CONTINUOUS SECURITY MONITORING WITH

ELK STACK

WITH JANITH MALINGA

Contents

- Why continuous security monitoring
- Intro to ELK Stack
- Install Elasticsearch and Cerebro
- Install Kibana and create dashboards
- Install Logstash and create config files
- Install filebeat agent and forward logs

INTRODUCTION TO

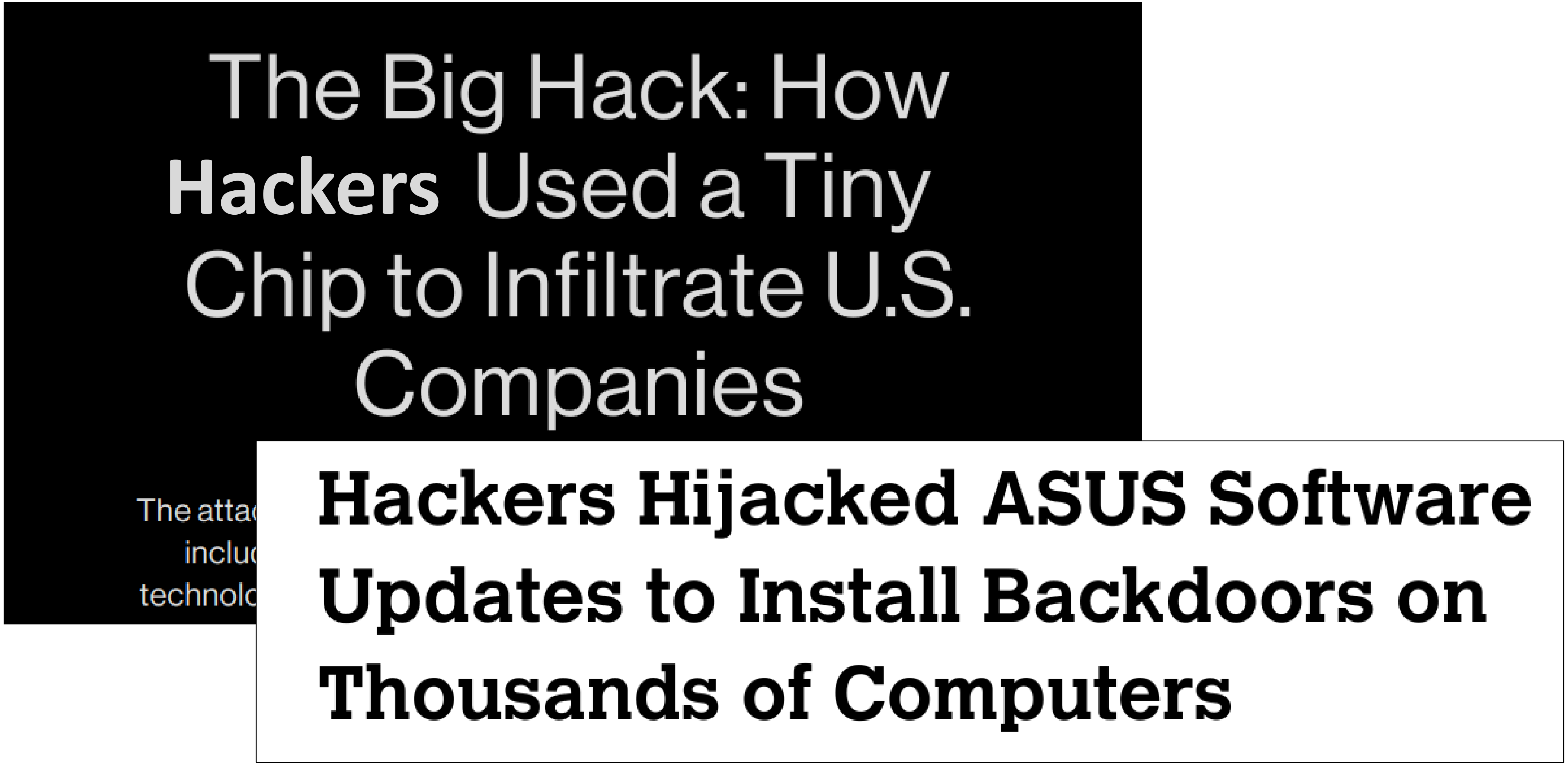
CONTINUOUS SECURITY MONITORING

Security Systems In Use

- Firewall
- Antivirus software
- Web application firewall (waf)

NEW TRENDS OF ATTACKS

Emerging Threats



The Big Hack: How **Hackers** Used a Tiny Chip to Infiltrate U.S. Companies

The attac
incluc
technolo

Hackers Hijacked ASUS Software Updates to Install Backdoors on Thousands of Computers

New Trends Of Attacks

- Supply chain management
- Hardware layer

SIEM

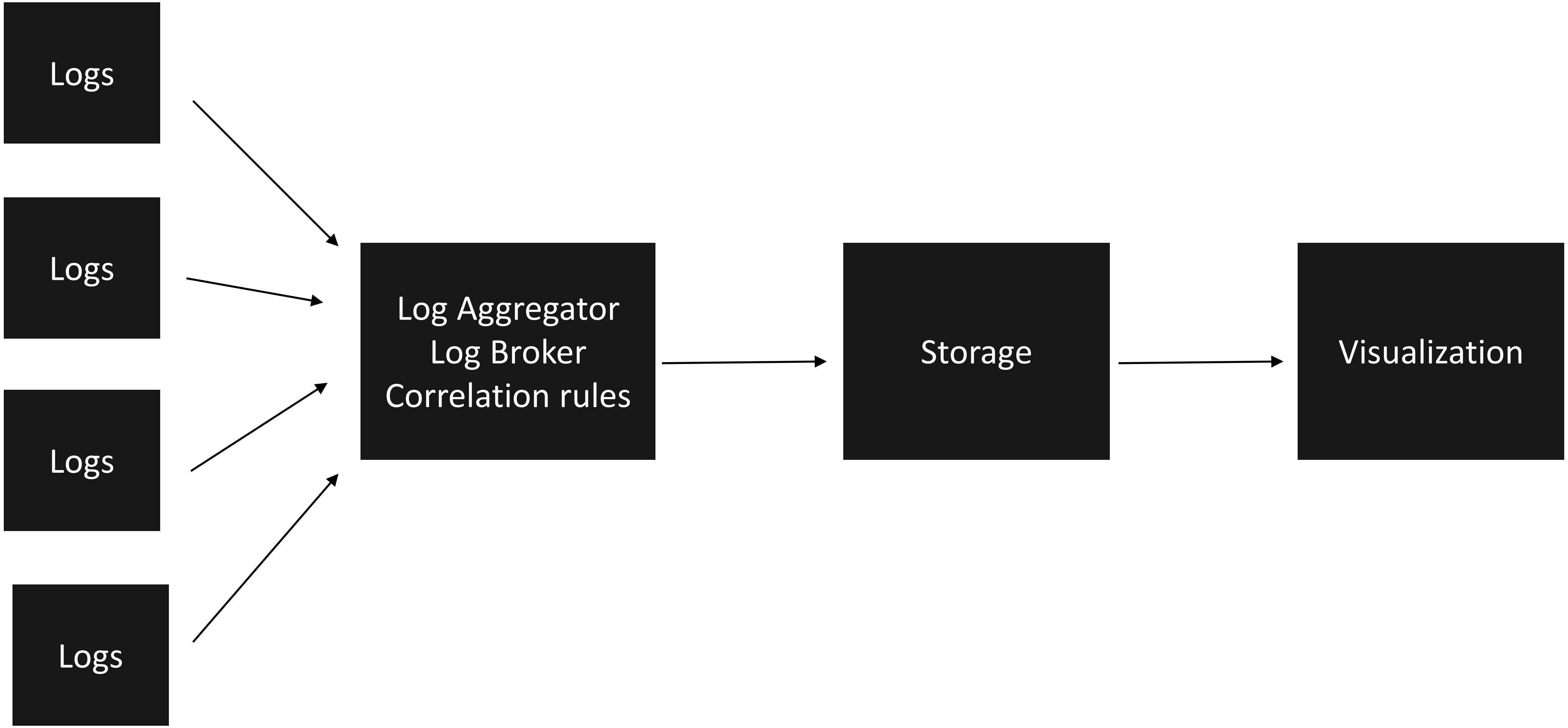
SIEM

"In the field of computer security, **security information and event management** (**SIEM**) software products and services combine security information management (SIM) and security event management (SEM). They provide real-time analysis of security alerts generated by applications and network hardware."

Wikipedia

The general perception is that setting up SIEM is a very expensive exercise, however with the right knowledge and skill it can be done at a fraction of the cost.

Functions of a SIEM



Logs

Logs

Logs

Logs

Log Aggregator
Log Broker
Correlation rules

Storage

Visualization

Continuous Security Monitoring

- End point security monitoring
- Network security monitoring

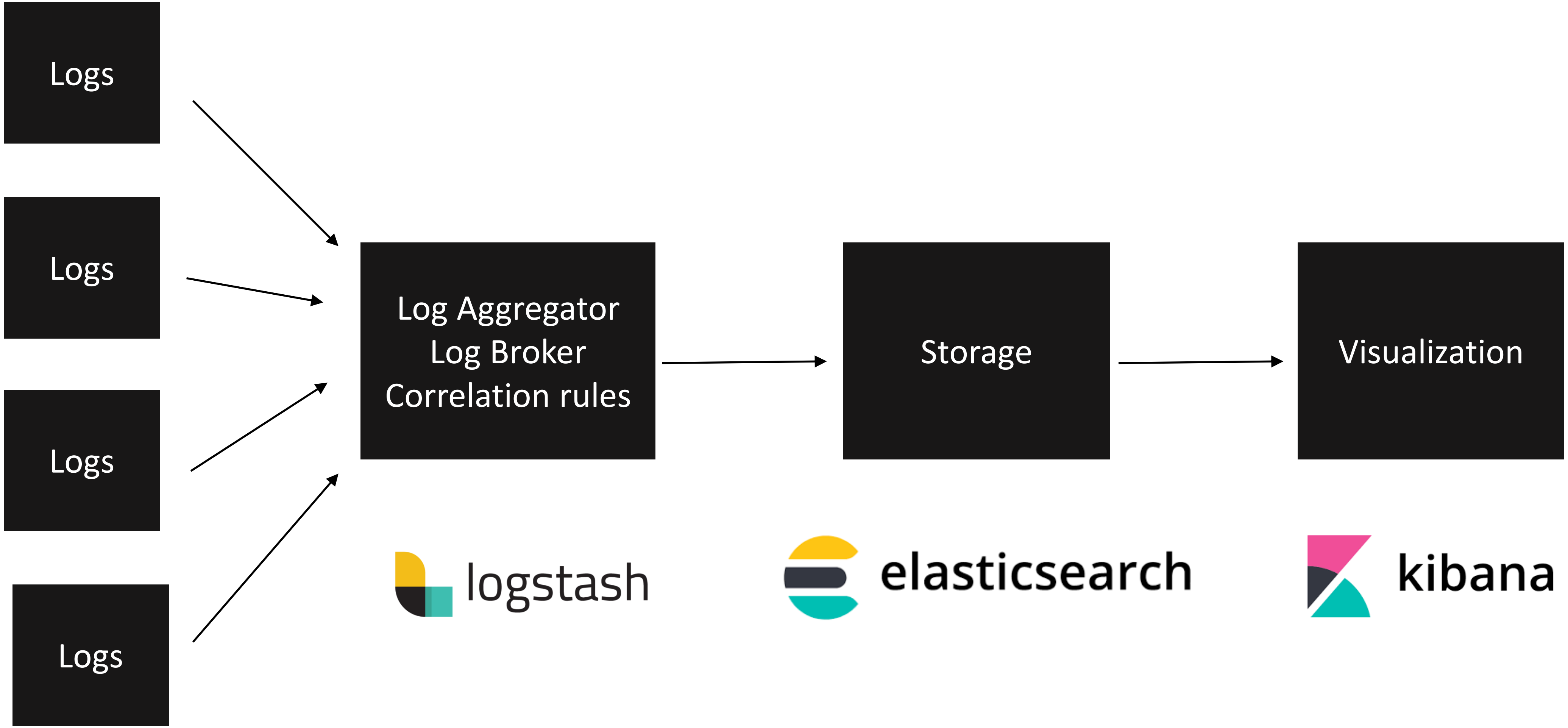
PRACTICAL SECURITY MONITORING WITH ELK STACK

elasticsearch

logstash

kibana

Functions of a SIEM



Elastic Stack vs Commercial SIEM

- Elastic Stack
- Free, Paid support features
- Outstanding visualizations
- Advanced log enrichments
- Capable handling high volume

- Commercial SIEM
- Licensed on volume, log sources, events per second
- Limited log enrichment
- High volume = High cost

Minimum Hardware Requirements

- Ram: 8GB
- Storage: 40GB
- 2 Network interfaces
- CPU: 64-bit 2.0+ GHz processor or higher

ELASTICSEARCH

Install Elasticsearch

```
#sudo dpkg -i elasticsearch-6.0.0.deb
```

Config files locations:-

Elasticsearch has three configuration files:

- **elasticsearch.yml** for configuring Elasticsearch
- **jvm.options** for configuring Elasticsearch JVM settings
- **log4j2.properties** for configuring Elasticsearch logging

Elasticsearch

- Distributed, real-time data store, real-time analysis full text search engine
- Opensource
- Highly scalable

Indices, Shards and Replicas

- An index is stored on a node, which is a part of a cluster
- Indices are broken into shards
- Each shard is either a primary or replica
- Each log item is a document that contains fields and values

CEREBRO

Cerebro

- Cerebro is an opensource Elasticsearh web admin tool
- Displays cluster health
- Makes index managements easy

Install Cerebro

```
#sudo unzip cerebro-0.7.1.zip -d /opt
#sudo mv /opt/cerebro-0.7.1/ /opt/cerebro/
```

Create a user for cerebro

```
#sudo useradd cerebro
```

Give permissions for the user

```
#sudo chown -R cerebro: /opt/cerebro/
```

Create a service for cerebro

```
#sudo cp cerebro.service /etc/systemd/system
#sudo systemctl daemon-reload
#sudo systemctl enable cerebro.service
#sudo service cerebro start
```

KIBANA

Install Kibana

```
#sudo dpkg -i kibana-6.0.0-amd64.deb
```

Enable kibana service

```
#sudo systemctl enable kibana.service
```

Start kibana service

```
#sudo service kibana start
```

LOGSTASH

Install Logstash

#sudo dpkg -I logstash-6.2.1.deb

Config file

jvm.options

Logstash Config File Format

```
input{
        }
filter{
        }
output{
        }
```

Logstash Config File Format

```
input {
  stdin { codec => "json" }
}
filter {
  if [event_id] == 123 {
    drop { }
  }
}
output {
  stdout { codec => rubydebug }
}
```

THANK YOU

FOLLOW US ON

/econIntconference

@econ_int

@int.econ