



# INCIDENT RESPONSE FOR CHEAPZ

A “QUICK” JOURNEY THROUGH INCIDENT RESPONSE IN THE OPEN SOURCE  
WORLD...

Security  
Distractions

## A LITTLE ABOUT ME

- British but starting to feel more and more like a Dane...
  - Yeah yeah, one day I will speak Danish to you all...
- Lived in Denmark 4.5 years, with my wife and 2 kids..
- Incident Response Lead/SOC Lead/SOC Architect/CTI/Whatever else is needed...
- I love open source security solutions, I run the Security Distractions blog...
- I also maintain ElastiMISPStash alongside Dennis Lund Christensen...



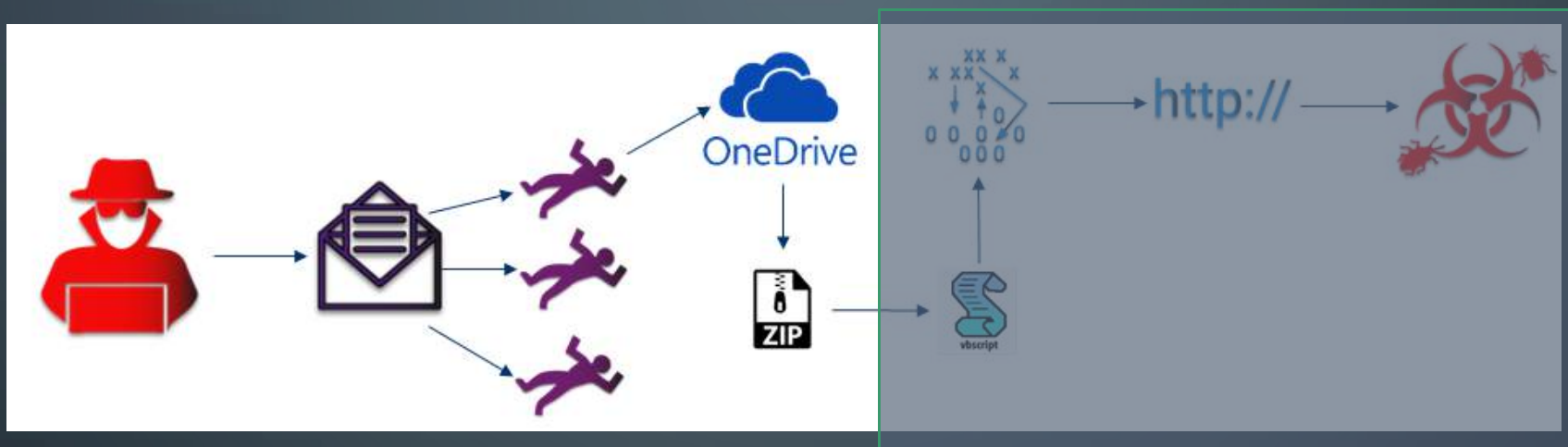
Security  
Distractions

# INTRODUCTION

Tonight we will talk about the following stuff:-

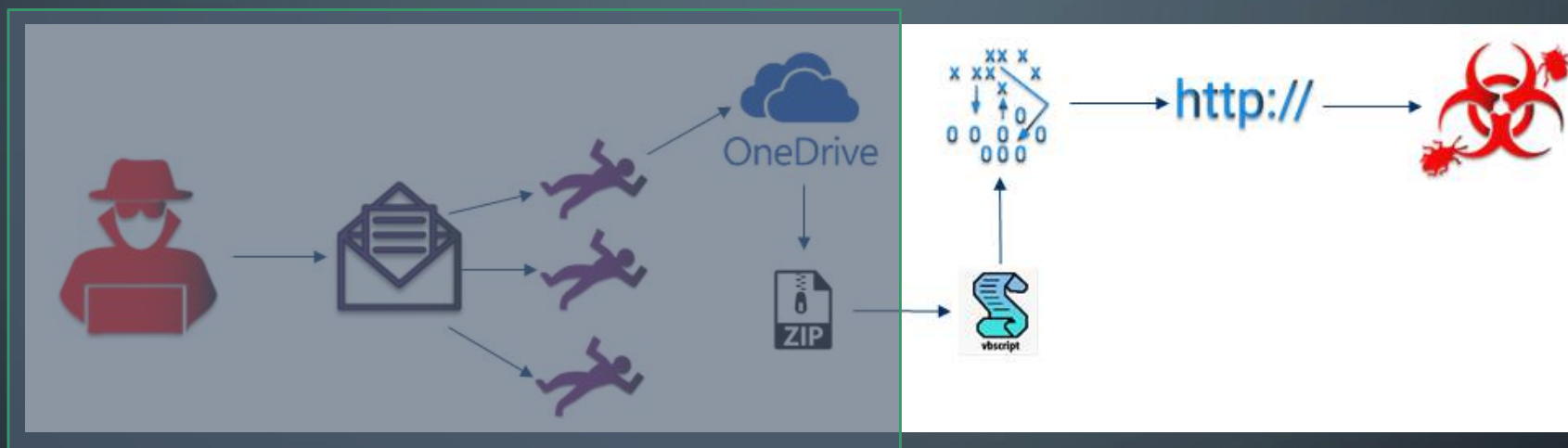
- Theory – Kill Chain, Courses of action, NIST IR model...
- Tools – MISP, ELK stack, ElastAlert, The Hive, elastimispstash...

## EXAMPLE - QBOT EARLY STAGES



A user receives a mail reply as part of a previous mail correspondence with a friend. The new reply has a OneDrive link inside, they click on the link which retrieves a ZIP file to their machine. They unzip the file and it contains a file with a double extension, helpguide.docx.vbs. The file is shown by Windows to be a docx, so the user opens the file.

## EXAMPLE – QBOT EARLY STAGES



The file was actually a VBS script, which when executed retrieved some information from WMI about the OS version, AV engine etc. It then attempted to retrieve, via BITS, second stage malware from 3 different domains, which all failed due to intelligence in the proxy filter.



### RECONNAISSANCE

Harvesting email addresses, conference information, etc.



### DELIVERY

Delivering weaponized bundle to the victim via email, web, USB, etc.



### INSTALLATION

Installing malware on the asset



### ACTIONS ON OBJECTIVES

With 'Hands on Keyboard' access, intruders accomplish their original goals



### WEAPONIZATION

Coupling exploit with backdoor into deliverable payload



### EXPLOITATION

Exploiting a vulnerability to execute code on victim's system



### COMMAND & CONTROL (C2)

Command channel for remote manipulation of victim

# KILL CHAIN MAPPING

**Recon** – Previous user mail compromise

**Weaponization** – Email

**Delivery** – Spearphishing link:  
[onedrive.com/file/1234](https://onedrive.com/file/1234)

**Exploitation** – User

**Installation** – Execution of docx.vbs:  
[helpguide.docx.vbs](https://helpguide.docx.vbs)

**C2** – VBS (WMI, BITS): [domain1.com](https://domain1.com),  
[domain2.com](https://domain2.com), [domain3.com](https://domain3.com)

**Actions on objectives** – Retrieve second stage malware: Hash

Security  
Distractions

SO WHATS NEXT??

Security  
Distractions

# COURSES OF ACTION

- Discover – You gained an indicator, go search your logs for history of it
- Detect – You gained an indicator, lets write a detection rule
- Deny – Creating a firewall block rule, proxy filter, AV hash filter etc
- Disrupt – Makes the event fail as it is occuring, example could be IPS
- Degrade – Slow down the intrusion in progress, could be via bandwidth throttling



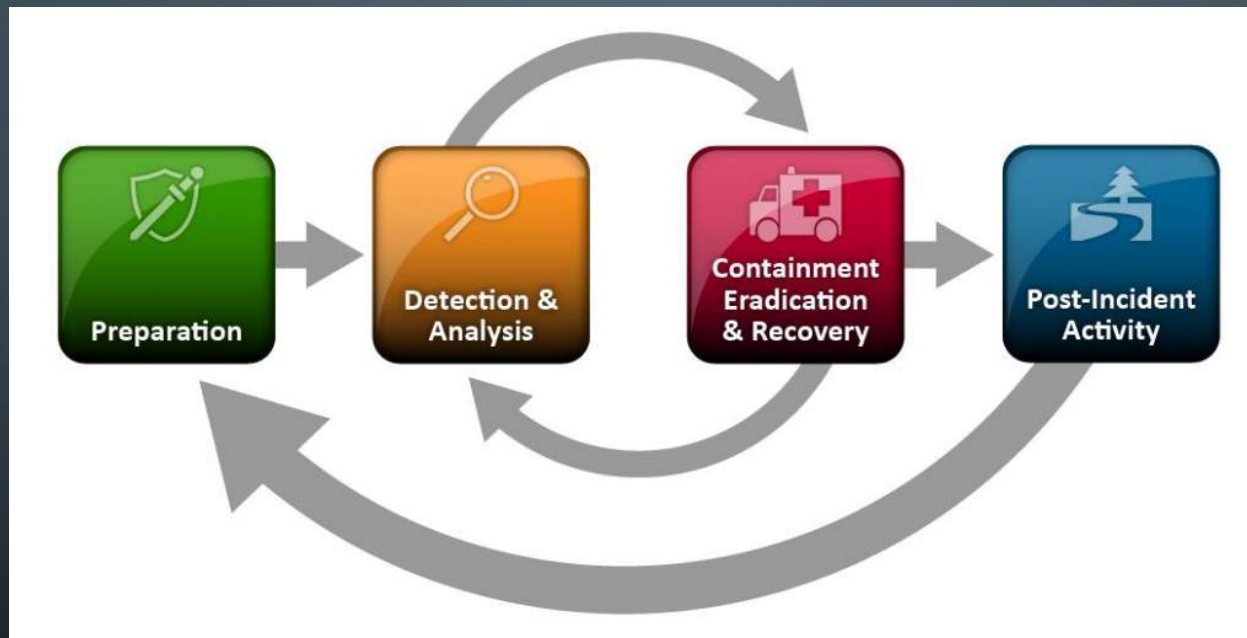
## COURSES OF ACTION – CONTINUED

- Deceive – Make the intruder think the attack is successful, forwarding traffic towards a honeypot
- Destroy – Offensive action against the intruder, arrest, physical destruction of property, hacking back (don't do this)....!

# COMBINING COA AND CYBER KILL CHAIN

	Discover	Detect	Deny
<b>Reconnaissance</b>	-	-	-
<b>Weaponization</b>	-	-	-
<b>Delivery</b> (onedrive.com/file/1234)	Mail gateway logs, proxy logs	Mail gateway logs, proxy logs	Mail gateway
<b>Exploitation</b> (User - Spearphishing)	-	-	User awareness
<b>Installation</b> (helpguide.docx.vbs)	Host logs	AV alerts, host logs	AV (hash of docx)
<b>C2</b> (domains)	Host logs, Proxy logs	Host logs, Intelligence alerts	Proxy filter, DNS Sinkholing
<b>Actions on objectives</b> (2 <sup>nd</sup> stage)	Proxy logs (domains)	AV alerts, host logs (hash)	AV (hash)

# NIST IR LIFECYCLE/MODEL/Framework/WHATEVER...



<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf>

Security  
Distractions

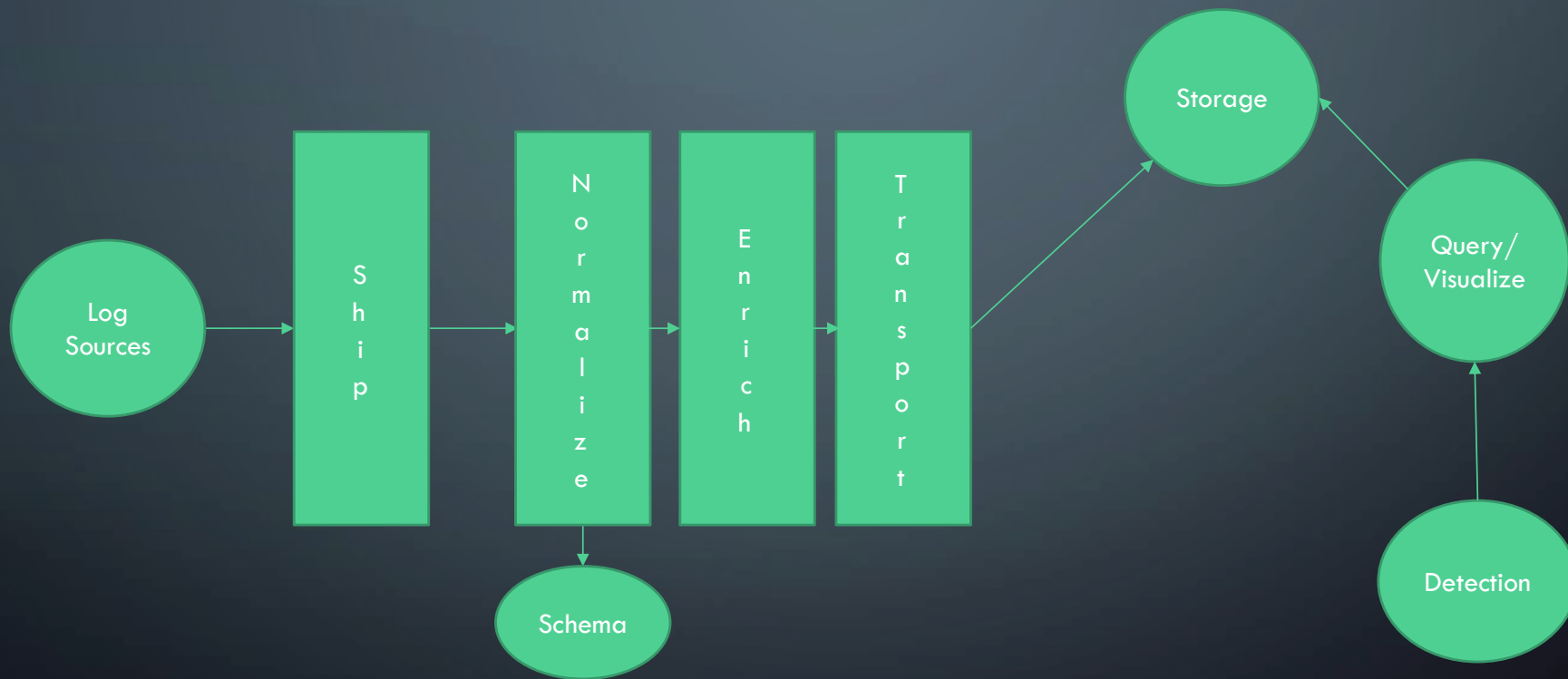
# DISCOVER AND PREPARATION

	Discover
<b>Reconnaissance</b>	-
<b>Weaponization</b>	-
<b>Delivery</b> (onedrive.com/file/1234)	Mail gateway logs, proxy logs
<b>Exploitation</b> (User - Spearphishing)	-
<b>Installation</b> (helpguide.docx.vbs)	Host logs
<b>C2</b> (domains)	Host logs, Proxy logs
<b>Actions on objectives</b> (2 <sup>nd</sup> stage)	Proxy logs (domains)



- We're probably going to need some logs.....

# LOGGING LOGGING LOGGING

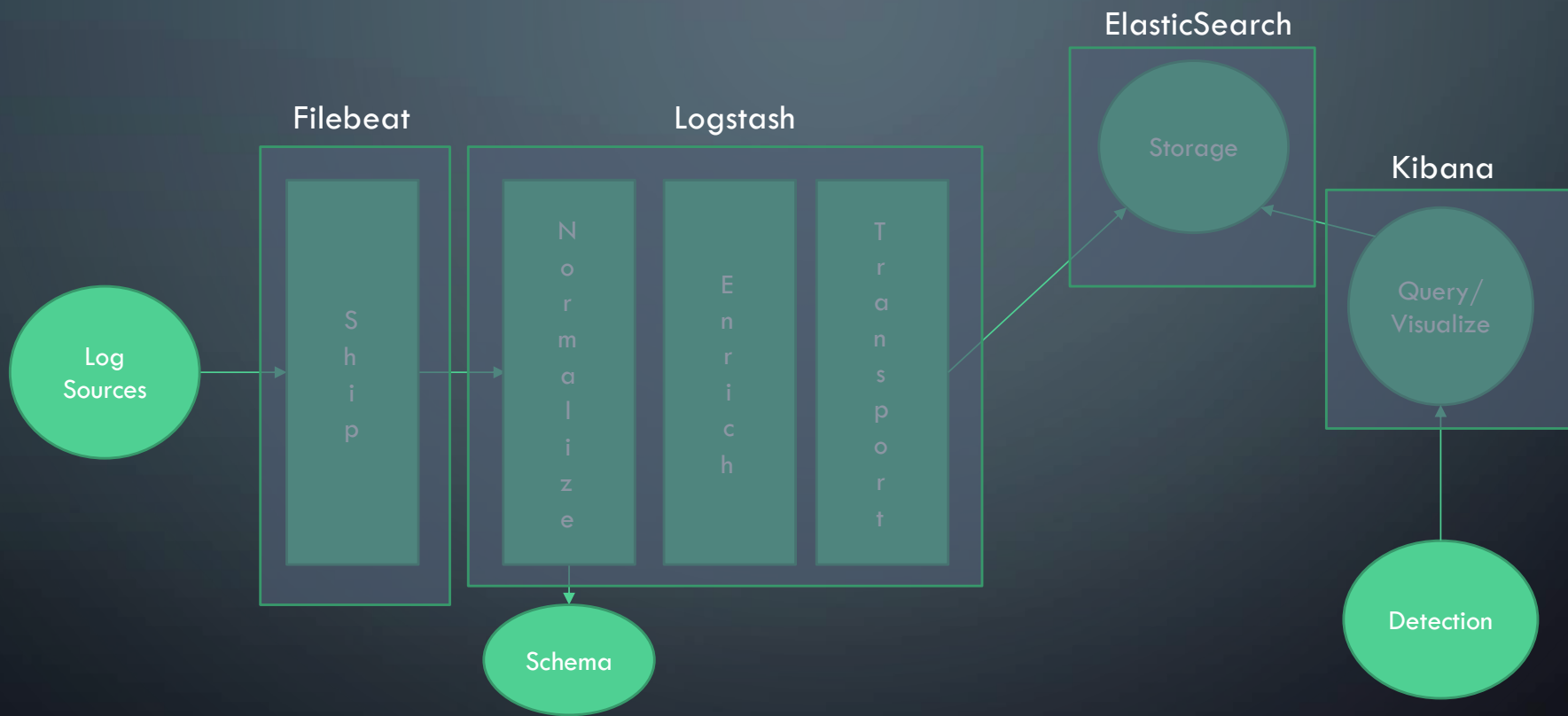


Security  
Distractions

# ELK STACK



- Made up of the following components:-
  - Filebeat – Log shipper
  - Logstash – Parsing logs, transforming and transporting them
  - Elasticsearch – Indexing and storing of data
  - Kibana – Displaying data from Elasticsearch and querying it
- Indexes on ingestion (sales sales sales)



Security  
Distractions

# DETECT AND DETECTION

	Detect
<b>Reconnaissance</b>	-
<b>Weaponization</b>	-
<b>Delivery</b> (onedrive.com/file/1234)	Mail gateway logs, proxy logs
<b>Exploitation</b> (User - Spearphishing)	-
<b>Installation</b> (helpguide.docx.vbs)	AV alerts, host logs
<b>C2</b> (domains)	Host logs, Intelligence alerts
<b>Actions on objectives</b> (2 <sup>nd</sup> stage)	AV alerts, host logs (hash)



- We're definitely going to need some logs.....
- Intelligence sharing...



# ELASTALERT



- Developed by YELP...
- Utilizes Elastic search API...
- Built in Python...
  - Rules are built in YAML...
- Modular rule design...
  - Monitor, Pattern, Alerter...

```
{  
  name: MISP-Alerter  
  type: any  
  index: sd-*  
  filter:  
    - query:  
      query_string:  
        query: "misp.tags: Feed-Alert"  
  
  alert: hivealerter"  
}
```

# ELASTALERT – EVEN MORE GOODNESS

- Plenty of Rule types
  - Any, Blacklist, Whitelist, Spike, etc etc
- Alerters
  - Slack, MS Teams, The Hive, HTTP POST, etc etc
- Sigma rule translator...
  - <https://github.com/Neo23x0/sigma/blob/master/contrib/sigma2elastalert.py>

# DENY AND CONTAINMENT

	Deny
<b>Reconnaissance</b>	-
<b>Weaponization</b>	-
<b>Delivery</b> (onedrive.com/file/1234)	Mail gateway
<b>Exploitation</b> (User - Spearphishing)	User awareness
<b>Installation</b> (helpguide.docx.vbs)	AV (hash of docx)
<b>C2</b> (domains)	Proxy filter, DNS Sinkholing
<b>Actions on objectives</b> (2 <sup>nd</sup> stage)	AV (hash)



- Security tools
  - Proxy, DNS sinkholing, AV
- User Awareness

# MISP – MALWARE INFORMATION SHARING PLATFORM



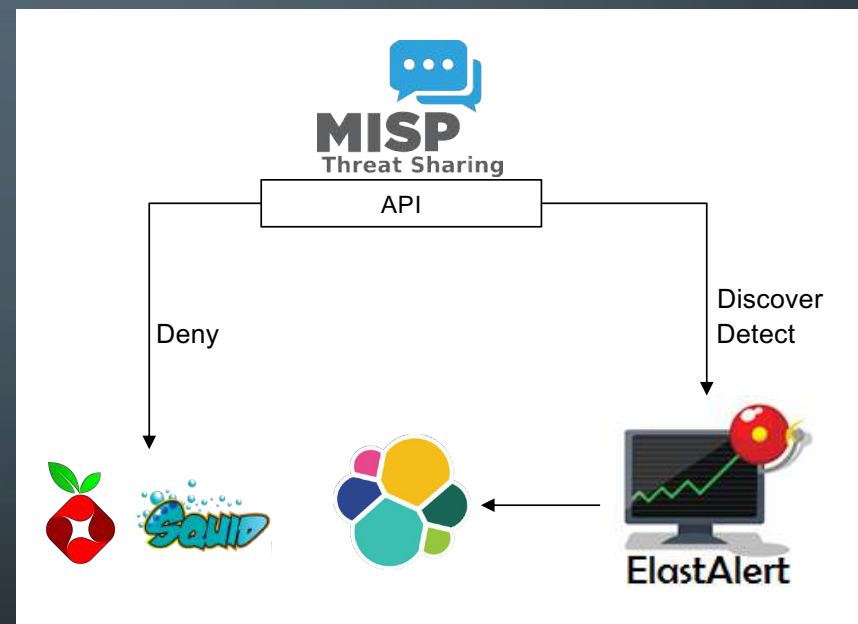
- Threat Intelligence Sharing Platform
  - Not just threat data!!
- Developed by CIRCL in Luxembourg
  - Originally a NATO project...
- MISP API
  - Used for automating lots of interesting things...

# MISP - EXAMPLE

<input type="checkbox"/>	Date ↑	Org	Category	Type	Value	Tags	Galaxies	Comment
<input type="checkbox"/>	2019-08-16		Payload installation	md5	321c3cf486ed509164edec1e1981fec8 🔍	<b>Feed-Discover</b> x 🌐+ 👤+	🌐+ 👤+	qbot 2nd stage
<input type="checkbox"/>	2019-08-16		Artifacts dropped	md5	7e641f6b9706d860baf09fe418b6cc87 🔍	<b>Feed-Deny</b> x 🌐+ 👤+	🌐+ 👤+	helpguide.docx.vbs
<input type="checkbox"/>	2019-08-16		Network activity	domain	domain1.com 🔍	<b>Feed-Alert</b> x 🌐+ 👤+	🌐+ 👤+	2nd stage retrieval domains
<input type="checkbox"/>	2019-08-16		Network activity	domain	domain2.com 🔍	<b>Feed-Alert</b> x 🌐+ 👤+	🌐+ 👤+	2nd stage retrieval domains
<input type="checkbox"/>	2019-08-16		Network activity	domain	domain3.com 🔍	<b>Feed-Alert</b> x 🌐+ 👤+	🌐+ 👤+	2nd stage retrieval domains

# MISP – COURSES OF ACTION...

- Feed-Discover
  - Go and out find this indicator in the entire log estate...
- Feed-Alert (Detect)
- Feed-Deny

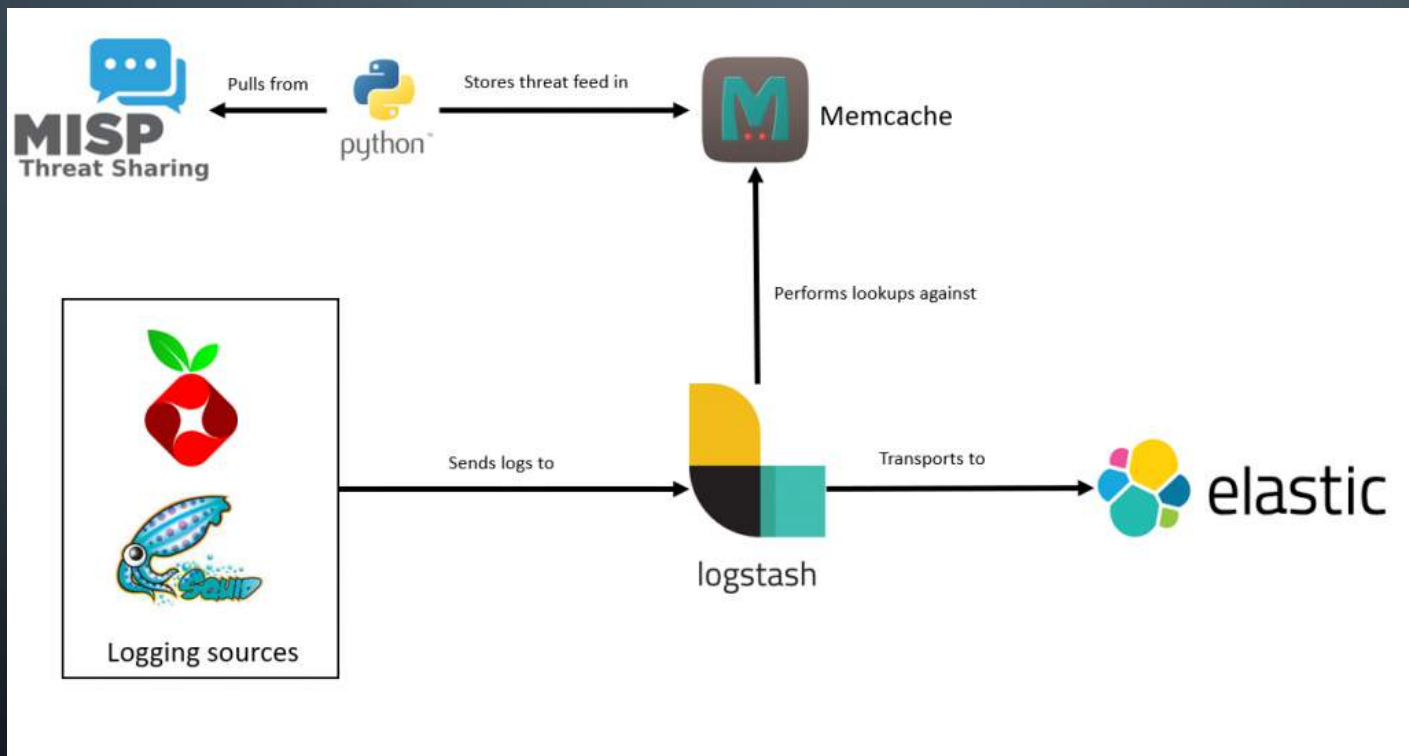


# ELASTIMISPSTASH

Some great security guys have written an integration between ELK and MISP...

- Enrichment on ingestion in real time...
- Highly scalable...
- Currently has support for ECS field types:-
  - Domain, ip and sha256

# ELASTIMISPSTASH





# WHAT DO WE NEED NEXT TIME?



- New indicators = New detections
- Does my current awareness training work?
- Do my security tools work?
- Do I have the correct logs?
- Is my log retention good enough?
- Am I receiving good intel?

A dark blue background with a light blue circuit board pattern consisting of lines and circles, primarily visible along the left and right edges.

WHOA WHOA WAIT... ONE LAST THING...  
WHERE DO THE ALERTS GO??

Security  
Distractions

## Alert Preview New

### H Alert - Empire Powershell Detected

[ID](#): b3428e699ddca180381e28aacabec3e0 [Date](#): Tue, Aug 27th, 2019 8:34 +02:00 [Type](#): Alert [Reference](#): 14a958 [Source](#): sd-squidproxy

[None](#)

#### Description

Possible Empire PowerShell has been detected, via common uri paths within the proxy logs, you can check your [Kibana dashboard](#) for more information.

#### Additional fields

*No additional information have been specified*

#### Observables (2)

All (2) hostname (1) domain (1)

Type	Data
hostname	iewin7[.]securitydistractions[.]net
domain	c2[.]0wasp[.]dk

Cancel

 Mark as read

 Ignore new updates

 Merge into case

Security  
Distractions

# THE HIVE



- Incident response case management tool...
- Works with the concept of "alerts" and "cases" and "observables".
- Observables (indicators) can be correlated based on:-
  - Previous cases...
  - Incoming alerts...
- You can map your playbooks in as case templates...

The background is a dark blue gradient. In the four corners, there are decorative white line-art patterns resembling circuit traces or neural network connections, with small circles at the end of the lines.

# DEMO – APT PERTO ON THE LOOSE

Security  
Distractions