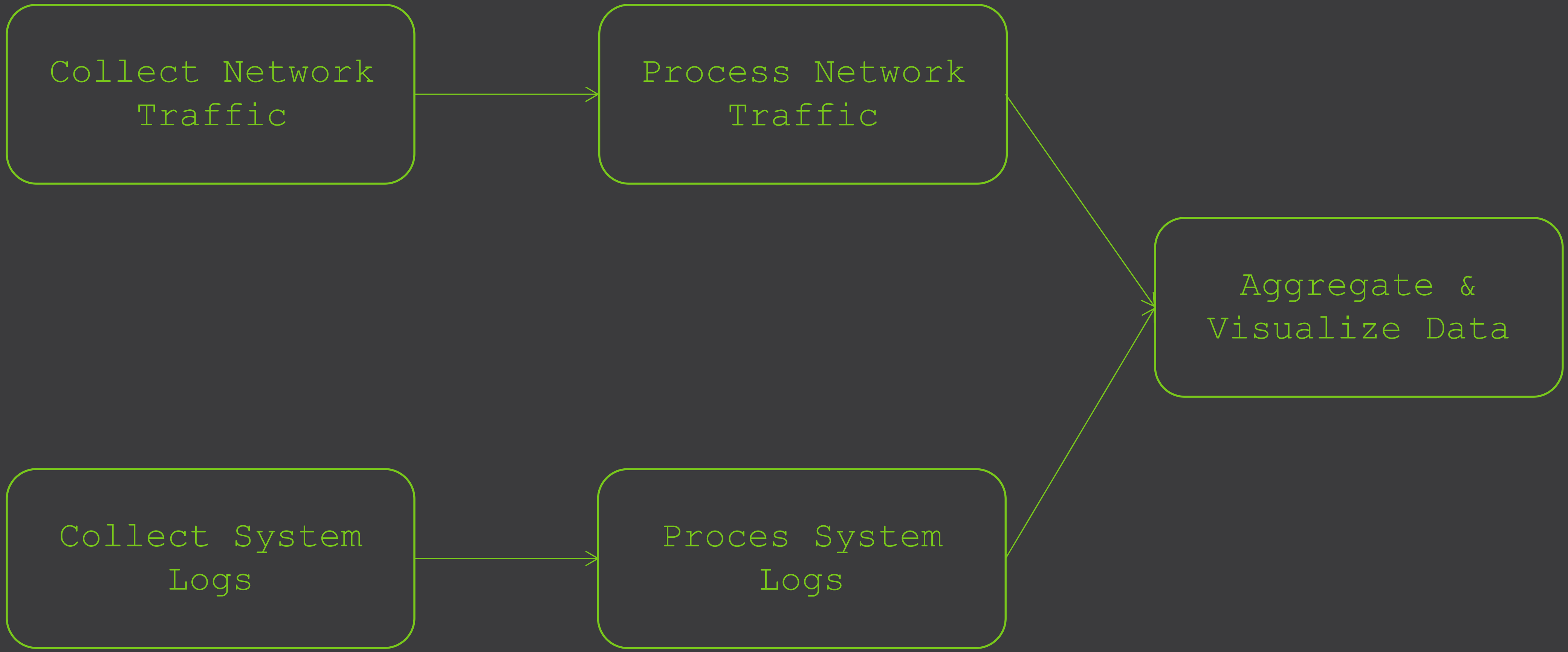
Open Source in SOC

HACKLAB BITM

@_tosto_

Hackers Eat Pizza
13-01-2019

IDS



Collect Network Traffic

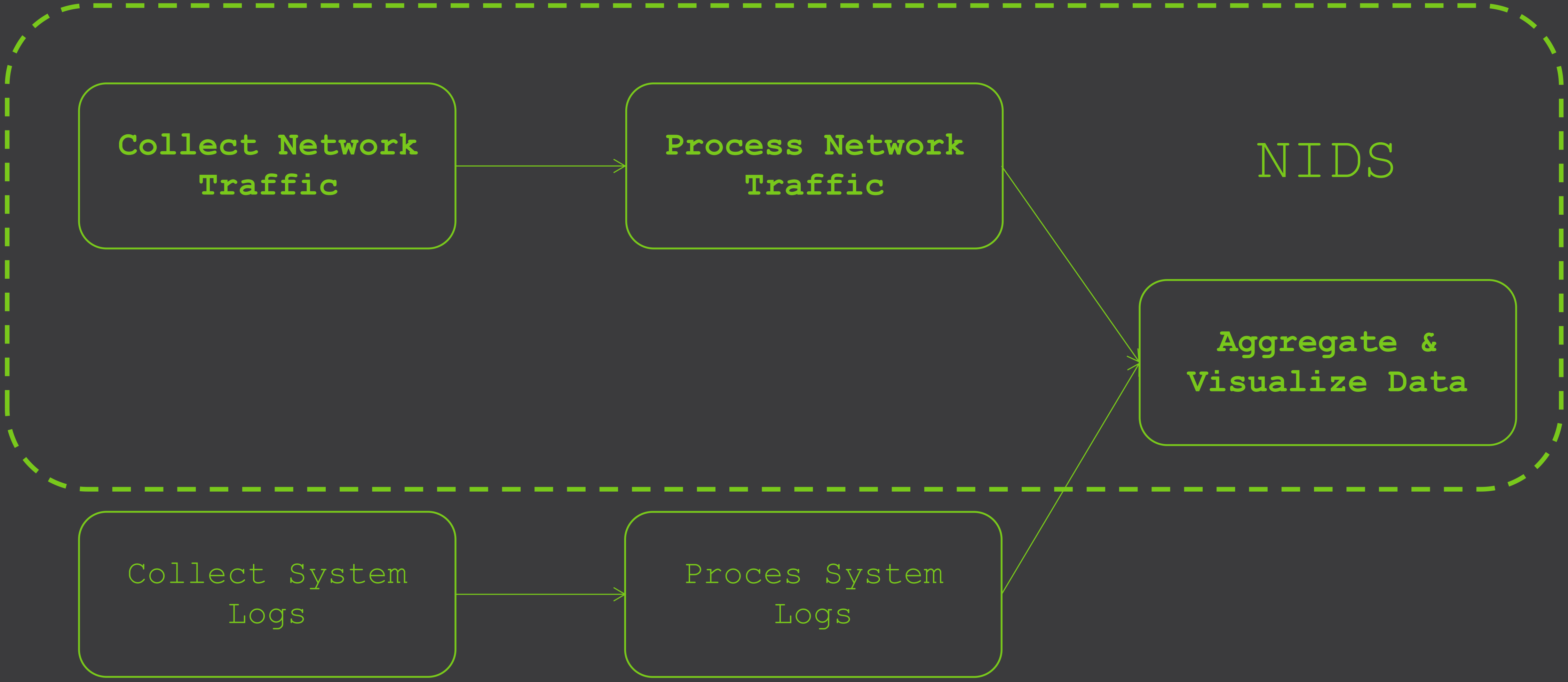
Process Network Traffic

Collect System Logs

Proces System Logs

Aggregate & Visualize Data

IDS


Collect Network Traffic
Process Network Traffic
NIDS
Aggregate & Visualize Data
Collect System Logs
Proces System Logs

Network IDS (NIDS)

- Netsniff-ng (https://github.com/netsniff-ng/netsniff-ng)
  - Full Packet Capture
- Snort|Suricata (https://www.snort.org/downloads | https://github.com/OISF/suricata)
  - IDS Rules
- Barnyard (https://github.com/firnsy/barnyard2)
  - Parse Snort Unified Binaries
- Bro(Zeek) (https://github.com/bro/bro)
  - Traffic Analysis
  - File Extraction
- PF Ring (https://github.com/ntop/PF_RING)
  - Parallelization

Network IDS (NIDS)

- Netsniff-ng (https://github.com/netsniff-ng/netsniff-ng)
  - Full Packet Capture
- **Snort|Suricata** (https://www.snort.org/downloads | https://github.com/OISF/suricata)
  - IDS Rules
- Barnyard (https://github.com/firnsy/barnyard2)
  - Parse Snort Unified Binaries
- Bro(Zeek) (https://github.com/bro/bro)
  - Traffic Analysis
  - File Extraction
- PF Ring (https://github.com/ntop/PF_RING)
  - Parallelization

Snort | Suricata

```
alert udp $HOME_NET any -> any 53 (msg:"BLACKLIST DNS request for known bad domain
hacklabg.net"; content:"|08|hacklabg|03|net|00|"; sid:9999999; rev:1;
metadata:created_at 2019_13_01;)
```

- alert
- udp
- $HOME_NET any
- any 53
- msg:"BLACKLIST DNS request for known bad domain hacklabg.net"
- content:"|08|hacklabg|03|net|00|"

Network IDS (NIDS)

- Netsniff-ng (https://github.com/netsniff-ng/netsniff-ng)
  - Full Packet Capture
- Snort|Suricata (https://www.snort.org/downloads | https://github.com/OISF/suricata)
  - IDS Rules
- Barnyard (https://github.com/firnsy/barnyard2)
  - Parse Snort Unified Binaries
- **Bro(Zeek)** (https://github.com/bro/bro)
  - Traffic Analysis
  - File Extraction
- PF Ring (https://github.com/ntop/PF_RING)
  - Parallelization

Bro (Zeek)

- Connections log
- dns/http/ftp/smtp log
- ssl log
- notice log
- file extraction
- Intel

MISP

- Malware Information Sharing Platform
  - Store
  - Correlate
  - Share

- API
  - Extract Snort/Suricata Rules
  - Extract Bro Intel

Aggregate & Visualize

elastic stack

elasticsearch

logstash

kibana

Aggregate & Visualize

elastic stack

elasticsearch

logstash

Log Parsing

kibana

Aggregate & Visualize

elastic stack

elasticsearch

Log Indexing

logstash

Log Parsing

kibana

Aggregate & Visualize

elastic stack

elasticsearch

Log Indexing

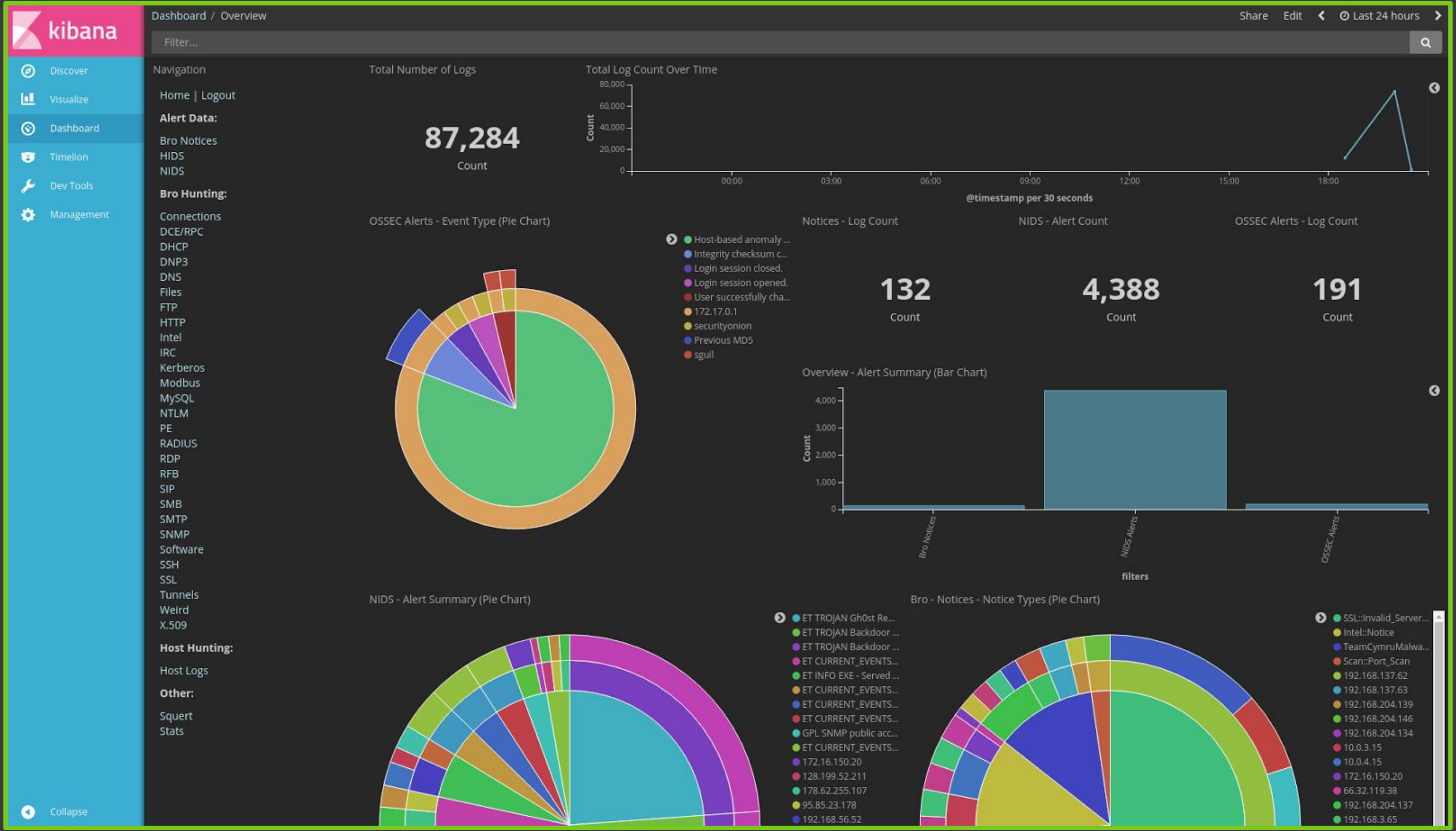
logstash

Log Parsing

kibana

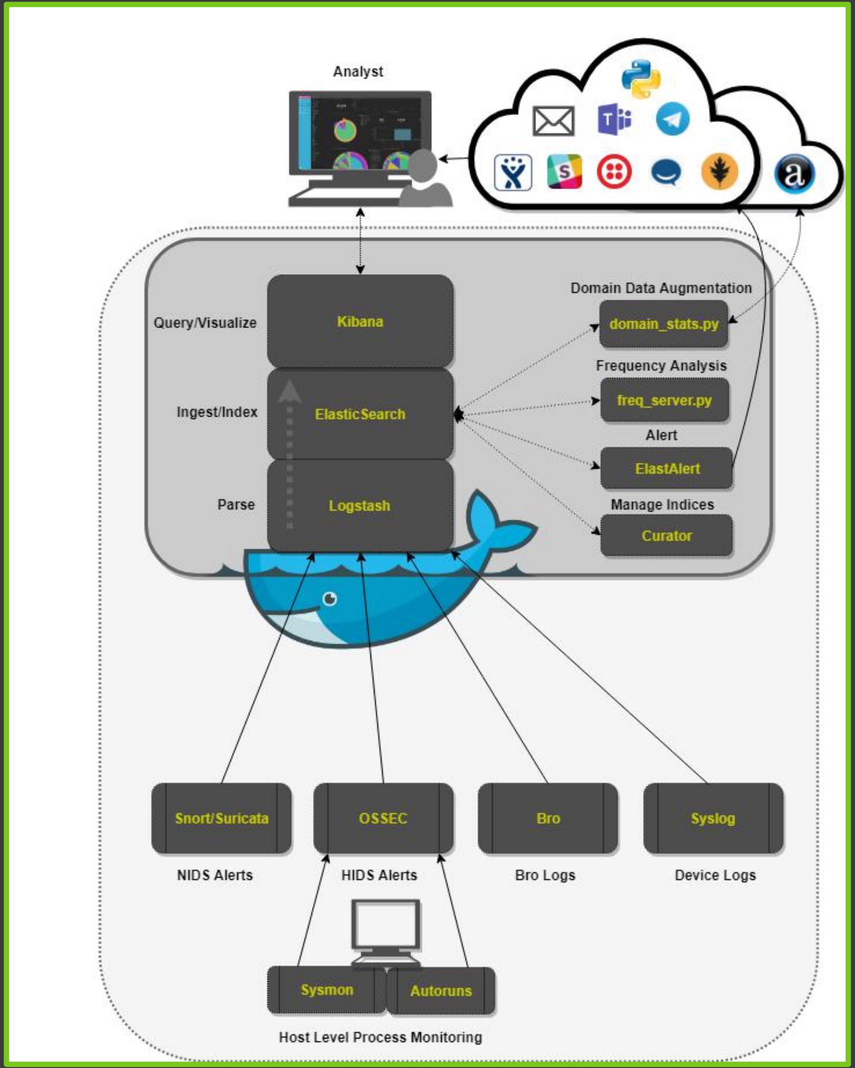
Log Visualization

Kibana Dashboards



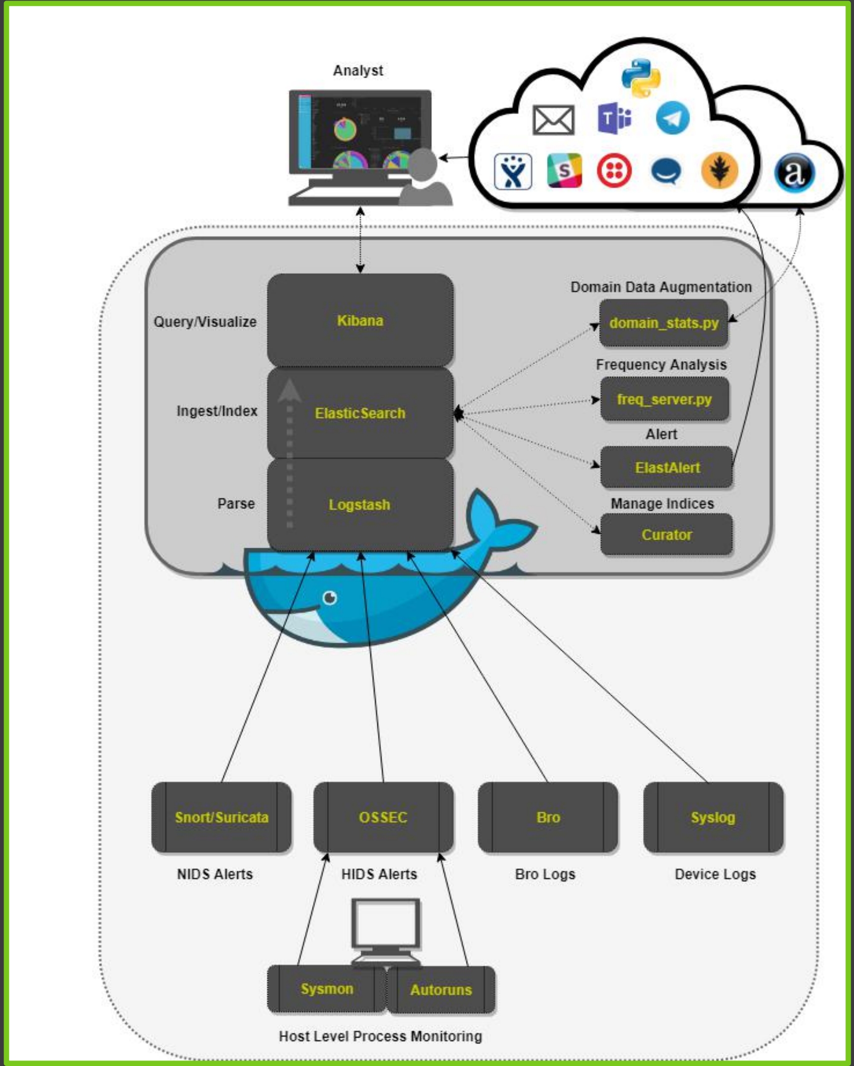
Security Onion

- Linux Distro for IDS (https://github.com/Security-Onion-Solutions/security-onion)
  - Ubuntu Based
  - Easy to configure
  - Scalable



Security Onion

- Linux Distro for IDS (https://github.com/Security-Onion-Solutions/security-onion)
    - Ubuntu Based
    - Easy to configure
    - **Scalable**



Security Onion - Node Types

- Master Server
  - Elasticsearch, Logstash, Kibana, Curator, Elastalert, Redis, OSSEC, Sguild
- Forward Node(Sensor Only)
  - Bro, Snort/Suricata, Netsniff-NG, OSSEC, Syslog-NG
- Heavy Node
  - Elasticsearch, Logstash, Curator, Bro, Snort/Suricata, Netsniff-NG, OSSEC, Syslog-NG
- Storage Node
  - Elasticsearch, Logstash, Curator, OSSEC

Security Onion - Configurations

- Standalone
- Distributed
  - Master Server + Heavy Nodes
- Heavy Distributed
  - Master Server + Forward Nodes + Storage Nodes

Grazie per l'attenzione!

HACKLAB

BITM

@_tosto_

Hackers Eat Pizza
13-01-2019