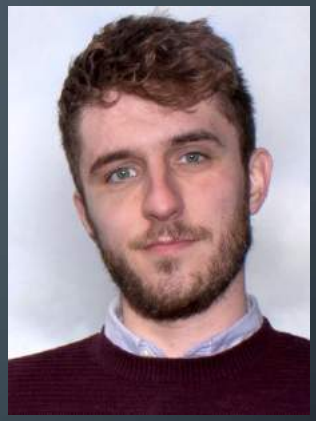
INCIDENT RESPONSE FOR CHEAPZ

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 Christiensen…

Security Distractions

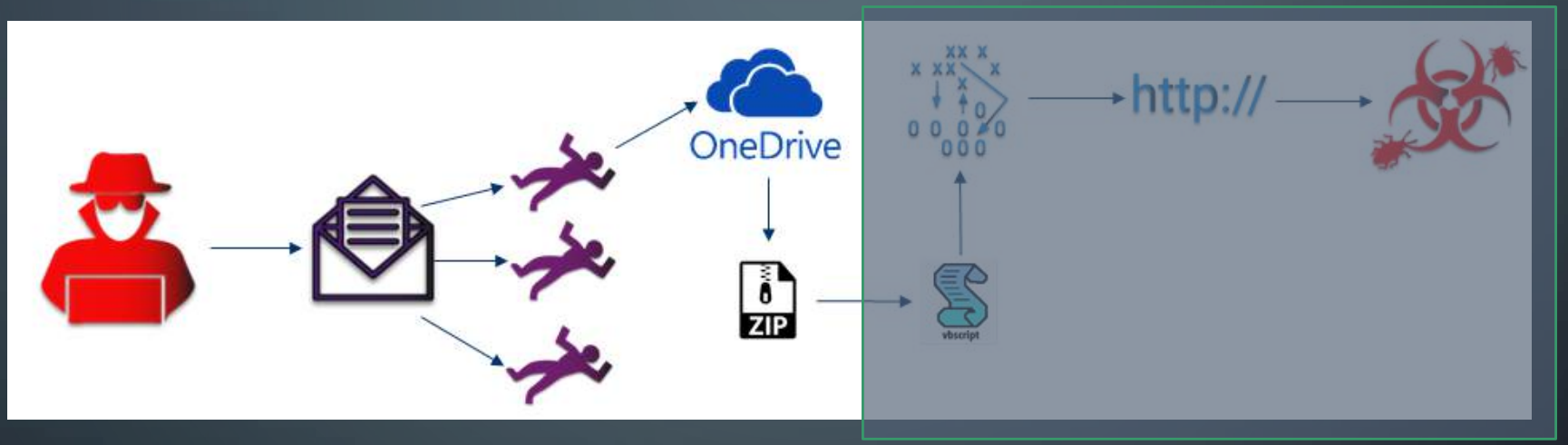
INTRODUCTION

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…

Security Distractions

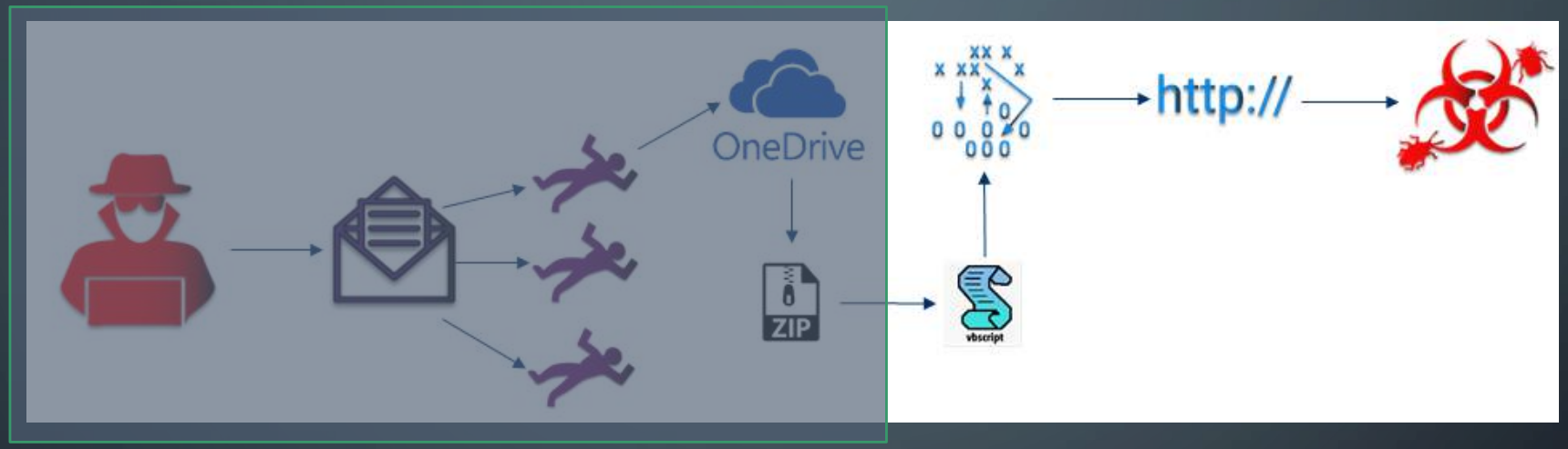
EXAMPLE - QBOT EARLY STAGES



A user recieves a mail reply as part of a previous mail correspondance 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.

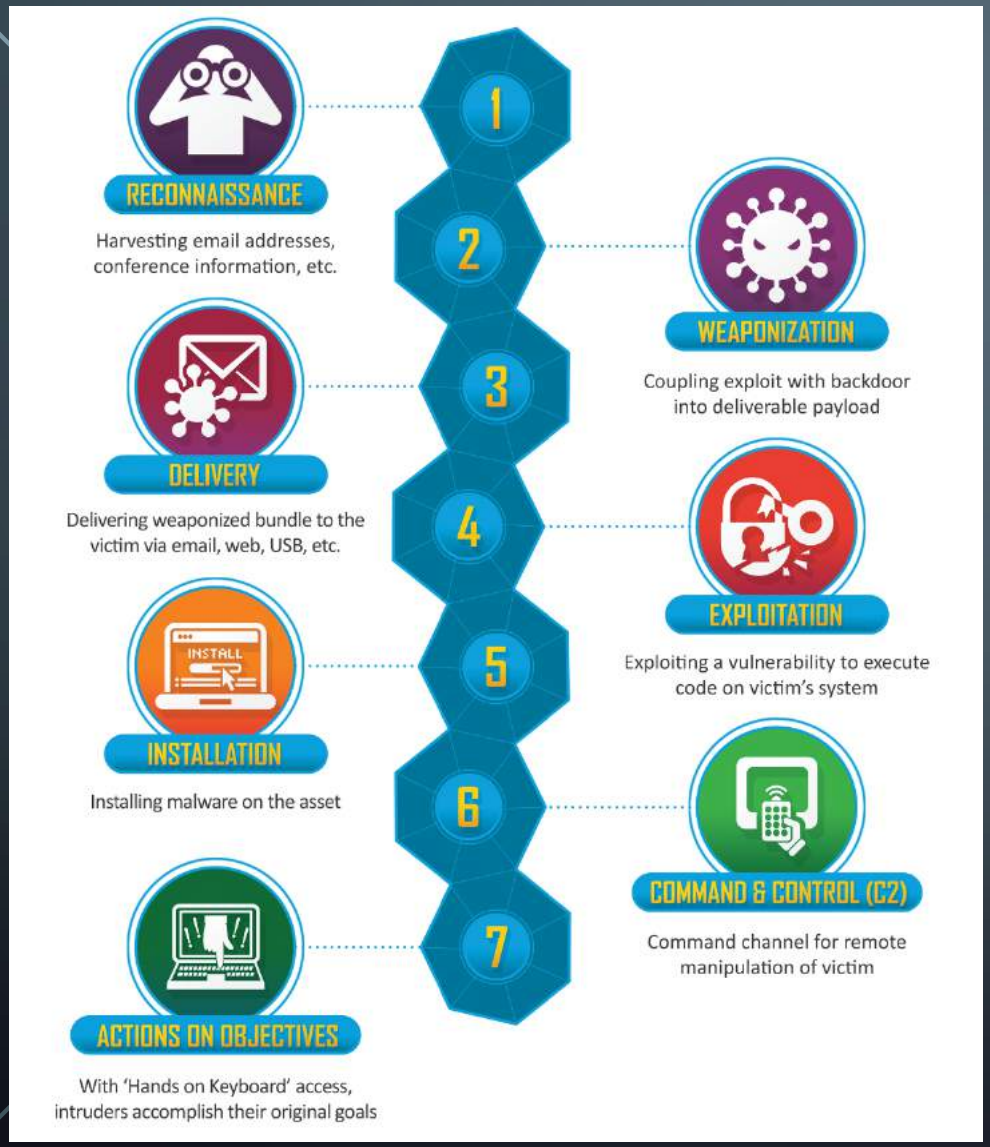
Security Distractions

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.

Security Distractions



KILL CHAIN MAPPING

Recon – Previous user mail compromise

Weaponization – Email

Delivery – Spearphishing link: onedrive.com/file/1234

Exploitation – User

Installation – Execution of docx.vbs: helpguide.docx.vbs

C2 – VBS (WMI, BITS): domain1.com, domain2.com, 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 bandwith throttling

Security Distractions

COURSES OF ACTION – CONTINUED

- Decieve – 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)….!

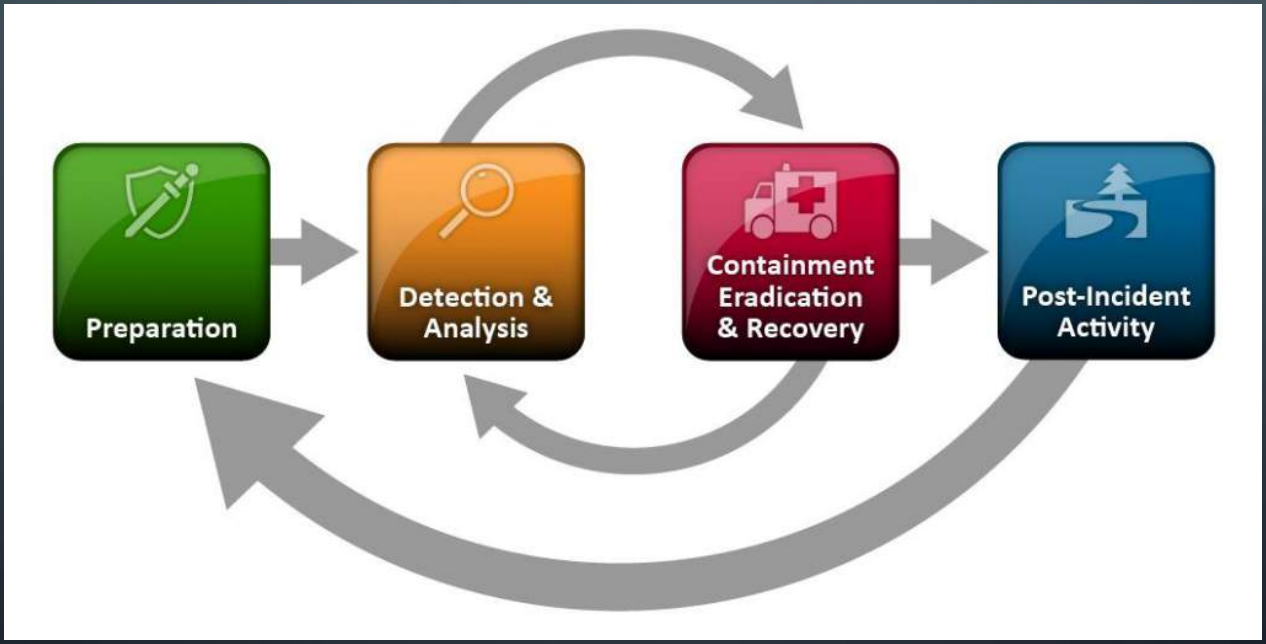
Security Distractions

COMBINING COA AND CYBER KILL CHAIN

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

Security Distractions

NIST IR LIFECYCLE/MODEL/FRAMEWORK/WHATEVER...



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

Security Distractions

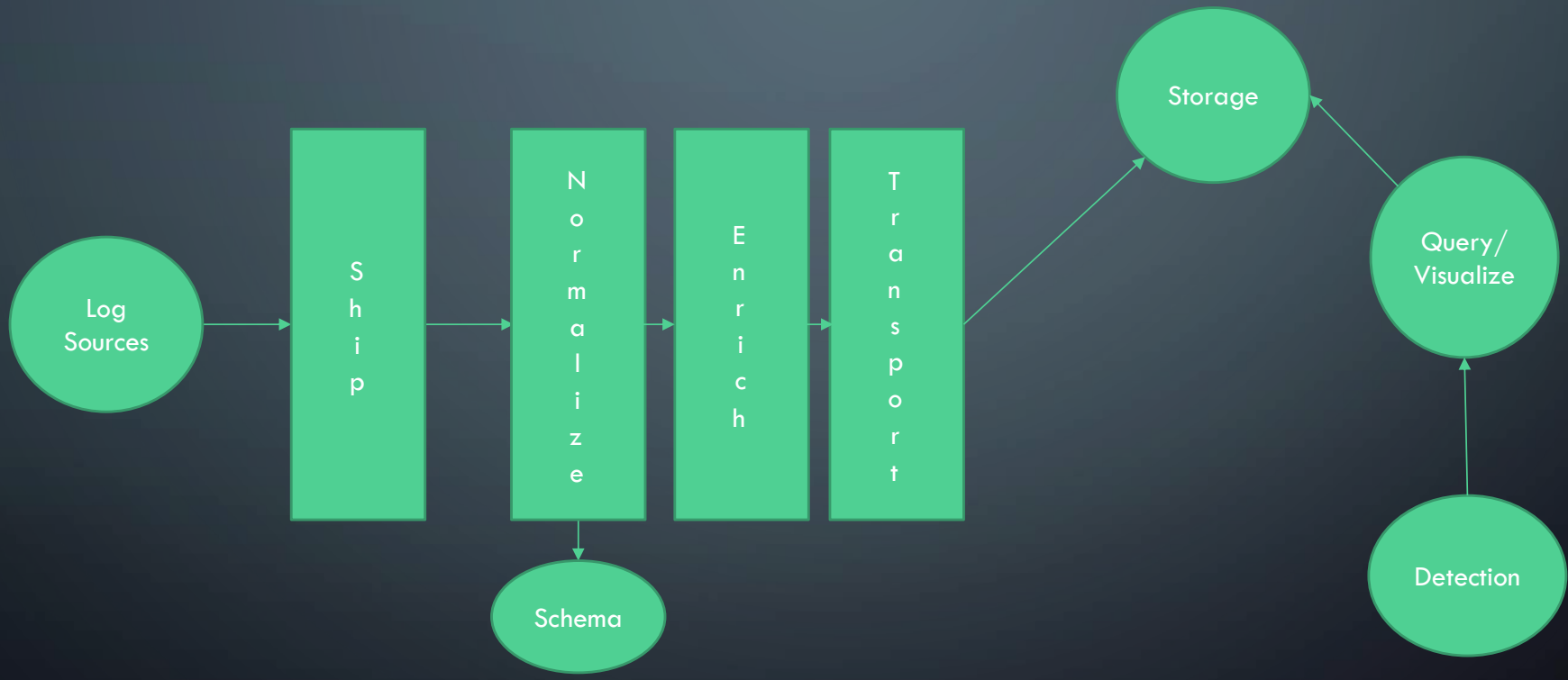
DISCOVER AND PREPARATION

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

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

Security Distractions

LOGGING LOGGING LOGGING

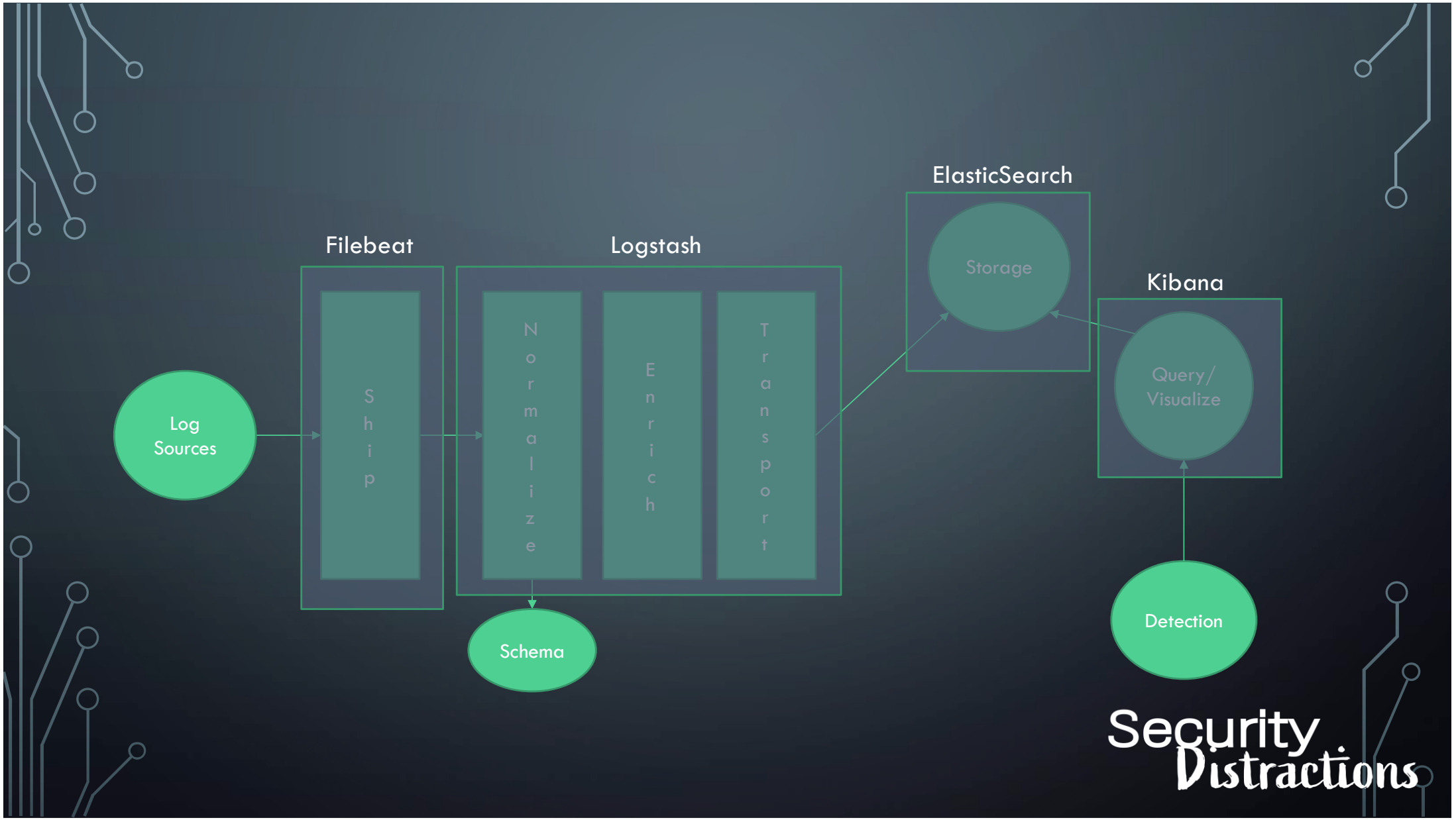


Security Distractions

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


ElasticSearch
Storage
Filebeat
Logstash
Kibana
Log Sources
Ship
Normalize
Enrich
Transport
Query / Visualize
Schema
Detection
Security Distractions

DETECT AND DETECTION

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

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

Security Distractions

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”
}
```

Security Distractions

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

Security Distractions

DENY AND CONTAINMENT

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

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

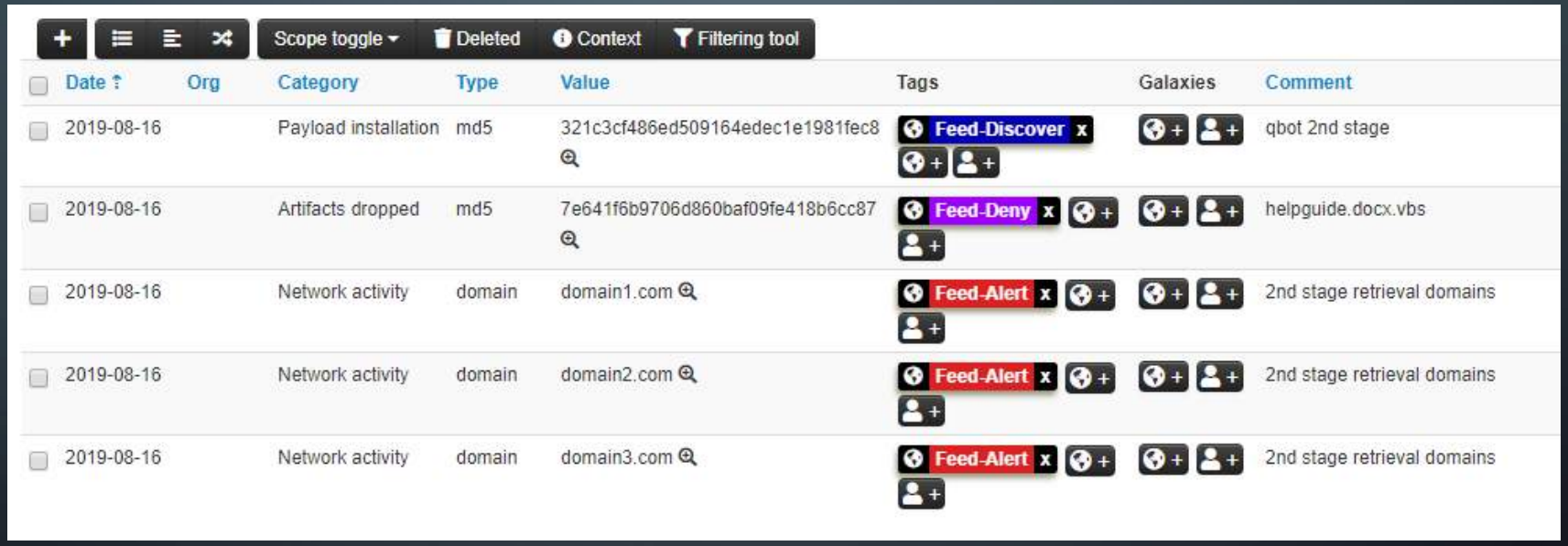
Security Distractions

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…

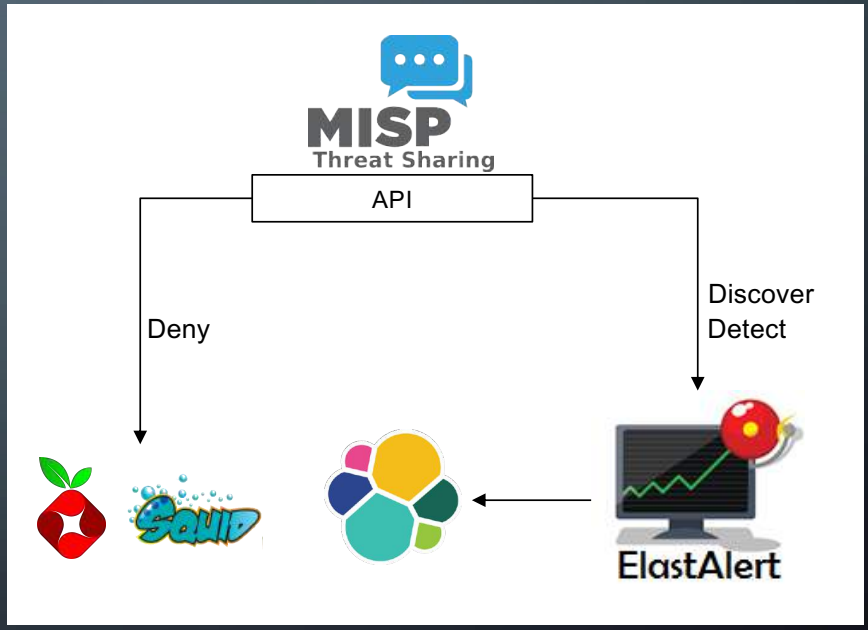
Security Distractions

MISP - EXAMPLE



MISP – COURSES OF ACTION…

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



Security Distractions

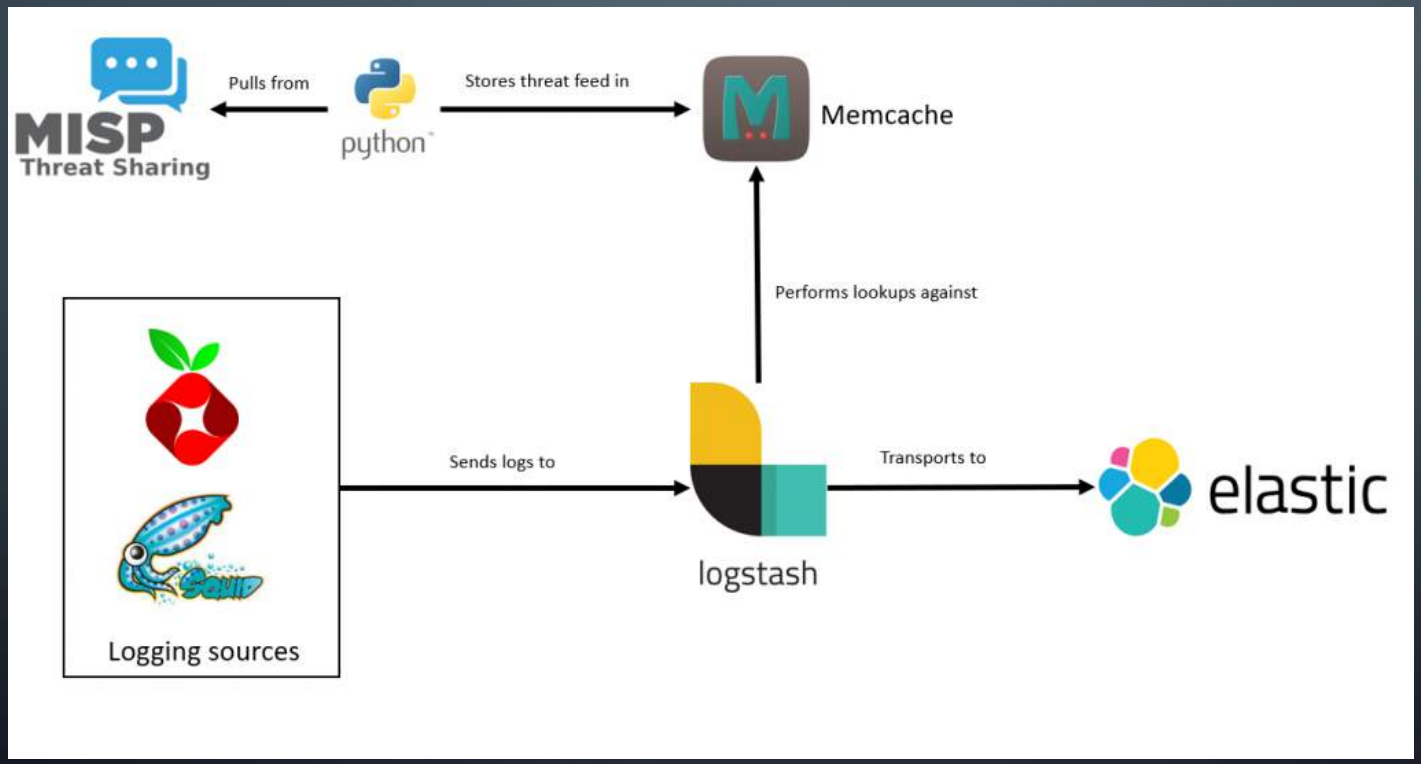
ELASTIMISPSTASH

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

Security Distractions

ELASTIMISPSTASH



Security Distractions

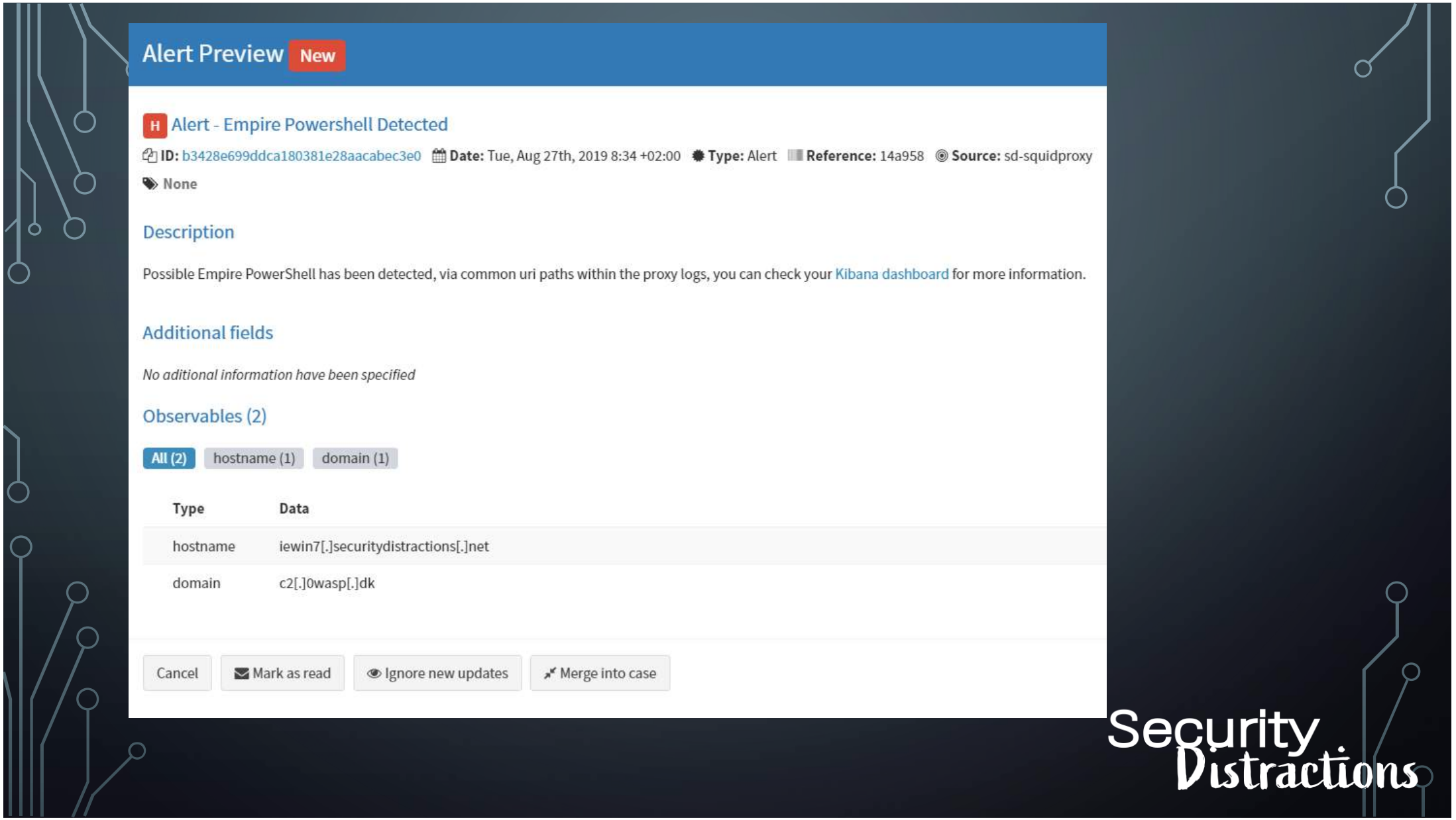
WHAT DO WE NEED NEXT TIME?

- 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?

Security Distractions

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

Security Distractions



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…

Security Distractions

DEMO – APT PERTO ON THE LOOSE

Security Distractions