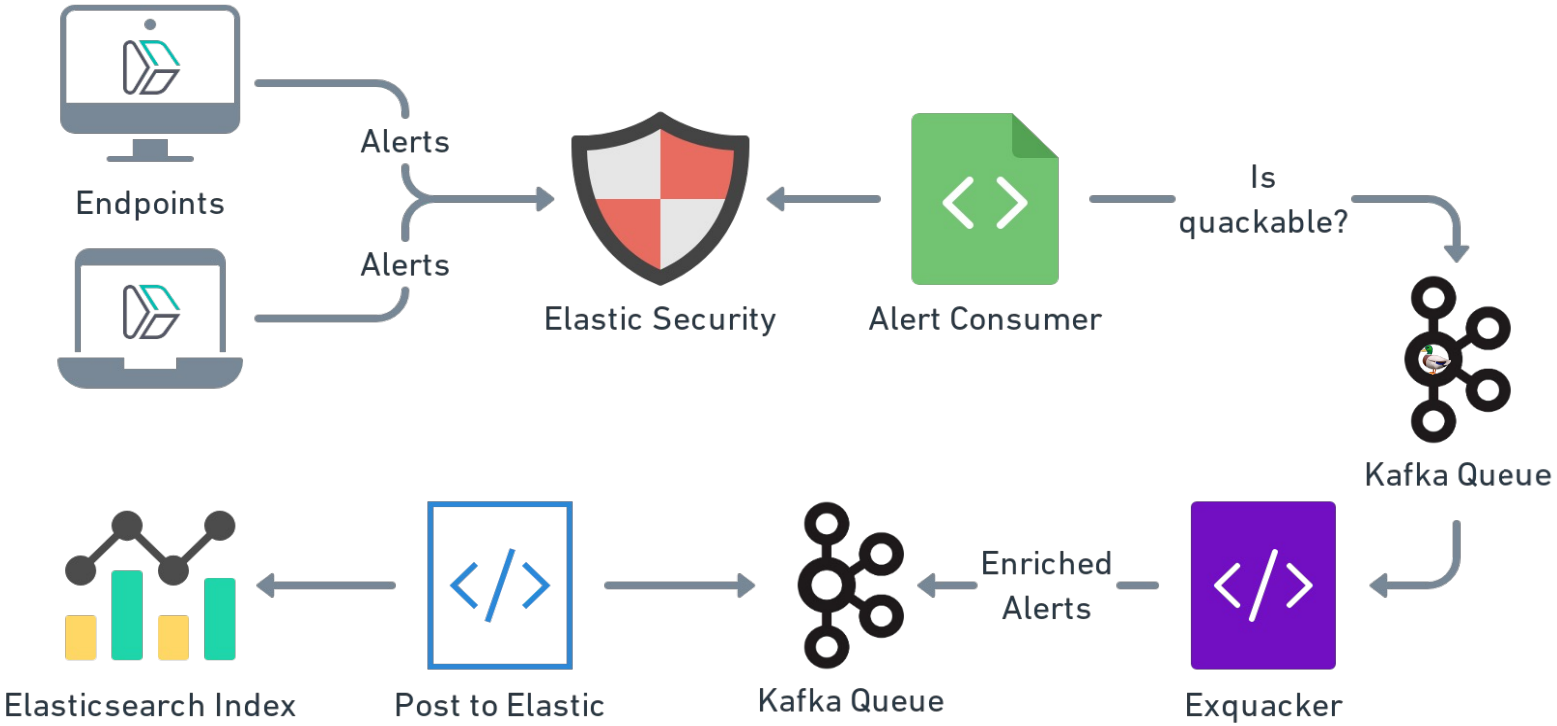
🦆 but what if we automated it?

- Currently running a daily batch job
- Looks back 1 day & loads the enhanced alerts into a new index



elastic

… but what if *always ran??*



Next Steps

Where is this project going next?

- Continue our automation journey
- Keep writing config extraction classes for different malware families
- Allow for additional modules with “KwakConf”
- Open source it!!!

elastic

Quacknowledgments 🦆

Thank you to:

- Security Protections
- Andrew Pease

elastic

Thanks for having us!

More info at our GitHub repo:
https://ela.st/sans-dfir-2022

@dcode

@jeska

elastic