Historic Overview of Threat Hunting

The Victory of Allied troops against Hitler's Army at World War II

Strategies

- Improved detection equipment to avoid moment of surprise.
- Improved offensive weapons to shoot down the bombers and sub-marines
- Improved training for the hunters.
- Decrypted the coded messages.

Source – Encyclopedia Britannica

People, Process and Technology

Leverage Open Source Technology to build your SOC

A. S. M. Shamim Reza

Link3 Technologies Limited

2021 APRICOT APNIC 51

Agenda

“ What to do, to build a SOC?

“ What not to do, to build a SOC?

What is a SOC?

> A **SOC** (*Security Operations Center*) is a team primarily composed of security analysts organized to detect, analyze, respond to, report on, and prevent Cybersecurity incidents.
>
> – Carson Zimmerman, MITRE

People

Threat Hunter
SOC Analyst
Forensic Investigator
Incident Responder

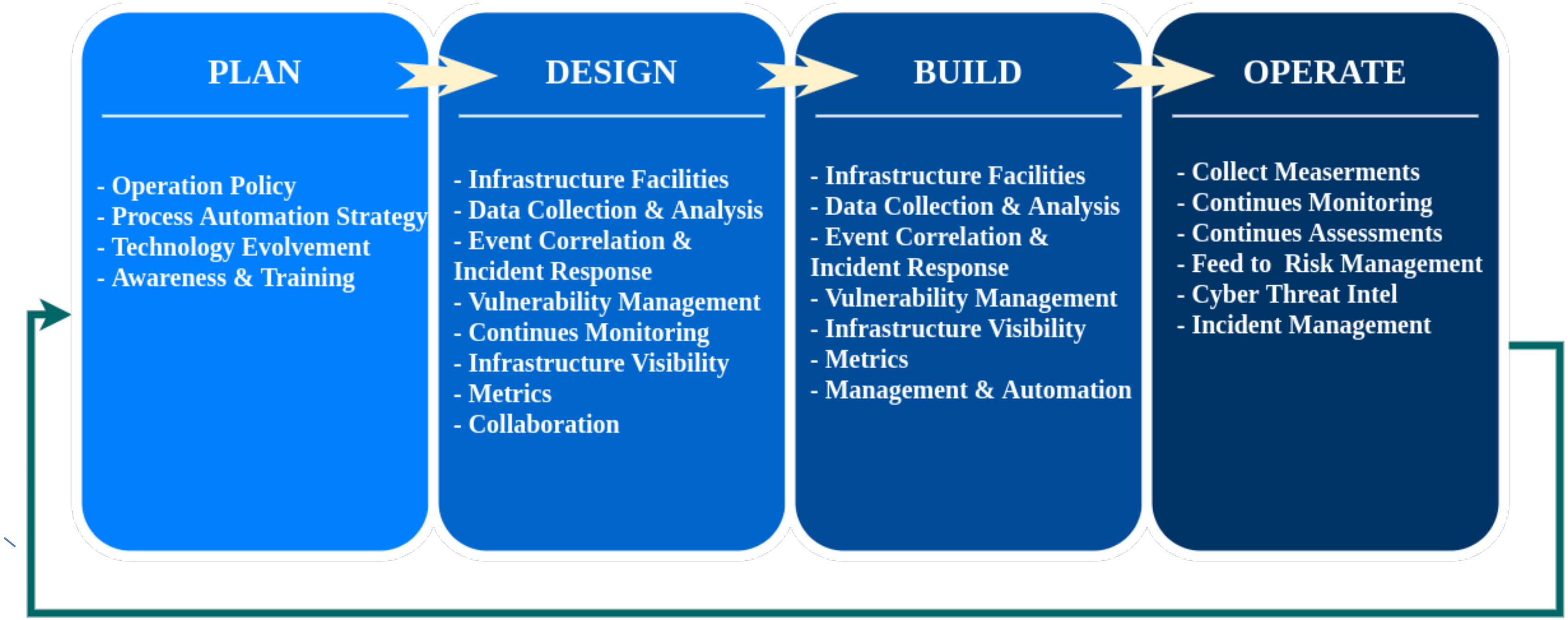
Process

Governance
Workflows
Best Practice

Technology

Data collection
Correlation
Monitoring
Threat Intelligence
Forensic Analysis
Incidence Response

Strategic move to Build a SOC



PLAN

- Operation Policy
- Process Automation Strategy
- Technology Evolvement
- Awareness & Training

DESIGN

- Infrastructure Facilities
- Data Collection & Analysis
- Event Correlation & Incident Response
- Vulnerability Management
- Continues Monitoring
- Infrastructure Visibility
- Metrics
- Collaboration

BUILD

- Infrastructure Facilities
- Data Collection & Analysis
- Event Correlation & Incident Response
- Vulnerability Management
- Infrastructure Visibility
- Metrics
- Management & Automation

OPERATE

- Collect Measerments
- Continues Monitoring
- Continues Assessments
- Feed to Risk Management
- Cyber Threat Intel
- Incident Management

Strategic move to Build a SOC – Plan

- Concerned about Cost.
- Define the use cases.
- Choosing the ***best fitted*** Open Source project; ***not the best one***.
- Scalability of the SOC infrastructure.

- Define the Operations policy.
- Categorizes the Awareness & Training phase.
- Define the Single Source of Truth.

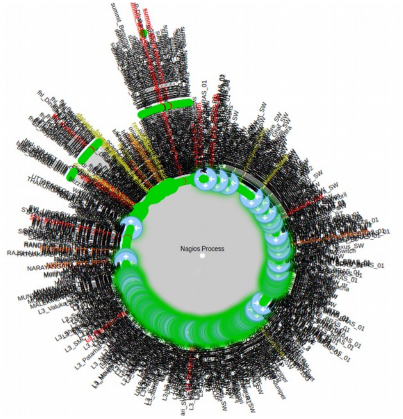
Strategic move to Build a SOC – Plan

- Zero trust policy on employee devices.
- Ensure the authority to do the job of SOC.
- A wiki portal to store –
  - SIEM monitoring and Notification (email, mobile, chat, etc.) procedure.
  - Event management process.
  - Security Incident Ticket management process .
  - Incident Handling, Reporting and Escalation process.
  - Daily activities process like checklist and handover.
  - Compliance monitoring process.
  - Daily, weekly and monthly report format to Management.

Strategic move to Build a SOC – Design

What we had in place, before thinking about the SOC!

- Event and Metric based monitoring system.
  - Run-time alerts
  - Daily, Weekly and Monthly auto-generated report
  - Time-series performance metrics
- Central syslog analytics platform.
  - Incident analysis
- Machine Learning based Threat Hunting into NetFlow data.
  - Pattern analysis
  - Human behavior analysis
- NIST framework to maintain regulatory compliance
- CIS benchmark to assess OS and service configuration security.



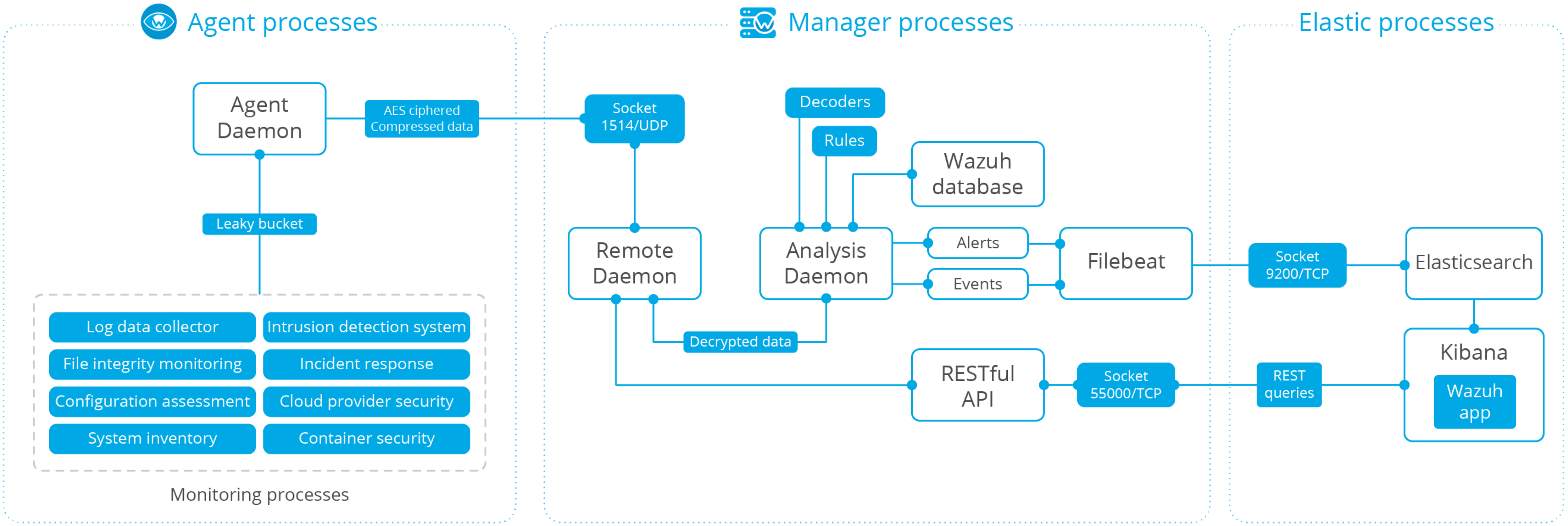
Strategic move to Build a SOC – Design *The Technology*

Service ?	Platform ?	Others?
• Intrusion Detection • File Integrity Monitoring • Vulnerability Detection • Configuration Assessments • Regulatory Compliance • Threat Intelligence • DNS Metrics • Network Traffic • Honeypot • Packet-capture • Incidence Response	• Docker-Container Based • Private Git-repository • Private Docker-Hub • System Management • Isolated LAB	• Identity & Access Management • Documentation • Backup • Private Communication Channel

Strategic move to Build a SOC – Build

The Technology

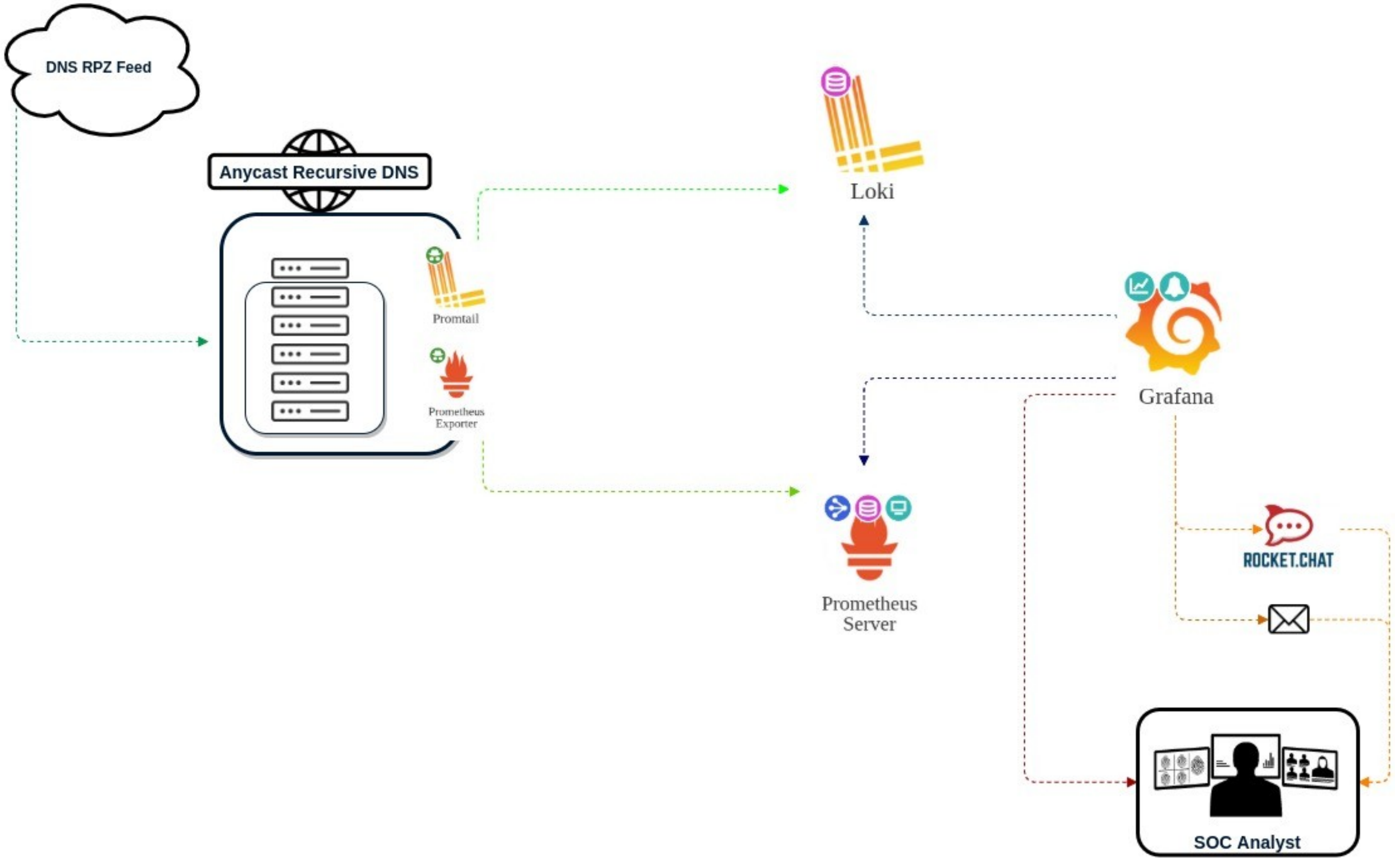
The SIEM platform



Strategic move to Build a SOC – Build

The Technology

The DNS Analytics



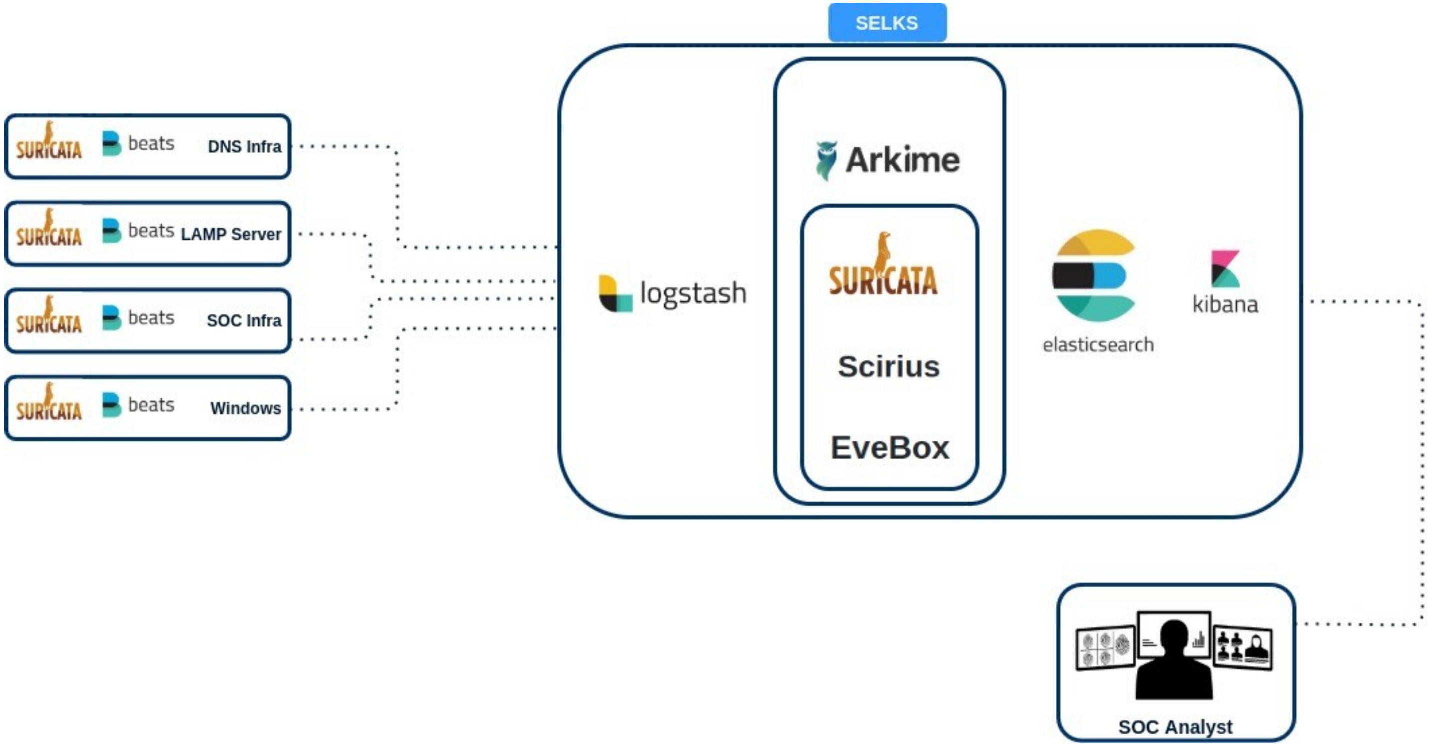
– ***Promtail*** is exporting the ***RPZ log*** to ***Loki*** server.

– ***Prometheus-exporter*** is exporting ***DNS metrics*** to the ***Prometheus*** server.

– ***Grafana*** visualizes the metrics and log data, and send alerts to ***rocket.chat*** and in ***email***.

Strategic move to Build a SOC – Build *The Technology*

The NIDS



– ***Suricata IDS*** is exporting the log with ***FileBeats*** to ***logstash.***

– The ***Suricata IDS*** event is stored at ***EveBox*** with ***Elasticsearch,***

– ***Scirius*** is managing ***Suricata*** rules

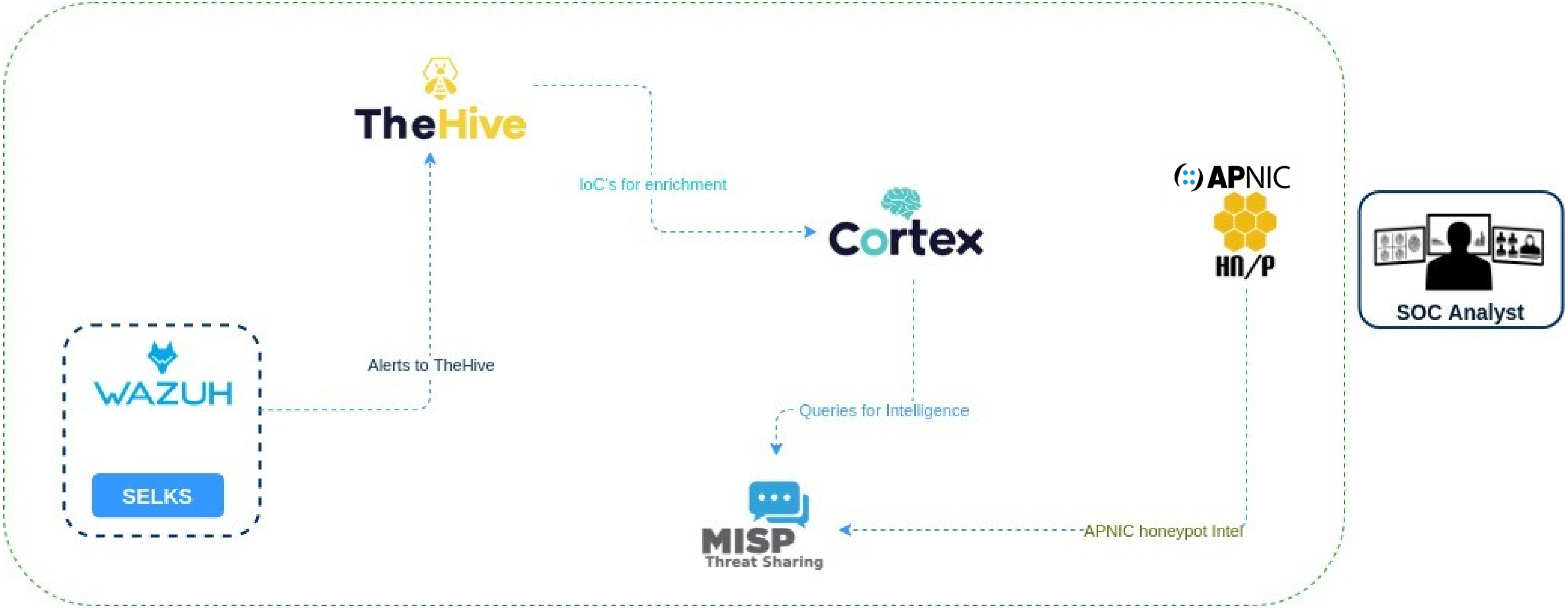
– ***Arkime*** (former *Moloch*) is working with the ***Packet-Capture.***

– The Platform is Custom build of ***SELKS*** distribution.

***** 90% of it has been shifted to Grafana Ecosystem*

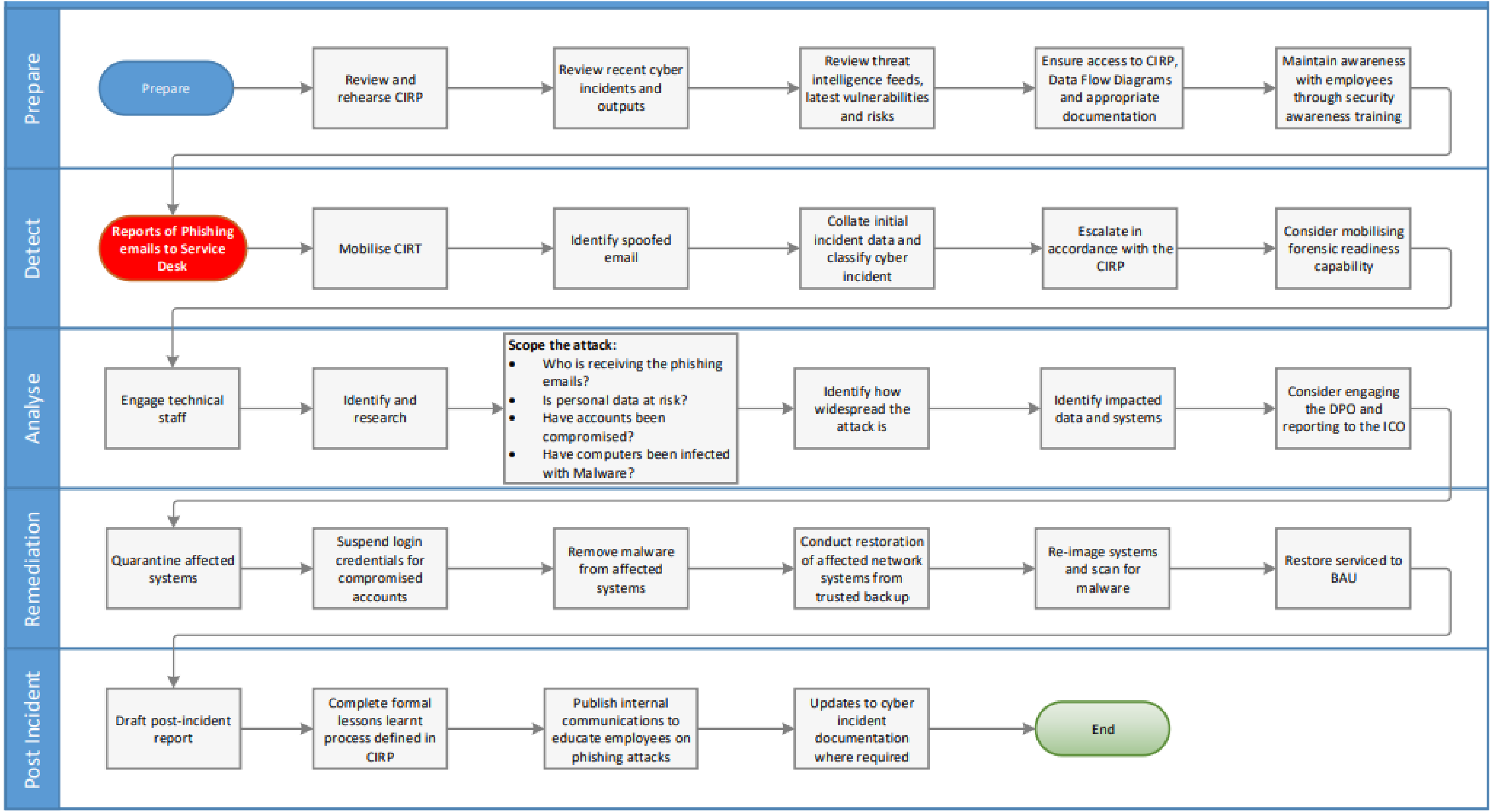
Strategic move to Build a SOC – Build *The Technology*

The Threat Intel



Strategic move to Build a SOC – Operate *Process*

Incidence Response – *Phishing Attack*



Prepare

Prepare

Review and rehearse CIRP

Review recent cyber incidents and outputs

Review threat intelligence feeds, latest vulnerabilities and risks

Ensure access to CIRP, Data Flow Diagrams and appropriate documentation

Maintain awareness with employees through security awareness training

Detect

Reports of Phishing emails to Service Desk

Mobilise CIRT

Identify spoofed email

Collate initial incident data and classify cyber incident

Escalate in accordance with the CIRP

Consider mobilising forensic readiness capability

Analyse

Engage technical staff

Identify and research

Scope the attack:

- Who is receiving the phishing emails?
- Is personal data at risk?
- Have accounts been compromised?
- Have computers been infected with Malware?

Identify how widespread the attack is

Identify impacted data and systems

Consider engaging the DPO and reporting to the ICO

Remediation

Quarantine affected systems

Suspend login credentials for compromised accounts

Remove malware from affected systems

Conduct restoration of affected network systems from trusted backup

Re-image systems and scan for malware

Restore serviced to BAU

Post Incident

Draft post-incident report

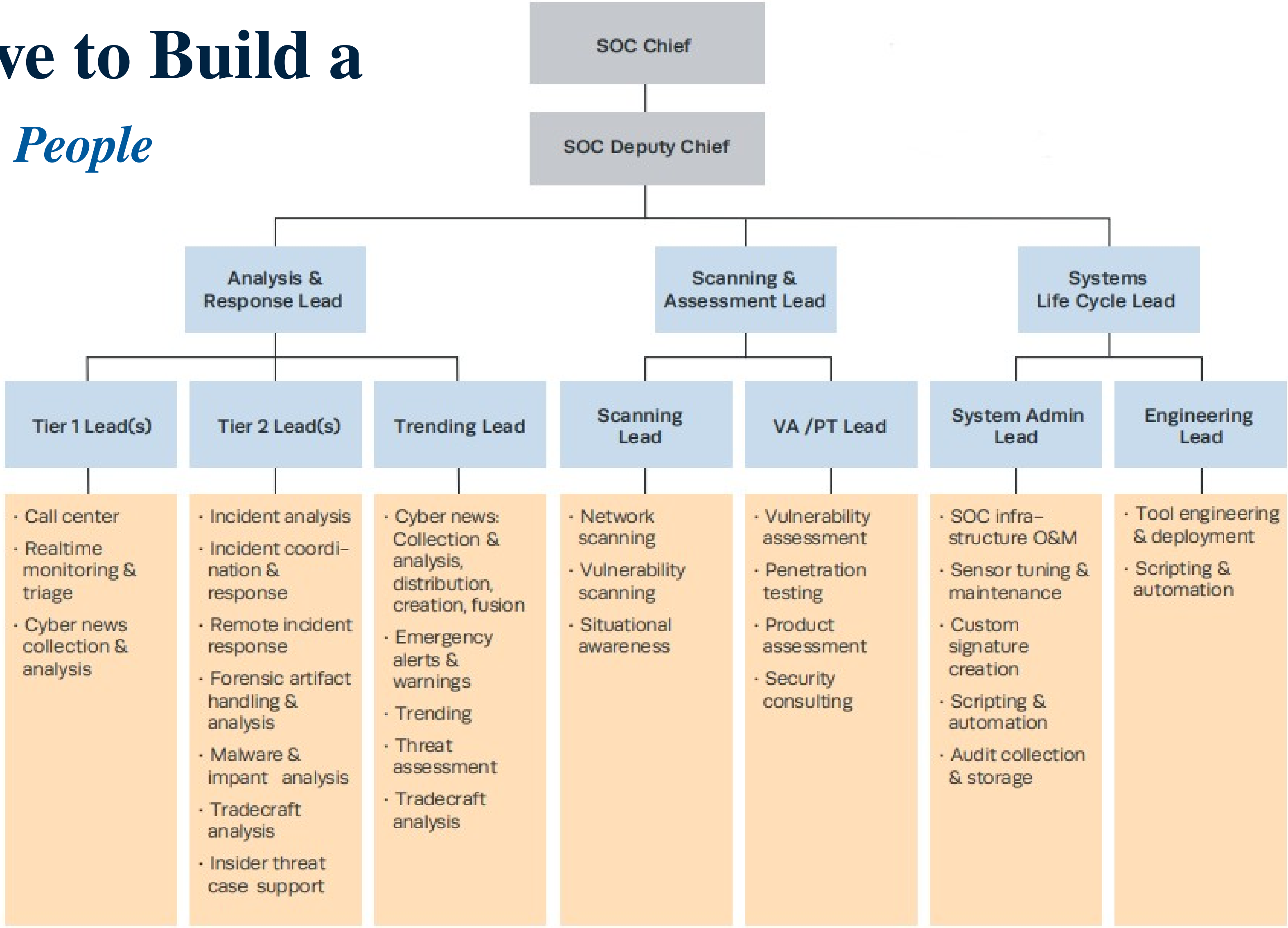
Complete formal lessons learnt process defined in CIRP

Publish internal communications to educate employees on phishing attacks

Updates to cyber incident documentation where required

End

Strategic move to Build a SOC – Operate *People*



SOC Chief

SOC Deputy Chief

Analysis & Response Lead

Scanning & Assessment Lead

Systems Life Cycle Lead

Tier 1 Lead(s)

- Call center
- Realtime monitoring & triage
- Cyber news collection & analysis

Tier 2 Lead(s)

- Incident analysis
- Incident coordination & response
- Remote incident response
- Forensic artifact handling & analysis
- Malware & impant analysis
- Tradecraft analysis
- Insider threat case support

Trending Lead

- Cyber news: Collection & analysis, distribution, creation, fusion
- Emergency alerts & warnings
- Trending
- Threat assessment
- Tradecraft analysis

Scanning Lead

- Network scanning
- Vulnerability scanning
- Situational awareness

VA /PT Lead

- Vulnerability assessment
- Penetration testing
- Product assessment
- Security consulting

System Admin Lead

- SOC infra-structure O&M
- Sensor tuning & maintenance
- Custom signature creation
- Scripting & automation
- Audit collection & storage

Engineering Lead

- Tool engineering & deployment
- Scripting & automation

*There is **no** replacement for the human analyst.*

Let’s talk Cases

Let’s talk cases!!

DGA – *Domain Generation Algorithm*

1st day, Got spike on “***Classification: Potentially Bad Traffic***” at IDS Platform.

DNS Query Log to check further –

```
11-Jan-2021 08:14:07.446 client 172.2.2.2 55823 (m21.wbputkk.cc): query: m21.wbputkk.cc IN A + (192.1.1.1)
11-Jan-2021 08:14:07.446 client 172.2.2.2 51934 (m15.harsnic.biz): query: m15.harsnic.biz IN A + (192.1.1.1)
11-Jan-2021 08:14:07.517 client 172.2.2.2 61810 (m36.oeudkwu.biz): query: m36.oeudkwu.biz IN A + (192.1.1.1)
11-Jan-2021 08:14:07.520 client 172.2.2.2 53623 (m38.jiawiqf.biz): query: m38.jiawiqf.biz IN A + (192.1.1.1)
11-Jan-2021 08:14:07.606 client 172.2.2.2 50235 (m37.klrfyid.cc): query: m37.klrfyid.cc IN A + (192.1.1.1)
11-Jan-2021 08:14:07.606 client 172.2.2.2 63923 (m16.zngcyck.cc): query: m16.zngcyck.cc IN A + (192.1.1.1)
11-Jan-2021 08:14:07.726 client 172.2.2.2 56077 (m31.yefjpws.biz): query: m31.yefjpws.biz IN A + (192.1.1.1)
11-Jan-2021 08:14:07.726 client 172.2.2.2 58133 (m7.lfkjkqh.cc): query: m7.lfkjkqh.cc IN A + (192.1.1.1)
11-Jan-2021 08:14:07.815 client 172.2.2.2 50647 (m23.nflotan.cc): query: m23.nflotan.cc IN A + (192.1.1.1)
```

** IP of DNS server and User has been faked here.

Let’s talk cases!!

DGA *(Issues that were raised)*

Two Issues are here –

- Never thought of configuring the ***Anycast DNS infra*** to store ***Passive-DNS info***.
    - Had to rely on ***Netflow*** data to find the ***covert channel.***
- The client is located in a remote place.
    - Managing a support personnel is tough, due to the ***Covid-19 situation.***

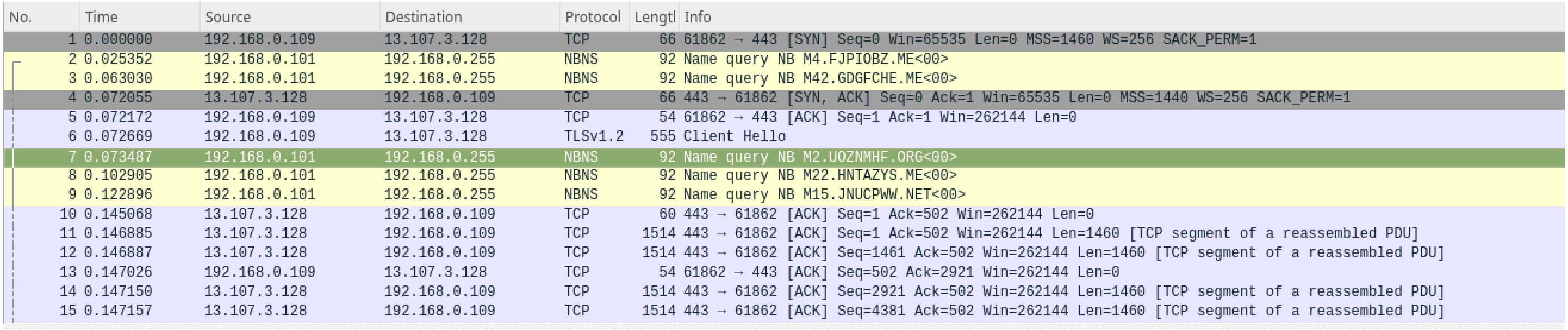
Let’s talk cases!!

DGA *(Packet Capture)*

Capturing packet was necessary, cause –

- Need to know the exact nature of the attack.
- Incompetence of Client IT Concern's to deal with IT security
- Need to assist the concern, as a service provider
- Provide some recommendation, not to repeat the issue

Anomalous Net-BIOS Activity



No.	Time	Source	Destination	Protocol	Lengtl	Info
1	0.000000	192.168.0.109	13.107.3.128	TCP	66	61862 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
2	0.025352	192.168.0.101	192.168.0.255	NBNS	92	Name query NB M4.FJPIOBZ.ME<00>
3	0.063030	192.168.0.101	192.168.0.255	NBNS	92	Name query NB M42.GDGFCHE.ME<00>
4	0.072055	13.107.3.128	192.168.0.109	TCP	66	443 → 61862 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM=1
5	0.072172	192.168.0.109	13.107.3.128	TCP	54	61862 → 443 [ACK] Seq=1 Ack=1 Win=262144 Len=0
6	0.072669	192.168.0.109	13.107.3.128	TLSv1.2	555	Client Hello
7	0.073487	192.168.0.101	192.168.0.255	NBNS	92	Name query NB M2.UOZNMHF.ORG<00>
8	0.102905	192.168.0.101	192.168.0.255	NBNS	92	Name query NB M22.HNTAZYS.ME<00>
9	0.122896	192.168.0.101	192.168.0.255	NBNS	92	Name query NB M15.JNUCPWW.NET<00>
10	0.145068	13.107.3.128	192.168.0.109	TCP	60	443 → 61862 [ACK] Seq=1 Ack=502 Win=262144 Len=0
11	0.146885	13.107.3.128	192.168.0.109	TCP	1514	443 → 61862 [ACK] Seq=1 Ack=502 Win=262144 Len=1460 [TCP segment of a reassembled PDU]
12	0.146887	13.107.3.128	192.168.0.109	TCP	1514	443 → 61862 [ACK] Seq=1461 Ack=502 Win=262144 Len=1460 [TCP segment of a reassembled PDU]
13	0.147026	192.168.0.109	13.107.3.128	TCP	54	61862 → 443 [ACK] Seq=502 Ack=2921 Win=262144 Len=0
14	0.147150	13.107.3.128	192.168.0.109	TCP	1514	443 → 61862 [ACK] Seq=2921 Ack=502 Win=262144 Len=1460 [TCP segment of a reassembled PDU]
15	0.147157	13.107.3.128	192.168.0.109	TCP	1514	443 → 61862 [ACK] Seq=4381 Ack=502 Win=262144 Len=1460 [TCP segment of a reassembled PDU]

Let’s talk cases!!

DGA *(The DGA Family)*

The Characteristics tells the activity is related to ***Conficker*** Family –

“Conficker use NBNS (NetBIOS Name Service or netbios-ns) protocol to propagate itself into network. NBNS will read the hostname which is tried to attach by Conficker botnet. The hostname will indicate which hostname or computer attach by Conficker. ”

Let’s talk cases!!

DGA *(NetFlow Pattern for C2C server)*

Day 1

```
Date first seen          Duration Proto      Src IP Addr:Port          Dst IP Addr:Port   Packets    Bytes Flows
2021-01-11 09:20:02.980     0.000 UDP        172.2.2.2:60948 ->   209.58.130.216:53             1       67     1
2021-01-11 09:20:02.980     0.000 UDP        172.2.2.2:60940 ->   119.81.145.164:53             1       67     1
2021-01-11 09:20:02.980     0.000 UDP        172.2.2.2:60942 ->   89.187.163.225:53             1       67     1
2021-01-11 09:20:02.980     0.000 UDP        172.2.2.2:60947 ->    119.81.212.83:53             1       67     1
2021-01-11 09:20:04.970     0.000 UDP        172.2.2.2:51716 ->   185.246.208.33:53             1      146     1
```

Day 2

```
2021-01-12 09:20:10.990     0.000 UDP        172.2.2.2:63512 ->  185.246.210.177:53             1       67     1
2021-01-12 09:20:10.990     0.000 UDP        172.2.2.2:63506 ->   119.81.145.164:53             1       67     1
2021-01-12 09:20:10.990     0.000 UDP        172.2.2.2:63511 ->   156.146.38.142:53             1       67     1
2021-01-12 09:20:10.950     0.000 UDP        172.2.2.2:63516 ->   89.187.163.225:53             1      146     1
2021-01-12 09:20:10.950     0.000 UDP        172.2.2.2:63521 ->    119.81.38.202:53             1      146     1
```

Day 3

```
2021-01-13 09:20:01.980     0.000 UDP        172.2.2.2:56822 ->   89.187.163.225:53             1       67     1
2021-01-13 09:20:01.990     0.000 UDP        172.2.2.2:56824 ->   119.81.145.164:53             1       67     1
2021-01-13 09:20:01.990     0.000 UDP        172.2.2.2:56829 ->     84.17.46.133:53             1       67     1
2021-01-13 09:20:01.990     0.000 UDP        172.2.2.2:56827 ->    192.99.100.41:53             1       67     1
2021-01-13 09:20:02.950     0.000 UDP        172.2.2.2:56845 ->    119.81.212.69:53             1      146     1
```

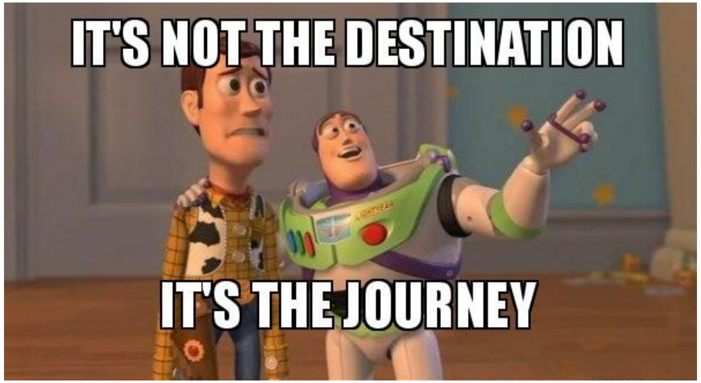
Challenges

- False-positive alert flood.
- SOC infrastructure escalation.
- Lack of subject matter expertise.
- Communication gap between the team.
- Amateurishness of end-user to an attack alert.

I've only been at work for an hour and this is already me 😩😩😩
Sweet Jesus, grant me the power to deal with this bullshit

Future Work

- Container orchestration in ***Kubernetes***
- ***PassiveDNS*** info for Anycast Recursive DNS infrastructure
- Move visualization from ELK stack to ***Grafana*** eco-system
- Incorporate ***osquery*** for EDR



Reference

- Ten Strategies of a World-Class Cybersecurity Operations Center - Carson Zimmerman, MITRE. https://www.mitre.org/sites/default/files/publications/pr-13-1028-mitre-10-strategies-cyber-ops-center.pdf
- 6 Phases In The Incident Response Plan, David Ellis. https://www.securitymetrics.com/blog/6-phases-incident-response-plan
- The Incident Handler’s Handbook, Patrick Kral. 2012. https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901
- NIST Computer Security Incident Handling Guide, SP 800-61r2, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf
- The Tao of Network Security Monitoring, BEYOND INTRUSION DETECTION by Richard Bejtlich
- Blue Team Handbook: SOC, SIEM, and Threat Hunting Use Cases, Don Murdoch
- https://thehive-project.org/
- https://www.misp-project.org/
- https://wazuh.com/
- https://suricata-ids.org/
- https://www.stamus-networks.com/scirius-open-source
- https://evebox.org/
- https://prometheus.io/
- https://grafana.com/
- https://rocket.chat/
- https://dnsrpz.info/
- https://arkime.com/
- https://www.elastic.co/
- https://www.docker.com/
- https://www.open-scap.org/
- https://attack.mitre.org/
- https://academy.apnic.net/
- https://www.gartner.com/doc/reprints?id=1-1YAR7TFJ&ct=200207&st=sb

2021

APRICOT

APNIC 51

Manila, Philippines

22 February – 4 March 2021

#apricot2021