Intrusion Detection Systems

Pythology 2018.1

Pradeep Gowda <@btbytes>

⚡ Who am I ⚡

- Member of IndyPy since *2008*
- Staff Software Engineer at Proofpoint
- Aquired Indy based **Emerging Threats** in 2015

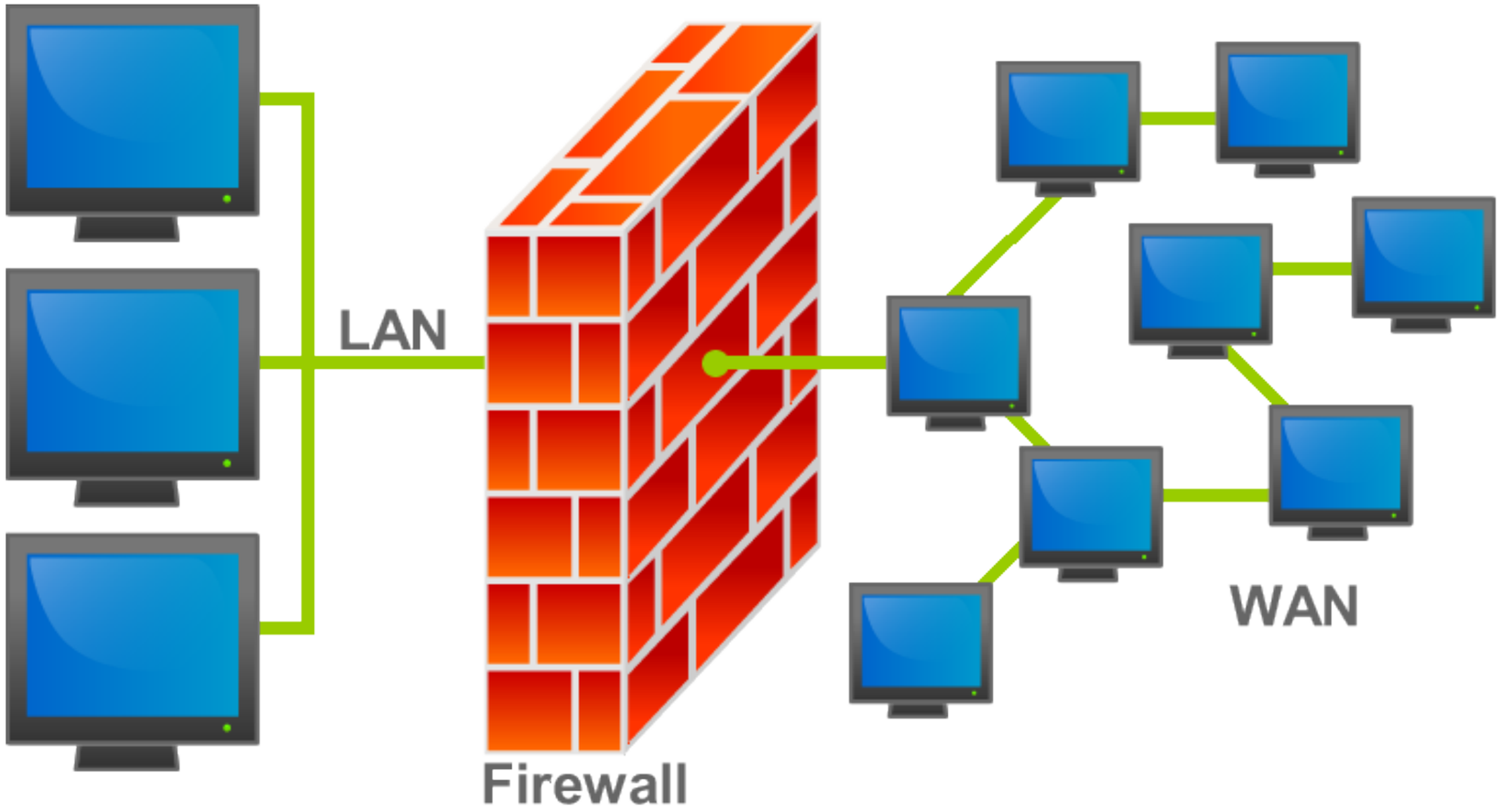
Proofpoint

- Email fraud defence
- Email protection
- Targeted attack protection (TAP)
- Mobile defence
- Social media protection
- **Threat Intelligence**

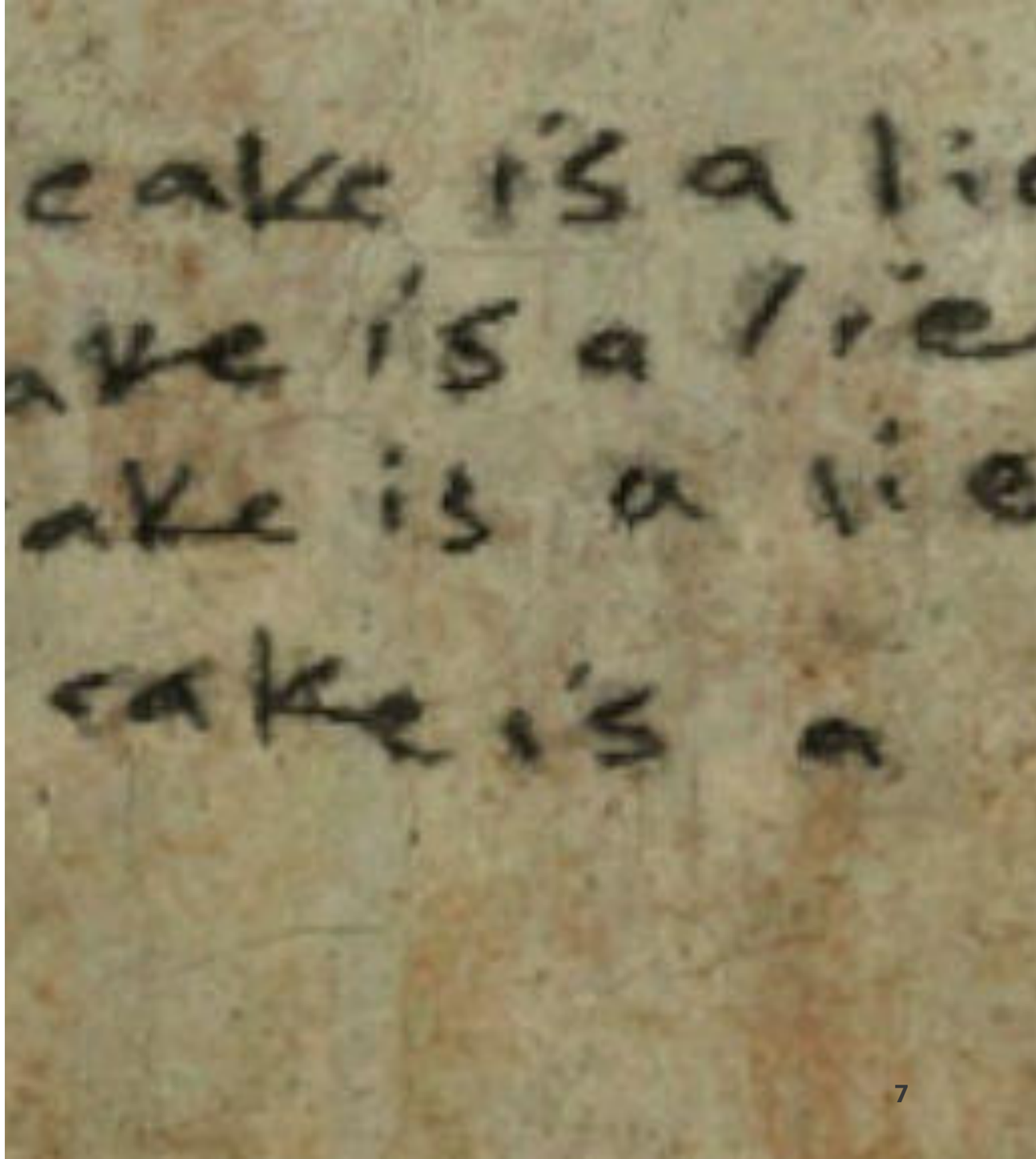
State of cyber-things

Antivirus

Firewall



The wall is a lie!



BYOD

Virtual Machines

Internet of things


movie.tumblr.com
WE'VE TRACED THE CALL
IT'S COMING FROM INSIDE THE HOUSE


BUT WHEN SHE TRACED THE KILLER'S IP ADDRESS... IT WAS IN THE 192.168/16 BLOCK!
GASP!

proofpoint.

PRODUCTS SOLUTIONS

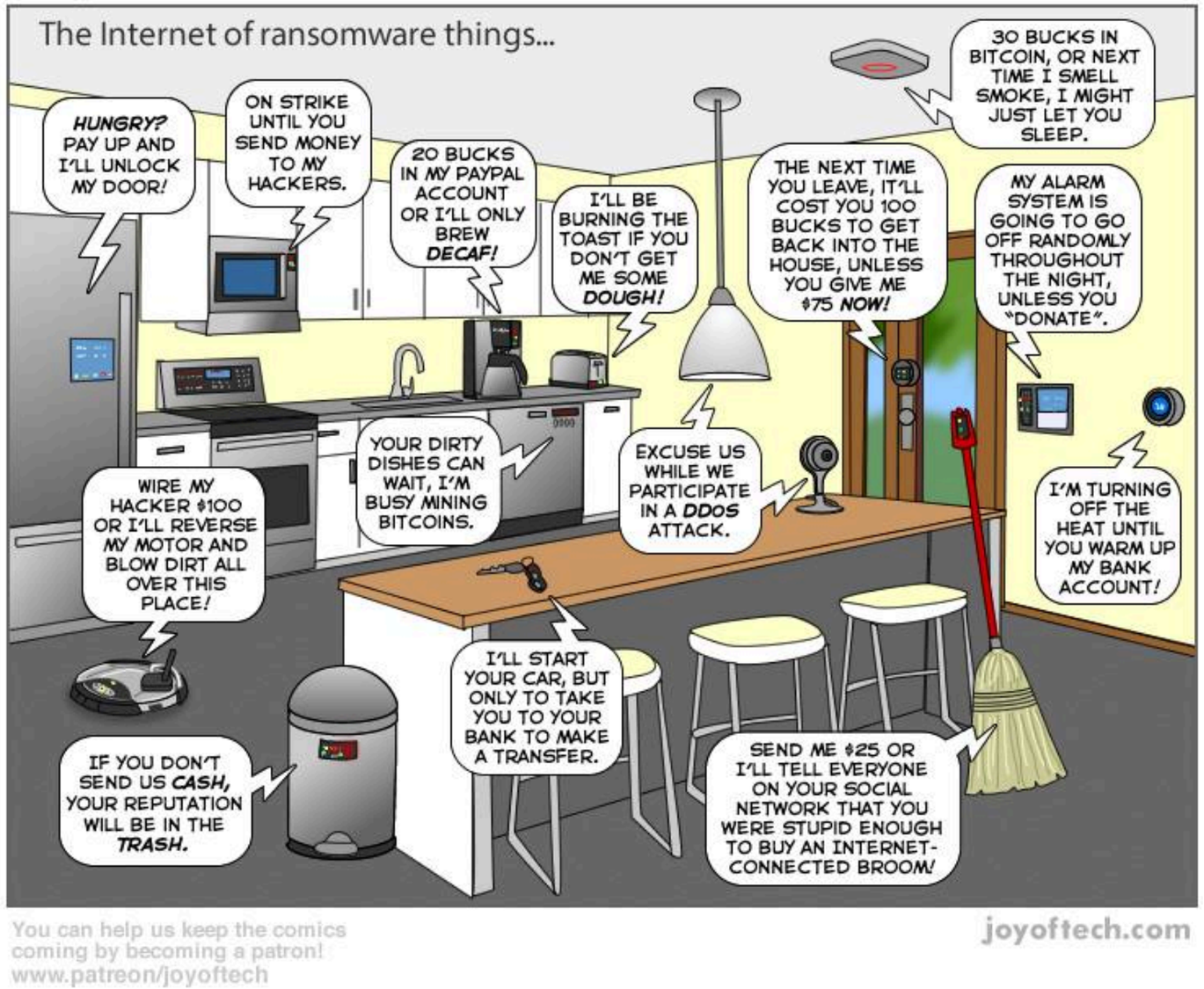
YOUR FRIDGE IS FULL OF SPAM: PROOF OF AN IOT-DRIVEN ATTACK

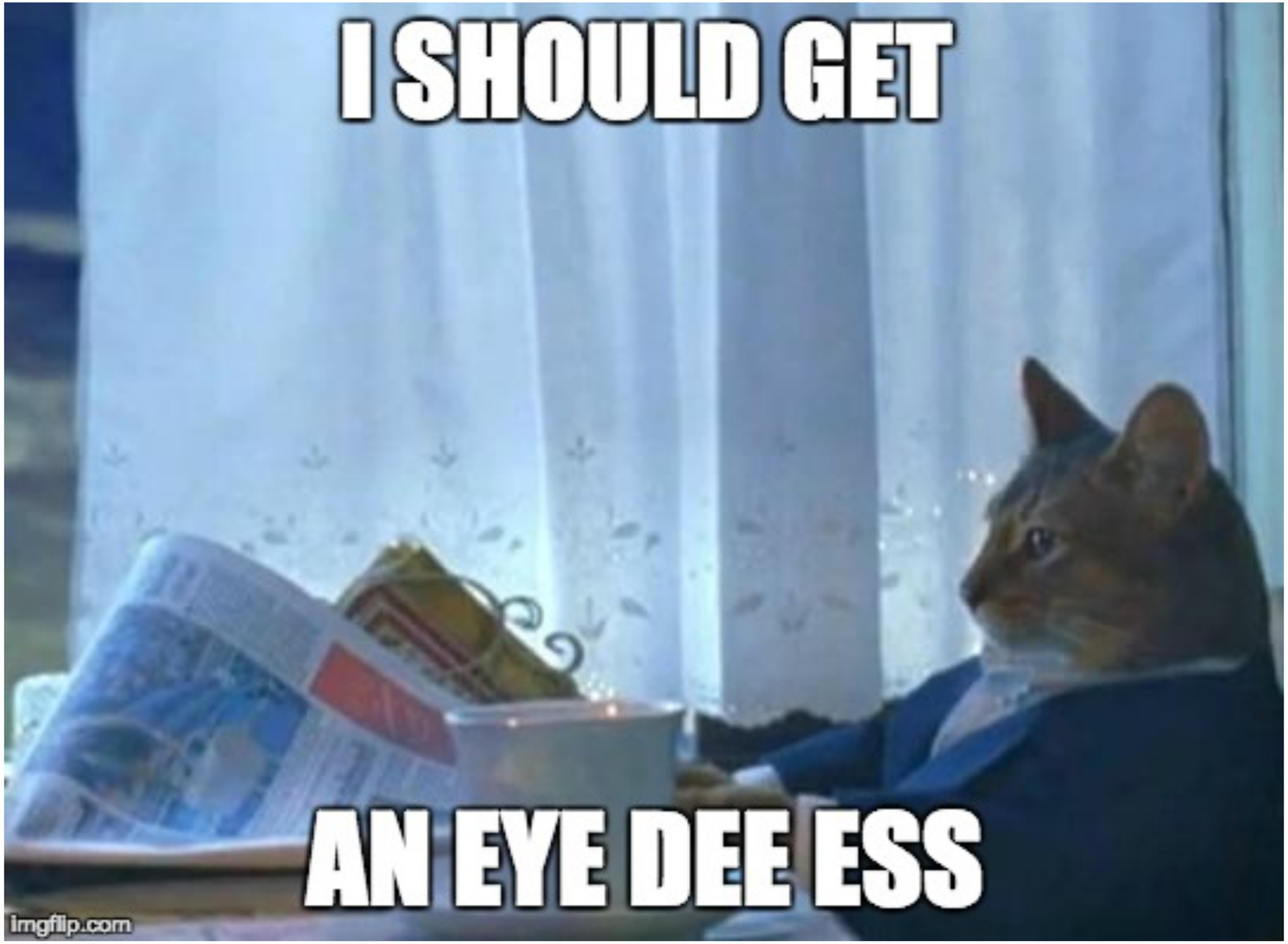
JANUARY 16, 2014

WIRED SUBSCR

LILY HAY NEWMAN SECURITY 12.09.16 07:00 AM

THE BOTNET THAT BROKE THE INTERNET ISN'T GOING AWAY


The Joy of Tech™ by Nitrozac & Snaggy
The Internet of ransomware things...
HUNGRY? PAY UP AND I'LL UNLOCK MY DOOR!
ON STRIKE UNTIL YOU SEND MONEY TO MY HACKERS.
20 BUCKS IN MY PAYPAL ACCOUNT OR I'LL ONLY BREW DECAF!
I'LL BE BURNING THE TOAST IF YOU DON'T GET ME SOME DOUGH!
30 BUCKS IN BITCOIN, OR NEXT TIME I SMELL SMOKE, I MIGHT JUST LET YOU SLEEP.
THE NEXT TIME YOU LEAVE, IT'LL COST YOU 100 BUCKS TO GET BACK INTO THE HOUSE, UNLESS YOU GIVE ME $75 NOW!
MY ALARM SYSTEM IS GOING TO GO OFF RANDOMLY THROUGHOUT THE NIGHT, UNLESS YOU "DONATE".
YOUR DIRTY DISHES CAN WAIT, I'M BUSY MINING BITCOINS.
EXCUSE US WHILE WE PARTICIPATE IN A DDOS ATTACK.
I'M TURNING OFF THE HEAT UNTIL YOU WARM UP MY BANK ACCOUNT!
WIRE MY HACKER $100 OR I'LL REVERSE MY MOTOR AND BLOW DIRT ALL OVER THIS PLACE!
I'LL START YOUR CAR, BUT ONLY TO TAKE YOU TO YOUR BANK TO MAKE A TRANSFER.
IF YOU DON'T SEND US CASH, YOUR REPUTATION WILL BE IN THE TRASH.
SEND ME $25 OR I'LL TELL EVERYONE ON YOUR SOCIAL NETWORK THAT YOU WERE STUPID ENOUGH TO BUY AN INTERNET-CONNECTED BROOM!
You can help us keep the comics coming by becoming a patron!
www.patreon/joyoftech
joyoftech.com


I SHOULD GET
AN EYE DEE ESS
imgflip.com

What is an N.I.D.S?

Network Intrusion Detection System (NIDS)

Commonly known as IDS

A software that is capable of:

- Real time analysis of network traffic
- Apply predefined rules
- Log interesting "things" (files, TLS certs)

How does an IDS work

- Process packets
- Decode packets
- Reassembly of IP packets, TCP streams
- Advanced HTTP parses and TLS
- Detection (packet, stream, state)

Which one(s)?

Fail2ban

- operates by monitoring log files
- `/var/log/auth.log`
- `/var/log/apache/access.log`
- for selected entries and running scripts based on them.

FAIL2BAN

Snort

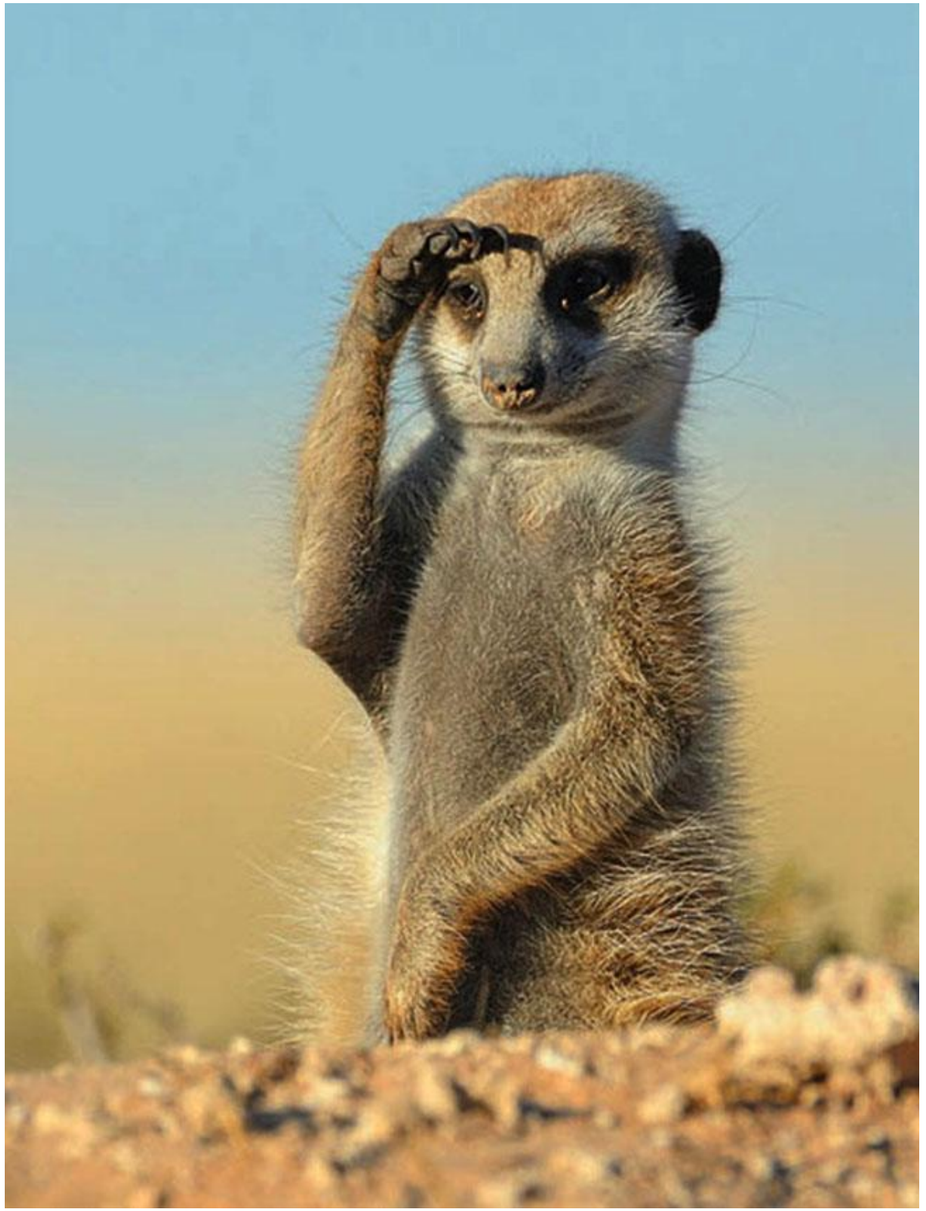
- OpenSource
- SourceFire/Cisco
- Sniffer/packet logger/IDS
- The well-known player

Bro IDS

- https://www.bro.org/
- Focussed on analyst automation

Suricata

- Snort++
- Multi threaded
- Hardware accelaration
- File extraction
- TLS Cert extraction
- Lua (scripting)




SURICATA

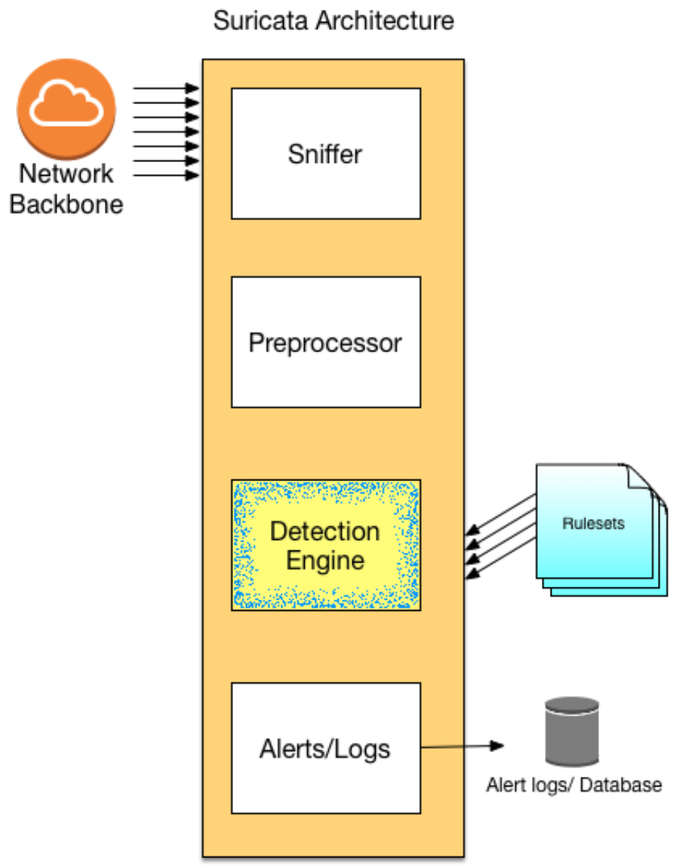
Suricata

- Suricata is a free and open source, mature, fast and robust network threat detection engine
- Built by OISF
- Indiana based non-profit
- Originally funded by DHS
- Supported by consortium of users around the world
- Proofpoint is one of the two Platinum consortium members

Advantage suricata

- Get most out of your hardware (multi threading, multicore, GPU)
- High level protocol detection (HTTP)
- Advanced HTTP inspection and logging
- JSON logging for easy post-processing

Suricata


Suricata Architecture
Network
Backbone
Sniffer
Preprocessor
Detection
Engine
Rulesets
Alerts/Logs
Alert logs/ Database

Rules / Signatures

- Most people use existing rulesets
- Writing rules requires extensive research and testing
- Performance and False-positives are a big concern

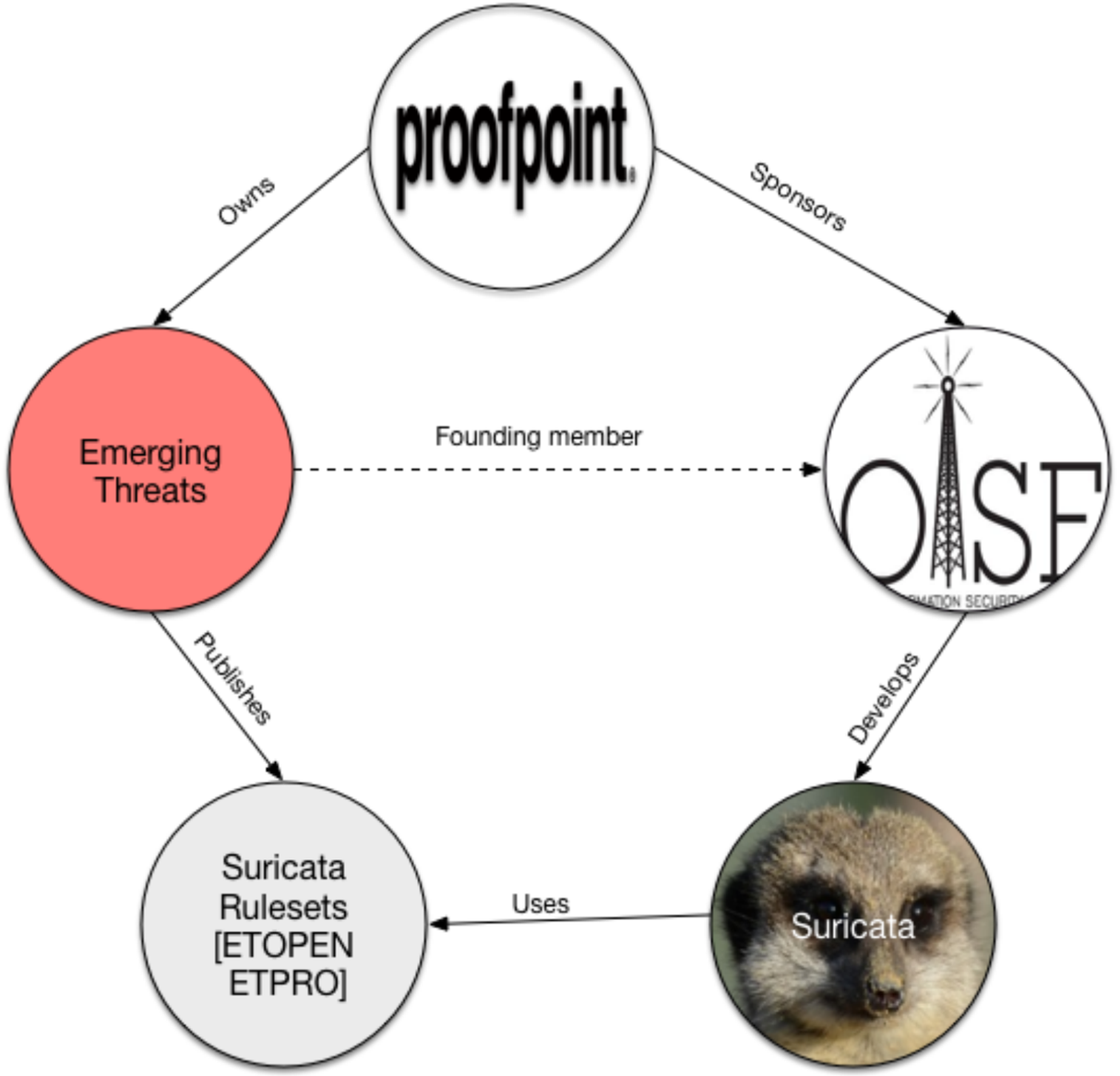
Rules / Signatures

- Most commonly used:
  - **ETOpen** - free to download and Use; community driven
  - **ETPro** - commerical offering by Proofpoint
  - Sourcefire VRT (Snort)

@ET_Labs

2 new Open, 15 new Pro (2 + 13). CoreBot CnC, Win32.Banload.XZH, Various Phishing, Various Mobile.

lists.emergingthreats.net/pipermail/emer …


proofpoint.
Owns
Sponsors
Emerging Threats
Founding member
OISF
Publishes
Develops
Suricata Rulesets [ETOPEN ETPRO]
Uses
Suricata

A Suricata Rule

```
alert http $EXTERNAL_NET any -> $HOME_NET any
    (   msg:"ET WEB_SERVER Possible Awesomeness (INDYPY Demo Rule)";
        flow:established,from_server;
        content:"l33thax0rs";
        reference:url,meetup.com/indypy;
        reference:url,caring-picture.surge.sh;
        classtype:successful-user;
        sid:2008208;
        rev:1;
        metadata:created_at 2018_02_01, updated_at 2018_02_02;
    )
```

Anatomy of a rule

- Action -- `alert`, `log`, `pass`, `drop`, `reject`
- Header -- `EXTERNAL_NET`, `HOME_NET`
- Rule options -- `[name]:settings;`

C.R.E.A.M

- Cache
- Rules
- Everything
- Around
- Me

Sc.R.E.A.M

- **S**uri**c**ata
- Rules
- Everything
- Around
- Me

TLS

Alert

If a cerificate for `.googleusercontent.com` is not signed by `Google-Internet-Authority`

```
alert tls any any -> any any (msg:"forged ssl google user";
            tls.subject:"CN=*.googleusercontent.com";
            tls.issuerdn:!"CN=Google-Internet-Authority"; sid:8; rev:1;)
```

TLS fingerprint match

Alert when subject matches the `Company` but not the fingerprint we expect it to have.

```
alert tls any any -> any any (msg:"Company fingerprint";
        tls.subject:"CN=www.company.com";
        tls.fingerprint:!"f8:30..blah.."; sid:1000012; rev:1;)
```

File extraction

- `filemagic`
- `fileextract`

TLS Store

```
alert tls any any -> any any
    (
        msg:"Company fingerprint";
        tls.subject:"CN=www.company.com";
        tls.fingerprint:!"f8:30:..blah..";
        filestore;
        sid:1000012;
        rev:1;
    )
```

Save -- metadata + TLS Cert

- 1346085544.64714-1.pem
- 1346085544.64714-1.meta

Metadata

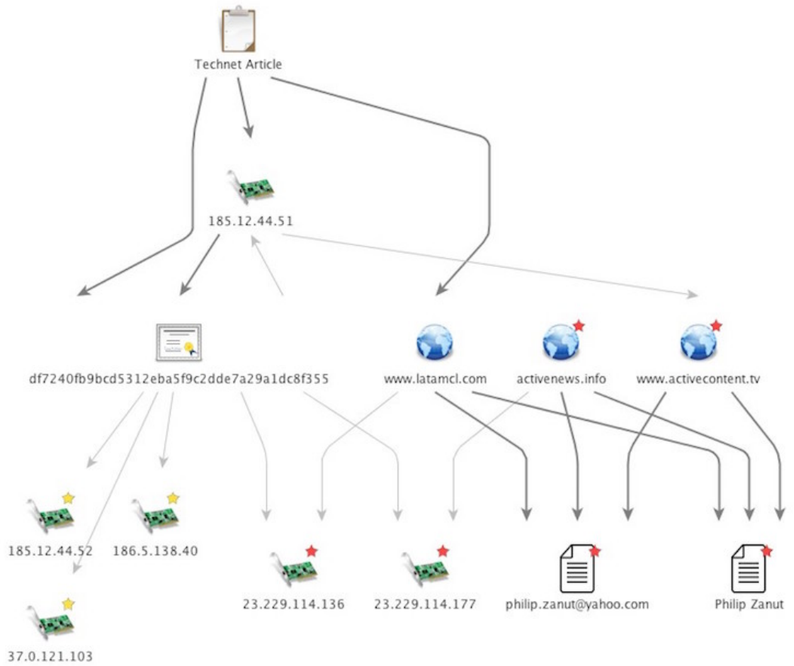
```
TIME:                08/27/2012-18:39:04.064714
SRC IP:              2a01:0e35:1394:5ed0:c147:93c6:8654:70fd
DST IP:              2001:41d0:0001:9598:0000:0000:0000:0001
PROTO:               6
SRC PORT:            53494
DST PORT:            443
TLS SUBJECT:         OU=Domain Control Validated, OU=Gandi Standard SSL, CN=home.regit.org
TLS ISSUERDN:        C=FR, O=GANDI SAS, CN=Gandi Standard SSL CA
TLS FINGERPRINT:     f3:40:21:48:70:2c:31:bc:b5:aa:22:ad:63:d6:bc:2e:b3:46:e2:5a
```

PEM file

```
-----BEGIN CERTIFICATE-----
MIIE2DCCA8CgAwIBAgIQXszObihffqDbQdTwC+ycCjANBgkqhkiG9w0BAQUFADBB
...
3WCiQrY7P56JbvG4jNJ5H4ERj90hQquHj/8Ej39db/MCCmNgjRLVLdVkW4l5DRCe
XX2Ac2xzZtLpVmft7sE3mQauGjW9tgCtpB/fxQqiA+uq+vm1PE37ukscByM=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIEozCCA4ugAwIBAgIQWrYdrB5NogYUx1U9Pamy3DANBgkqhkiG9w0BAQUFADCB
...
8/ifBlIK3se2e4/hEfcEejX/arxbx1BJCHBvlEPNnsdw8dvQbdqP
-----END CERTIFICATE-----
```

Pivoting

Pivoting



https://mpars0ns.github.io/bsidescharm-2016slides/

How can I use suricata?

Install it from scratch

```
## Download and install Suricata
wget "https://www.openinfosecfoundation.org/download/suricata-4.0.3.tar.gz"
tar -xvf suricata-4.0.3.tar.gz
cd suricata-4.0.3
./configure --sysconfdir=/etc --localstatedir=/var
make
make install
make install-conf
mkdir /etc/suricata/rules
mkdir /var/log/suricata/certs

# Copy our config over the default
cp /vagrant/resources/suricata.yaml /etc/suricata/suricata.yaml
```

How to draw an owl

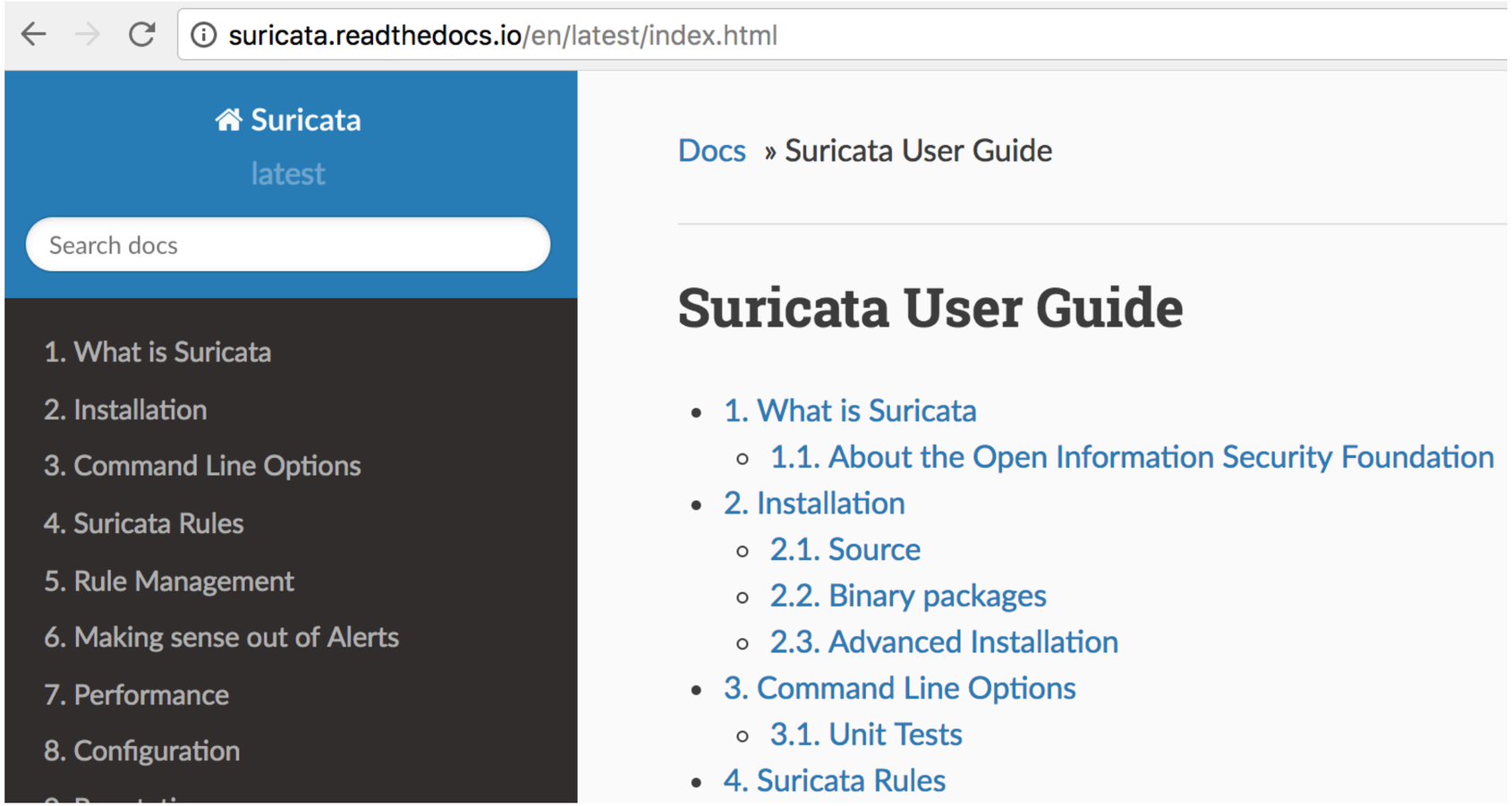
1.

2.

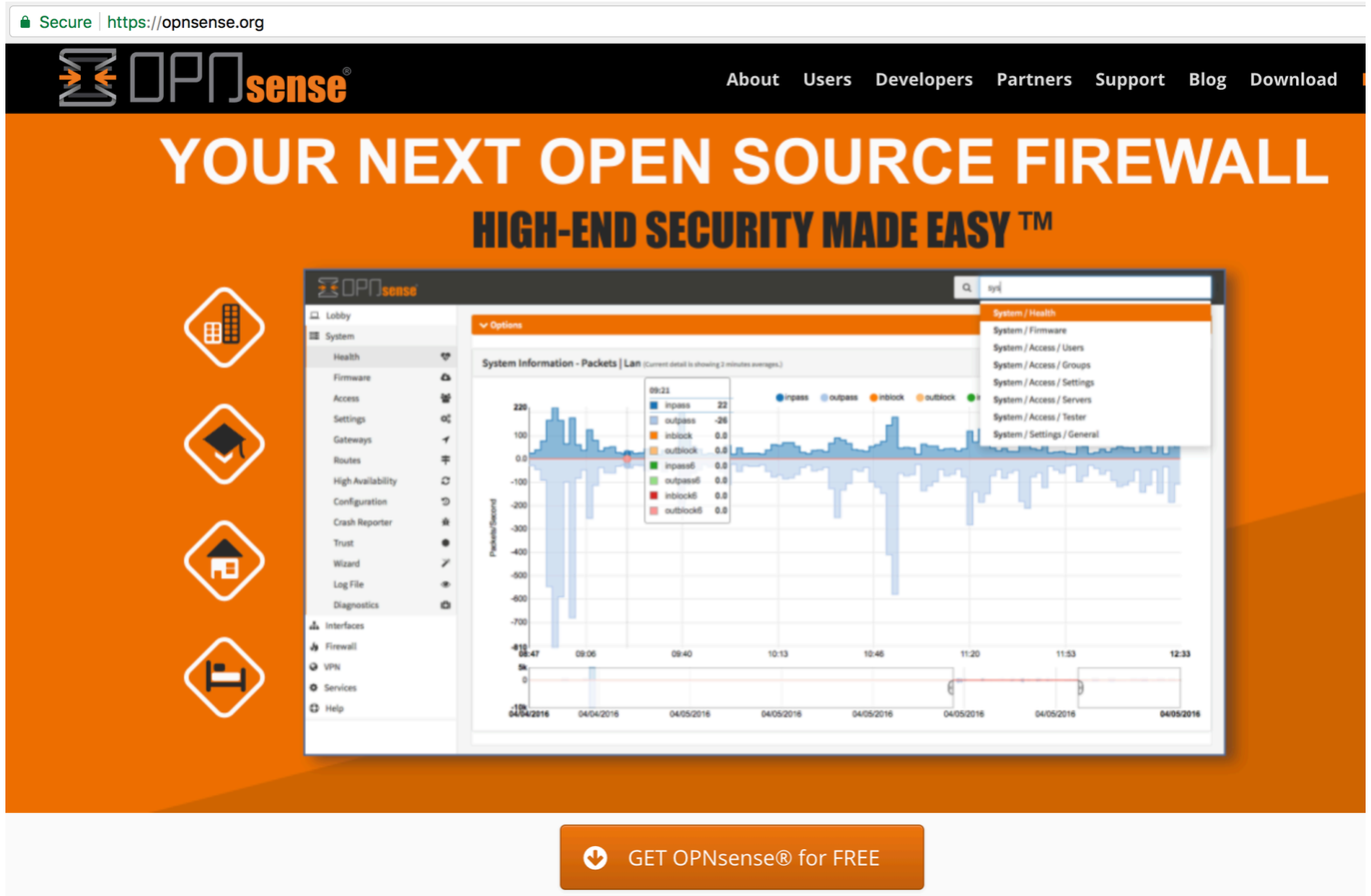
1. Draw some circles

2. Draw the rest of the ducking owl

Works great on Ubuntu



OpnSense


Secure | https://opnsense.org
OPNsense
About Users Developers Partners Support Blog Download
YOUR NEXT OPEN SOURCE FIREWALL
HIGH-END SECURITY MADE EASY ™
GET OPNsense® for FREE

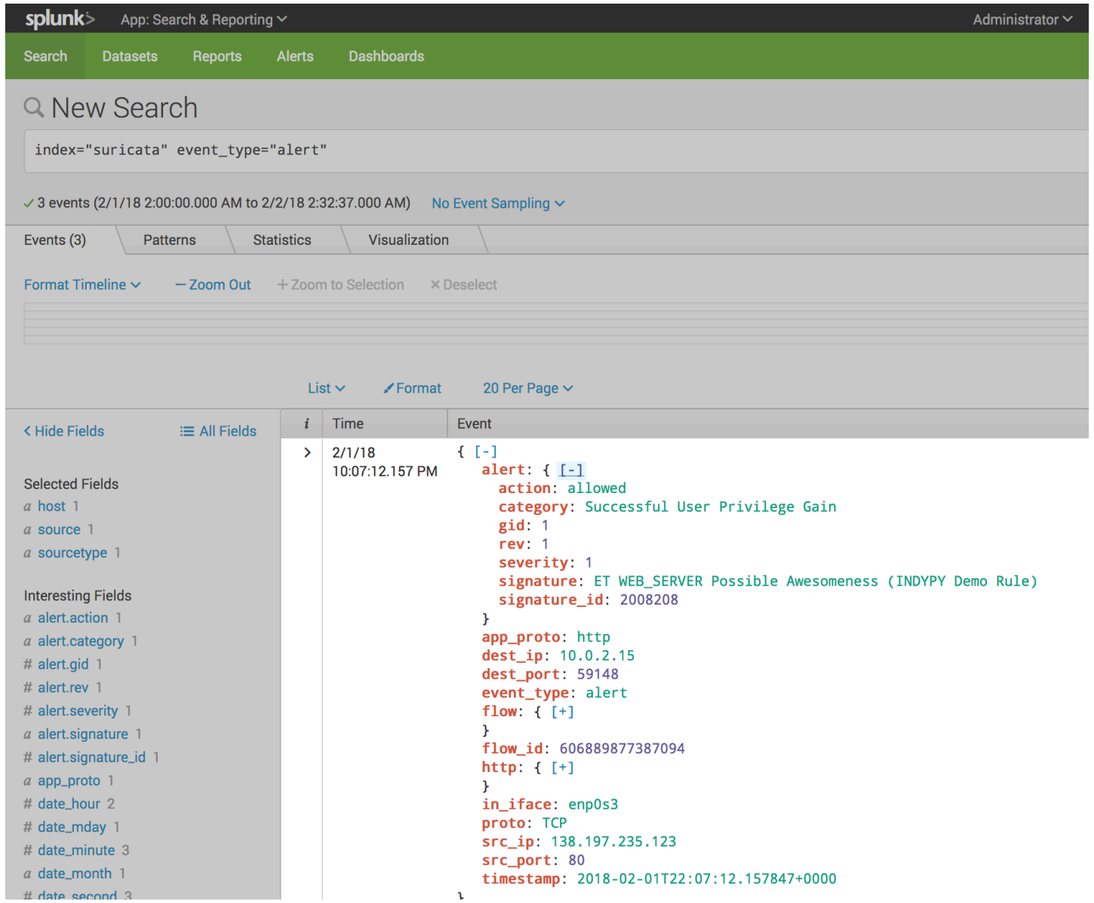
Stamus Network

How do I **use** the data that comes out?

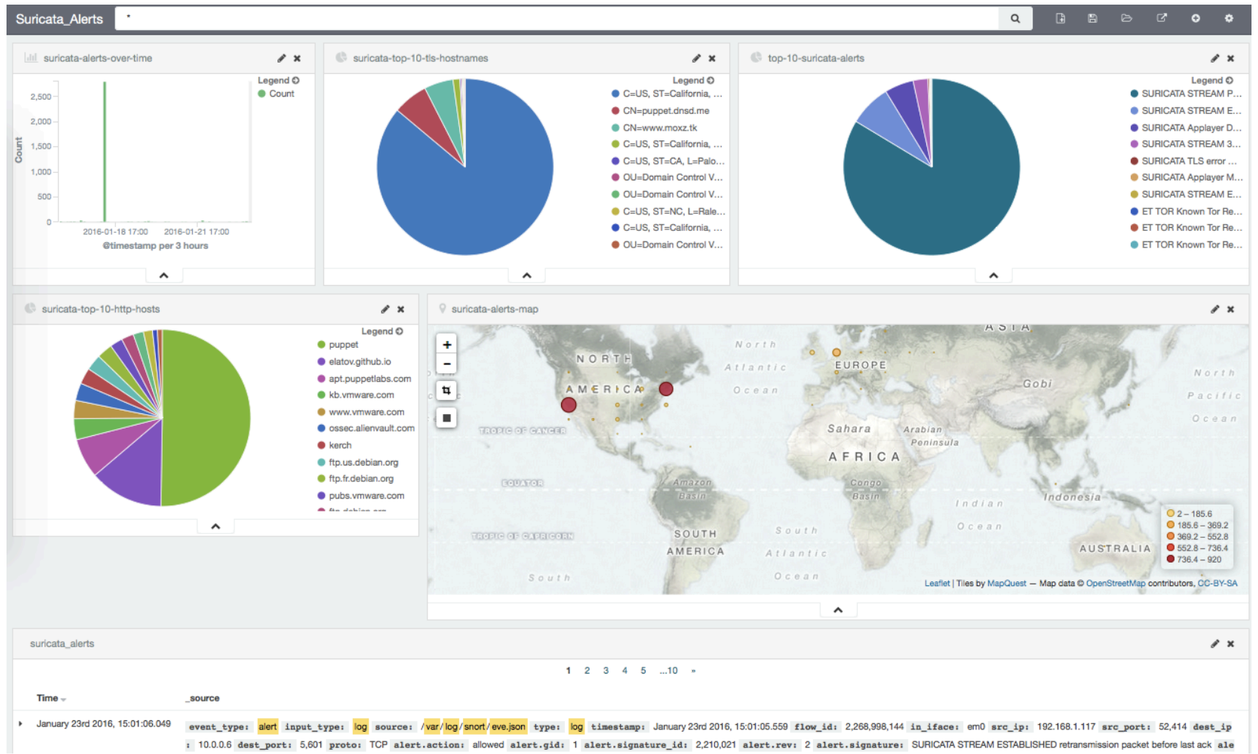
SIEM -- Security information and event management

- Data aggregation
- Correlation
- Alerting
- Dashboards
- Compliance
- Forensic analysis

Splunk

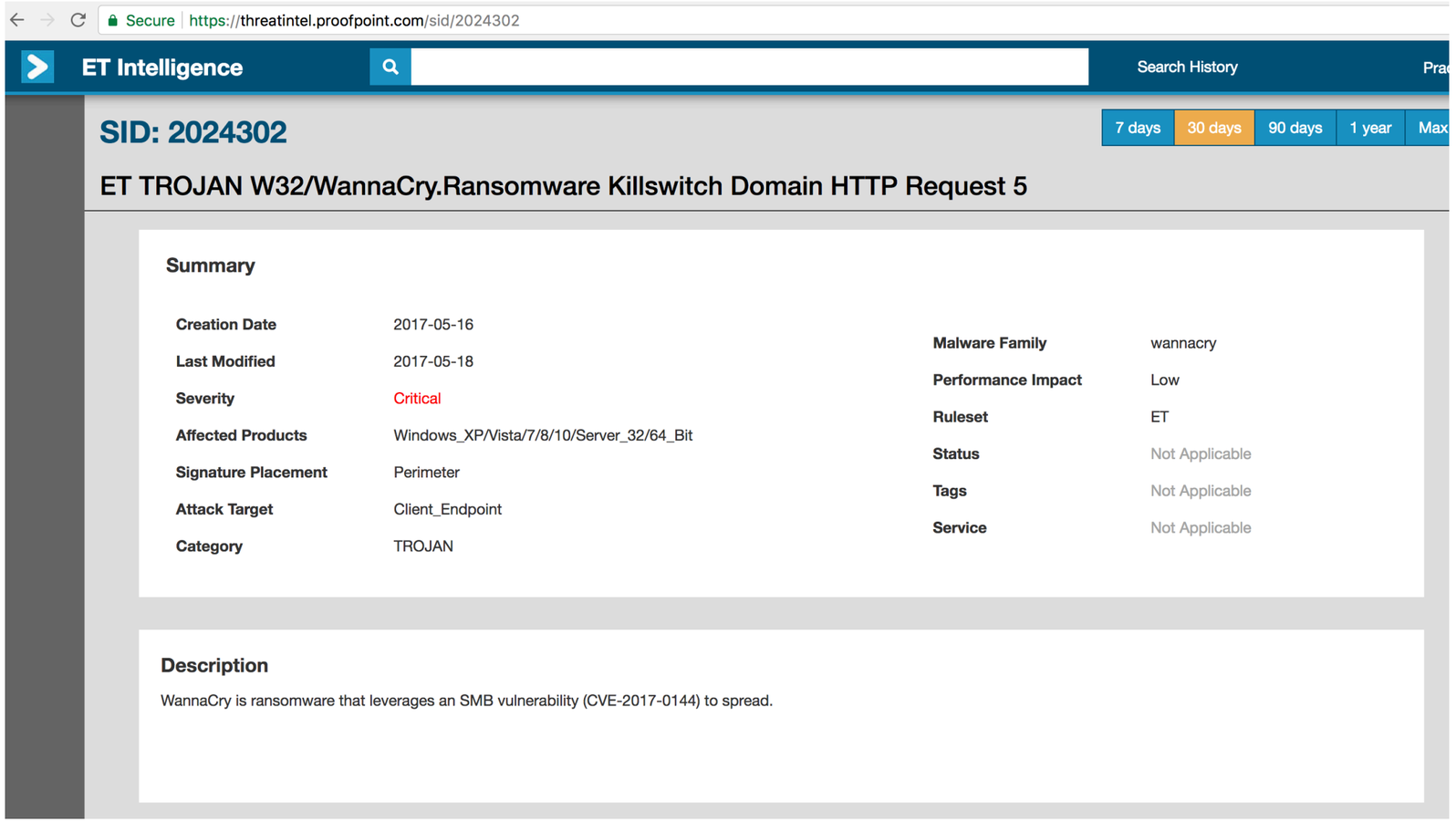

splunk> App: Search & Reporting
Administrator
Search
Datasets
Reports
Alerts
Dashboards
New Search
index="suricata" event_type="alert"
3 events (2/1/18 2:00:00.000 AM to 2/2/18 2:32:37.000 AM)
No Event Sampling
Events (3)
Patterns
Statistics
Visualization
Format Timeline
Zoom Out
Zoom to Selection
Deselect
List
Format
20 Per Page
Hide Fields
All Fields
Selected Fields
a host 1
a source 1
a sourcetype 1
Interesting Fields
a alert.action 1
a alert.category 1
alert.gid 1
alert.rev 1
alert.severity 1
a alert.signature 1
alert.signature_id 1
a app_proto 1
date_hour 2
date_mday 1
date_minute 3
a date_month 1
date_second 3
i
Time
Event
2/1/18
10:07:12.157 PM
{ [-]
alert: { [-]
action: allowed
category: Successful User Privilege Gain
gid: 1
rev: 1
severity: 1
signature: ET WEB_SERVER Possible Awesomeness (INDYPY Demo Rule)
signature_id: 2008208
}
app_proto: http
dest_ip: 10.0.2.15
dest_port: 59148
event_type: alert
flow: { [+]
}
flow_id: 606889877387094
http: { [+]
}
in_iface: enp0s3
proto: TCP
src_ip: 138.197.235.123
src_port: 80
timestamp: 2018-02-01T22:07:12.157847+0000
}

ELK stack



http://elatov.github.io/2016/04/suricata-logs-in-splunk-and-elk/

threatIntel.proofpoint.com



To learn more

Suricata download -- https://suricata-ids.org

Suricata Events (training) -- https://oisf.net

OpnSense appliance -- https://opnsense.org

Thank you

Slide deck

github.com/indypy/PythologyFeb2018