AI for detection of threats from the darkweb

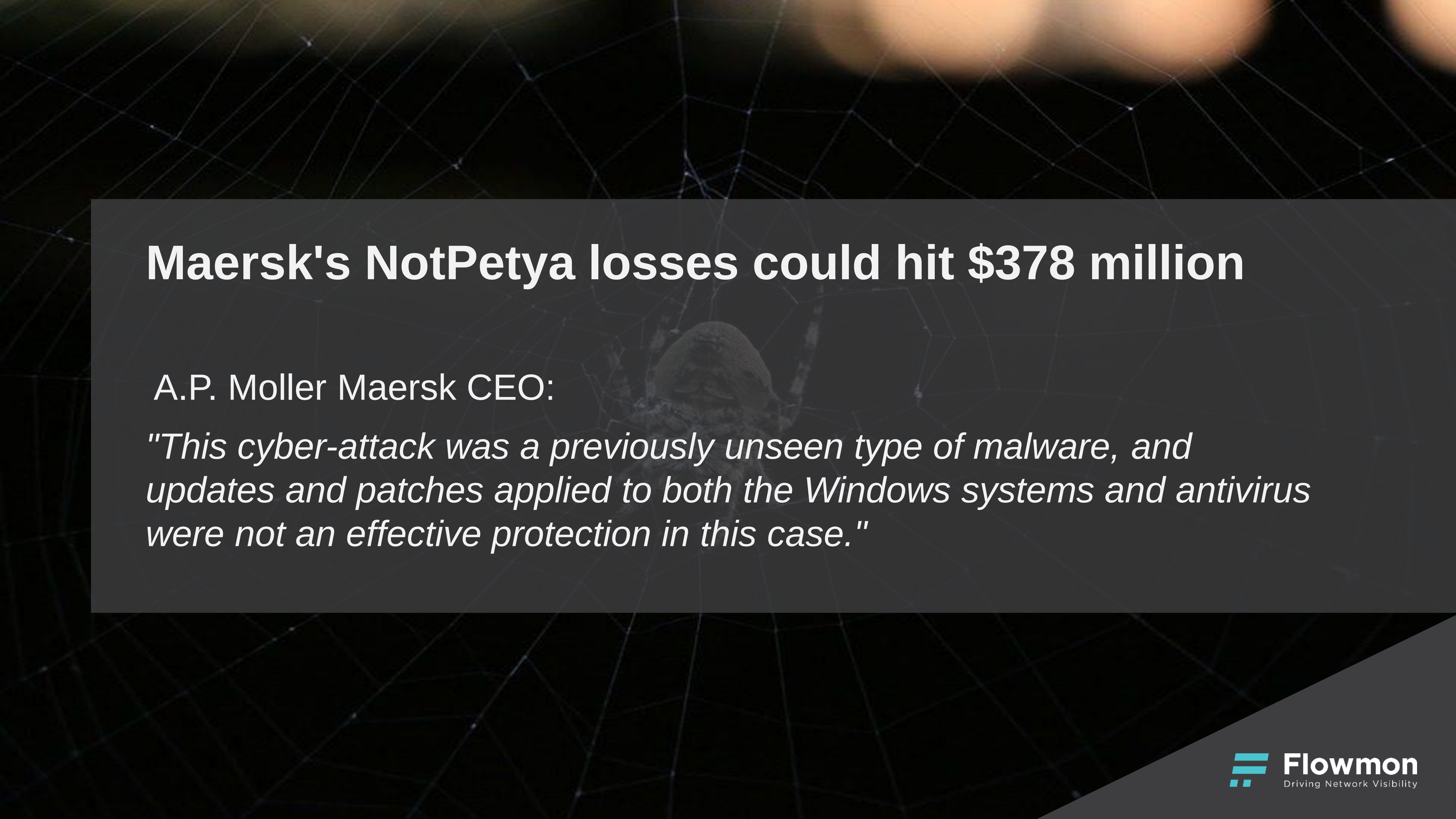
Tempest Judgment Day, 9th November 2017

Roman Cupka, Country Manager SEE

Artur Kane, Technology Evangelist

Flowmon

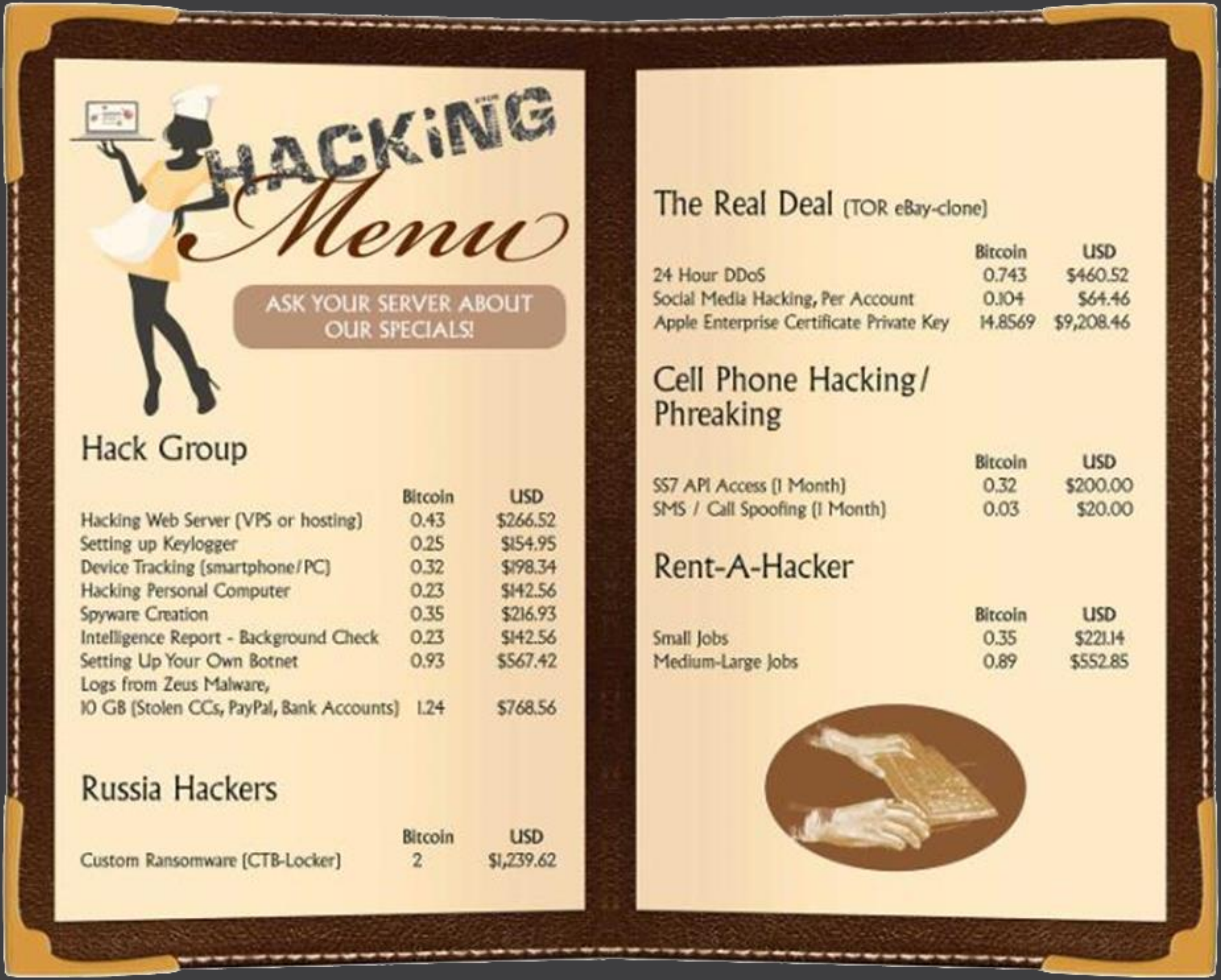
Driving Network Visibility



Maersk's NotPetya losses could hit $378 million

A.P. Moller Maersk CEO:

"This cyber-attack was a previously unseen type of malware, and updates and patches applied to both the Windows systems and antivirus were not an effective protection in this case."



HACKiNG Menu

ASK YOUR SERVER ABOUT OUR SPECIALS!

Hack Group

	Bitcoin	USD
Hacking Web Server (VPS or hosting)	0.43	$266.52
Setting up Keylogger	0.25	$154.95
Device Tracking (smartphone/PC)	0.32	$198.34
Hacking Personal Computer	0.23	$142.56
Spyware Creation	0.35	$216.93
Intelligence Report - Background Check	0.23	$142.56
Setting Up Your Own Botnet	0.93	$567.42
Logs from Zeus Malware, 10 GB (Stolen CCs, PayPal, Bank Accounts)	1.24	$768.56

Russia Hackers

	Bitcoin	USD
Custom Ransomware (CTB-Locker)	2	$1,239.62

The Real Deal (TOR eBay-clone)

	Bitcoin	USD
24 Hour DDoS	0.743	$460.52
Social Media Hacking, Per Account	0.104	$64.46
Apple Enterprise Certificate Private Key	14.8569	$9,208.46

Cell Phone Hacking/ Phreaking

	Bitcoin	USD
SS7 API Access (1 Month)	0.32	$200.00
SMS / Call Spoofing (1 Month)	0.03	$20.00

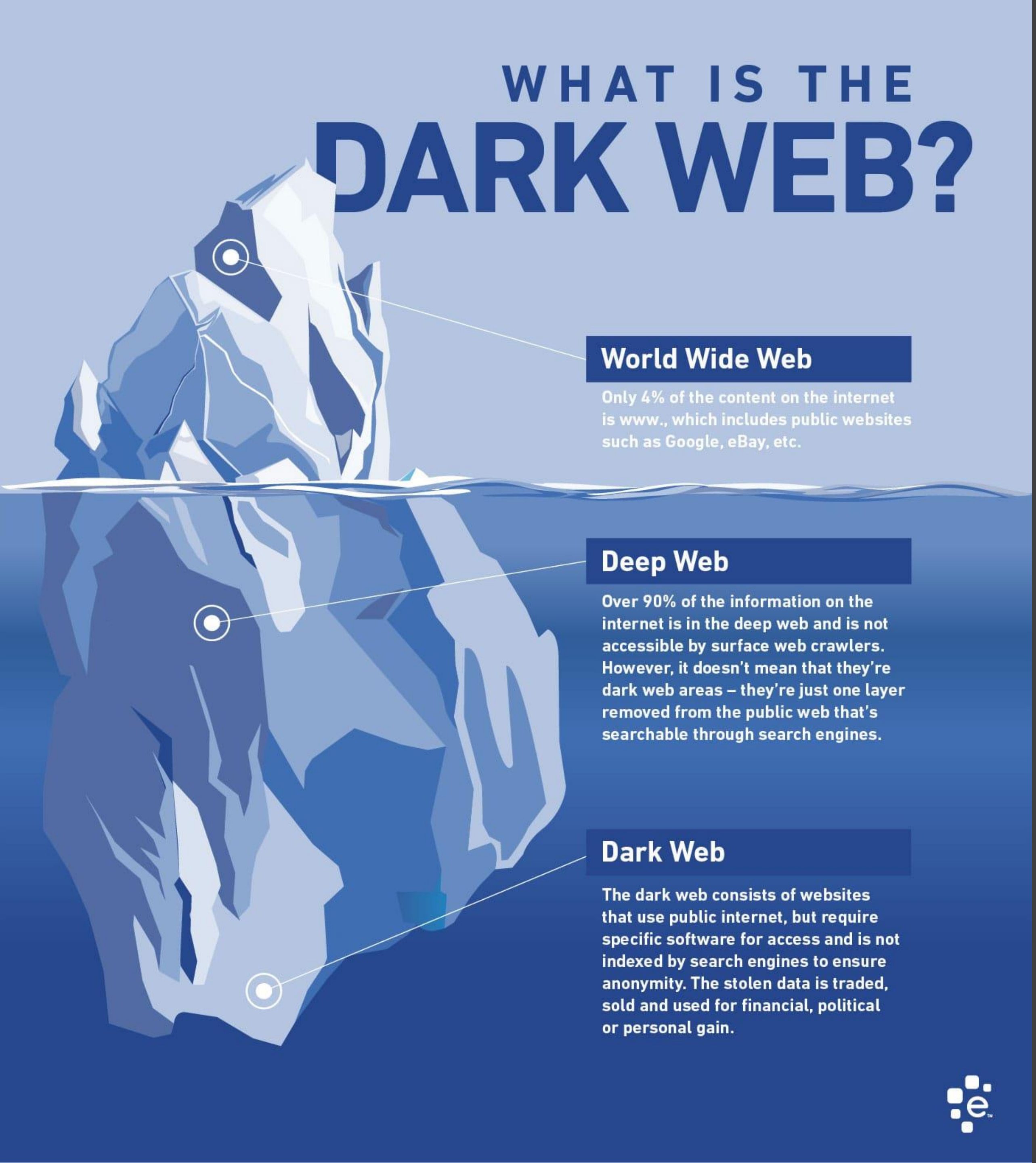
Rent-A-Hacker

	Bitcoin	USD
Small Jobs	0.35	$221.14
Medium-Large Jobs	0.89	$552.85

Marc Laliberte, Information Threat Analyst at WatchGuard

“Using a botnet in order to target companies to take them offline, stealing intellectual property and intentionally damaging hardware or software sound like complicated undertakings to most people. And they are. But they've never been more accessible.”

“Ultimately, crimeware-as-a-service (CaaS) offerings like these make it much easier for less technically sophisticated individuals to gain access to fairly sophisticated computer and network attacks – they lower the barrier to entry significantly for cybercriminals.“



WHAT IS THE DARK WEB?

World Wide Web

Only 4% of the content on the internet is www., which includes public websites such as Google, eBay, etc.

Deep Web

Over 90% of the information on the internet is in the deep web and is not accessible by surface web crawlers. However, it doesn't mean that they're dark web areas – they're just one layer removed from the public web that's searchable through search engines.

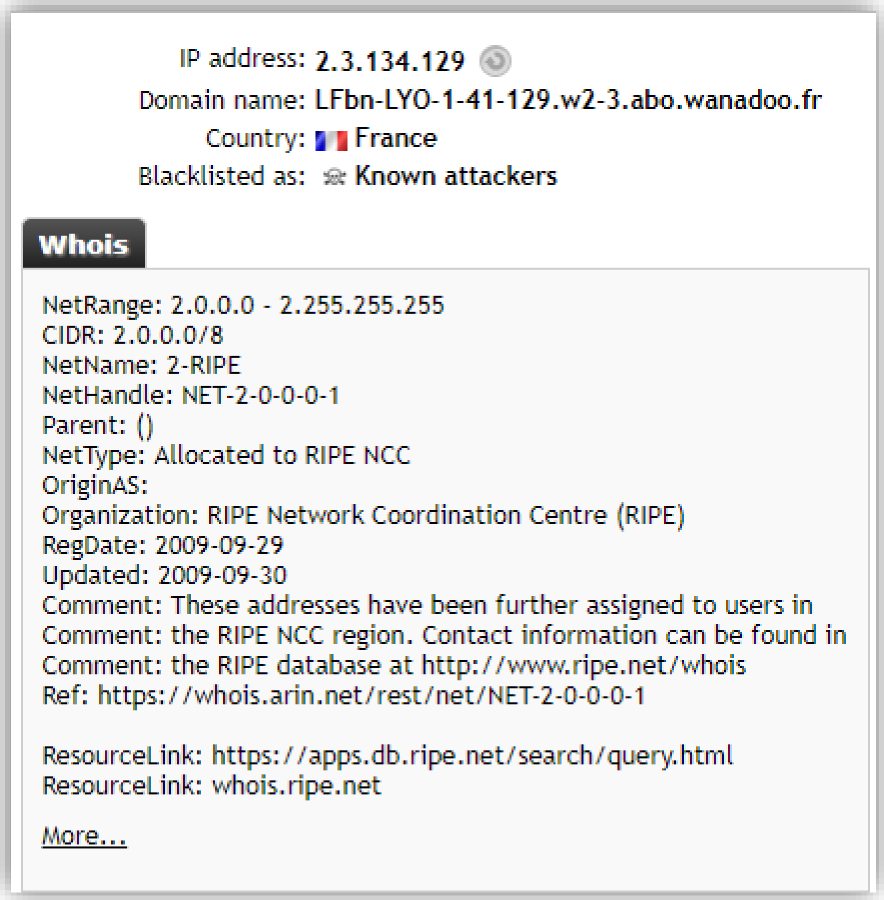
Dark Web

The dark web consists of websites that use public internet, but require specific software for access and is not indexed by search engines to ensure anonymity. The stolen data is traded, sold and used for financial, political or personal gain.

The Dark Web

is an encrypted computer network that exists between TOR (The Onion Router) servers and their clients. It is a place for various illegal activities, from the sale of drugs and weapons, to the cyber-attacks.

Flowmon
Driving Network Visibility



IP address: 2.3.134.129

Domain name: LFbn-LYO-1-41-129.w2-3.abo.wanadoo.fr

Country: France

Blacklisted as: Known attackers

```
NetRange: 2.0.0.0 - 2.255.255.255
CIDR: 2.0.0.0/8
NetName: 2-RIPE
NetHandle: NET-2-0-0-0-1
Parent: ()
NetType: Allocated to RIPE NCC
OriginAS:
Organization: RIPE Network Coordination Centre (RIPE)
RegDate: 2009-09-29
Updated: 2009-09-30
Comment: These addresses have been further assigned to users in
Comment: the RIPE NCC region. Contact information can be found in
Comment: the RIPE database at http://www.ripe.net/whois
Ref: https://whois.arin.net/rest/net/NET-2-0-0-0-1

ResourceLink: https://apps.db.ripe.net/search/query.html
ResourceLink: whois.ripe.net
```

It’s easy to start detecting TOR

Use Blacklists that are fairly up-to-date

Market places and cryptocurrencies

Early Bitcoin developer Amir Taaki:

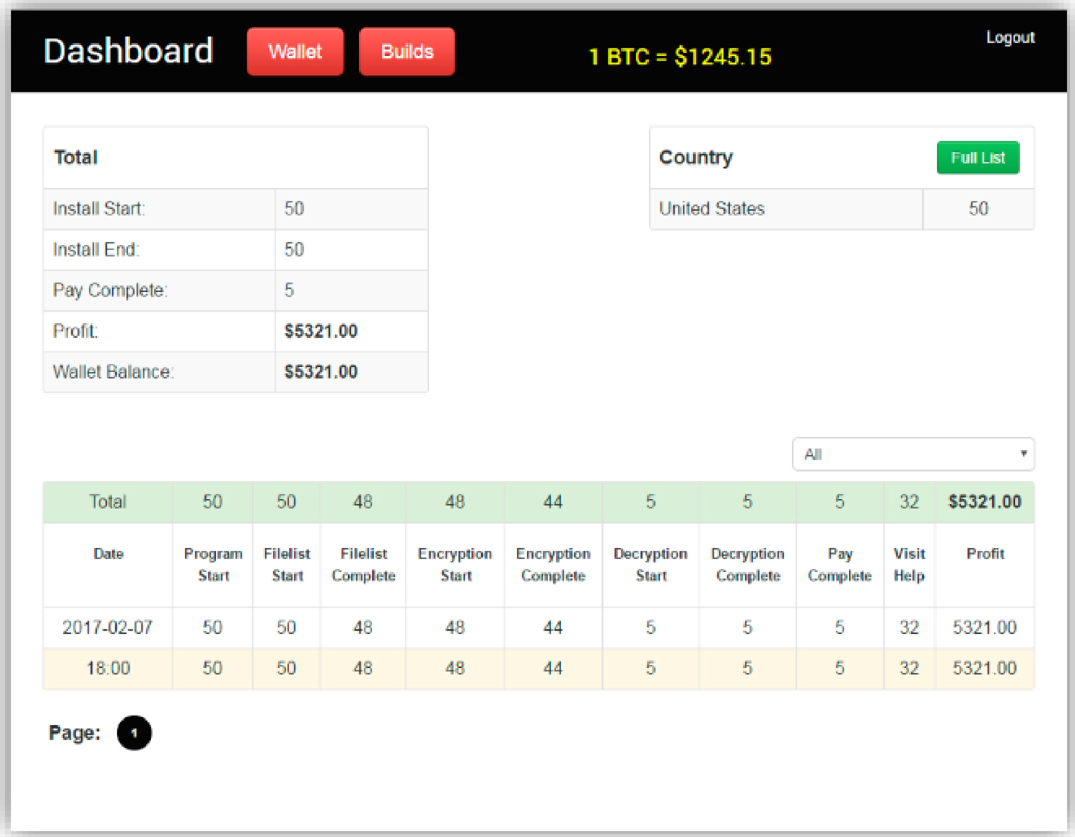
“I would argue that a big reason why Bitcoin became so cool and became so interesting was because of drug markets. Bitcoin did not get where it is because people could buy coffee or buy socks off the Internet. It got to where it is because it was seen as a potent weapon that people could actually use to thrust forward their politics and their ideology.”

It is a dangerous business

A Canadian man who was found hanged in a cell at the Narcotics Suppression Bureau headquarters in Bangkok was the admin the world's largest marketplace on the Dark Web, it has been claimed.

It had been dubbed “the new Silk Road”, and was typically only accessible via special software or secret domains.

http://www.nationmultimedia.com/detail/breakingnews/30320753



1 BTC = $1245.15

Total	
Install Start:	50
Install End:	50
Pay Complete:	5
Profit:	**$5321.00**
Wallet Balance:	**$5321.00**

Country	Full List
United States	50

All

Total	50	50	48	48	44	5	5	5	32	**$5321.00**
Date	Program Start	Filelist Start	Filelist Complete	Encryption Start	Encryption Complete	Decryption Start	Decryption Complete	Pay Complete	Visit Help	Profit
2017-02-07	50	50	48	48	44	5	5	5	32	5321.00
18.00	50	50	48	48	44	5	5	5	32	5321.00

Page: 1

The Fatboy ransomware is dynamic in the way it targets its victims; the amount of *ransom demanded* is determined *by the victim’s location*.

According to a member of a top-tier Russian cyber criminal forum “polnowz”, Fatboy uses a *payment* scheme *based on The economist’s Big Mac Index*(cited as the “McDonald’s Index” in the product description), meaning that victims in areas with a higher cost of living will be charged more to have their data decrypted.

Did you hear about EternalRocks?

This worm, dubbed EternalRocks *uses seven leaked NSA hacking tools* to infect a computer via SMB ports exposed online. WannaCry used just one.

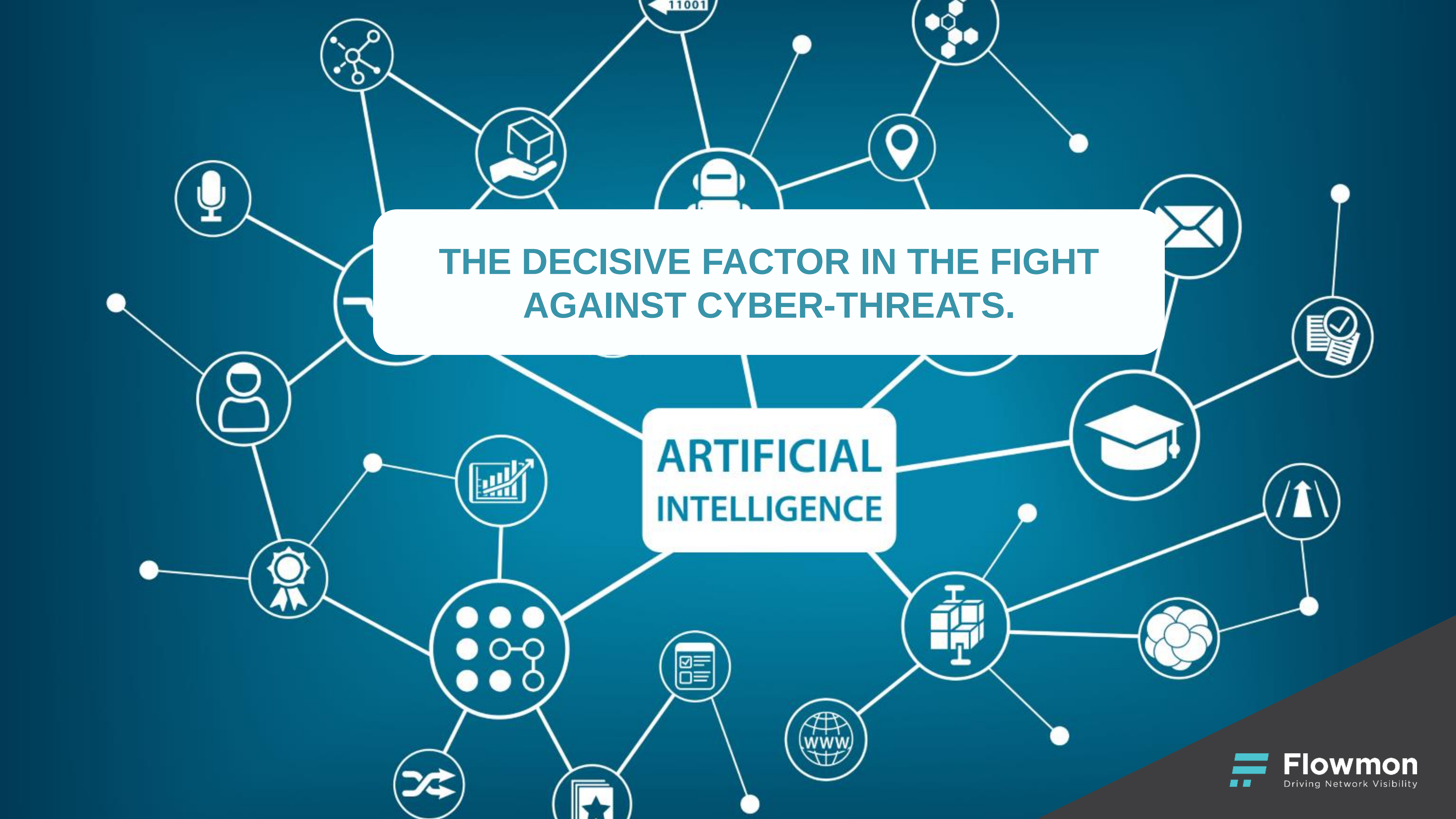
Flowmon
Driving Network Visibility

Early detection and response is mandatory

Artificial Intelligence and Machine Learning

Signature based detection is like border control – you aren’t on a blacklist, you may pass

THE DECISIVE FACTOR IN THE FIGHT AGAINST CYBER-THREATS.



Using data from airport surveillance, Anomaly Detection is a brain with capability to detect suspicious behavior of an unknown attacker anywhere, anytime, real-time.

Attacks

port scanning, dictionary attacks, DoS, DDoS, Telnet

Traffic anomalies

DNS, DHCP, ICMP. multicast

Internal security

viruses, malware, ransomware, botnets, data leaking

Unwanted applications

P2P networks, instant messaging, anonymization services

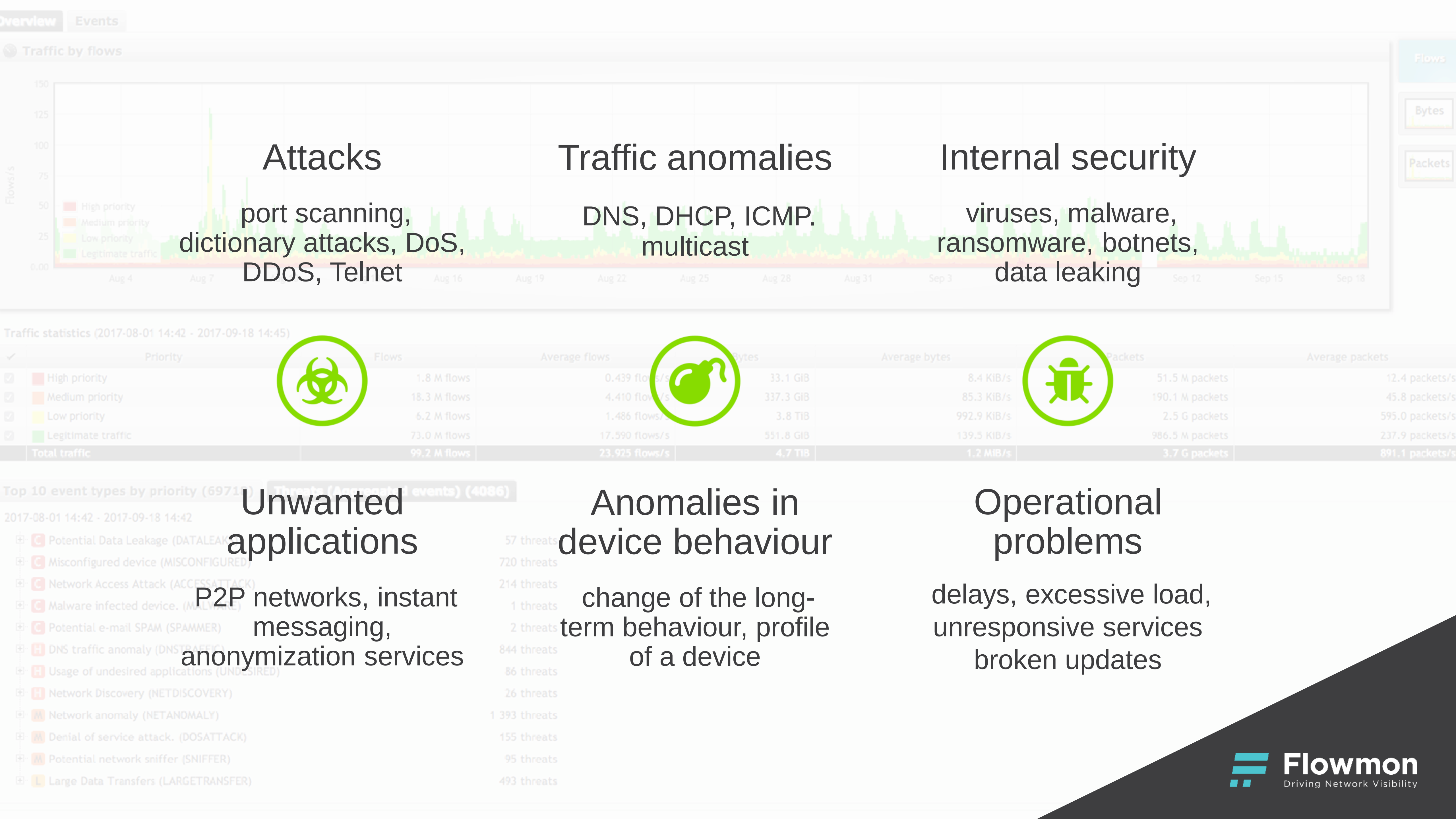
Anomalies in device behaviour

change of the long-term behaviour, profile of a device

Operational problems

delays, excessive load, unresponsive services broken updates

Flowmon
Driving Network Visibility



Traffic statistics (2017-08-01 14:42 - 2017-09-18 14:45)

Priority	Flows	Average flows	Bytes	Average bytes	Packets	Average packets
☑ 🟥 High priority	1.8 M flows	0.439 flows/s	33.1 GiB	8.4 KiB/s	51.5 M packets	12.4 packets/s
☑ 🟧 Medium priority	18.3 M flows	4.410 flows/s	337.3 GiB	85.3 KiB/s	190.1 M packets	45.8 packets/s
☑ 🟨 Low priority	6.2 M flows	1.486 flows/s	3.8 TiB	992.9 KiB/s	2.5 G packets	595.0 packets/s
☑ 🟩 Legitimate traffic	73.0 M flows	17.590 flows/s	551.8 GiB	139.5 KiB/s	986.5 M packets	237.9 packets/s
Total traffic	99.2 M flows	23.925 flows/s	4.7 TiB	1.2 MiB/s	3.7 G packets	891.1 packets/s

Top 10 event types by priority (69716) | Threats (Aggregated events) (4086)

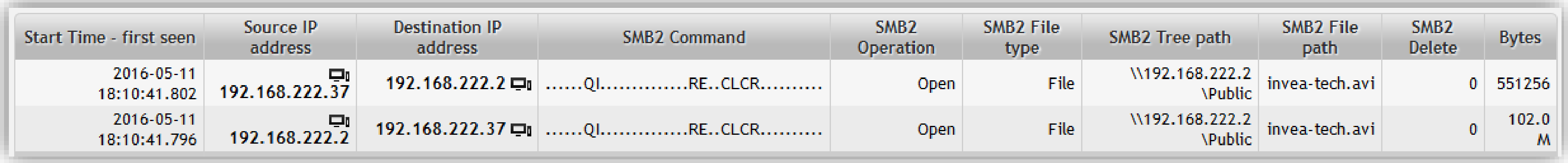
2017-08-01 14:42 - 2017-09-18 14:42

C Potential Data Leakage (DATALEAK	57 threats
C Misconfigured device (MISCONFIGURED)	720 threats
C Network Access Attack (ACCESSATTACK)	214 threats
C Malware infected device. (MALWARE)	1 threats
C Potential e-mail SPAM (SPAMMER)	2 threats
H DNS traffic anomaly (DNSTRAFFIC)	844 threats
H Usage of undesired applications (UNDESIRED)	86 threats
H Network Discovery (NETDISCOVERY)	26 threats
M Network anomaly (NETANOMALY)	1 393 threats
M Denial of service attack. (DOSATTACK)	155 threats
M Potential network sniffer (SNIFFER)	95 threats
L Large Data Transfers (LARGETRANSFER)	493 threats

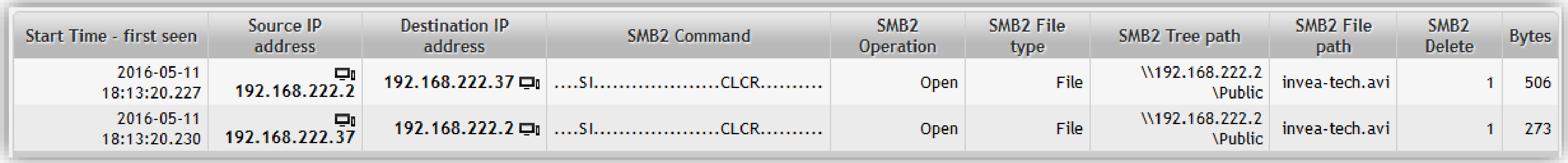
Indicators of Compromise

- After initial compromise, malware **communicates over the network**
- Malware activity represents **anomalies** and can be detected
  - Port Scanning, dictionary attacks
  - Tunneling, protocol anomalies
  - Rouge DHCP or DNS server
  - High uploads
  - TOR traffic, P2P communications
  - Communications with blacklisted hosts
- Malware tries to be **undetected**
  - Low volumes of network traffic
  - Detected only by the right technology & tools

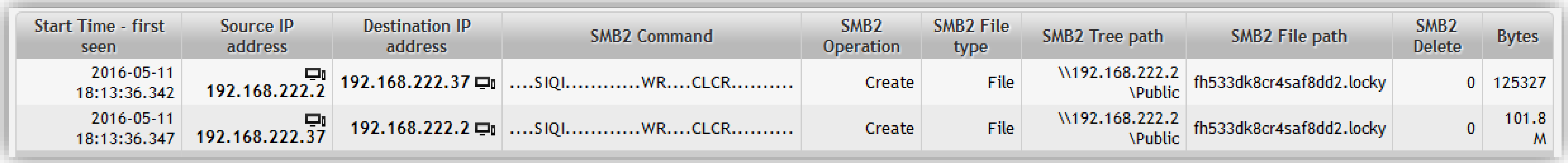
What ransomware does in the network



Start Time - first seen	Source IP address	Destination IP address	SMB2 Command	SMB2 Operation	SMB2 File type	SMB2 Tree path	SMB2 File path	SMB2 Delete	Bytes
2016-05-11 18:10:41.802	192.168.222.37	192.168.222.2	......QI..............RE..CLCR..........	Open	File	\\192.168.222.2 \Public	invea-tech.avi	0	551256
2016-05-11 18:10:41.796	192.168.222.2	192.168.222.37	......QI..............RE..CLCR..........	Open	File	\\192.168.222.2 \Public	invea-tech.avi	0	102.0 M



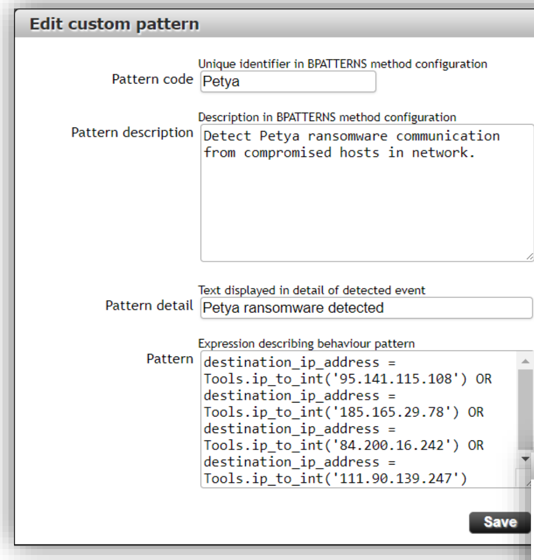
Start Time - first seen	Source IP address	Destination IP address	SMB2 Command	SMB2 Operation	SMB2 File type	SMB2 Tree path	SMB2 File path	SMB2 Delete	Bytes
2016-05-11 18:13:20.227	192.168.222.2	192.168.222.37	....SI....................CLCR..........	Open	File	\\192.168.222.2 \Public	invea-tech.avi	1	506
2016-05-11 18:13:20.230	192.168.222.37	192.168.222.2	....SI....................CLCR..........	Open	File	\\192.168.222.2 \Public	invea-tech.avi	1	273



Start Time - first seen	Source IP address	Destination IP address	SMB2 Command	SMB2 Operation	SMB2 File type	SMB2 Tree path	SMB2 File path	SMB2 Delete	Bytes
2016-05-11 18:13:36.342	192.168.222.2	192.168.222.37	....SIQI............WR....CLCR..........	Create	File	\\192.168.222.2 \Public	fh533dk8cr4saf8dd2.locky	0	125327
2016-05-11 18:13:36.347	192.168.222.37	192.168.222.2	....SIQI............WR....CLCR..........	Create	File	\\192.168.222.2 \Public	fh533dk8cr4saf8dd2.locky	0	101.8 M

1. Copying a file from shared storage onto the infected station
2. Deleting the copied file from the shared storage
3. Uploading encrypted version of the file back

Signature is not necessary



Edit custom pattern

Unique identifier in BPATTERNS method configuration
Pattern code: Petya

Description in BPATTERNS method configuration
Pattern description:

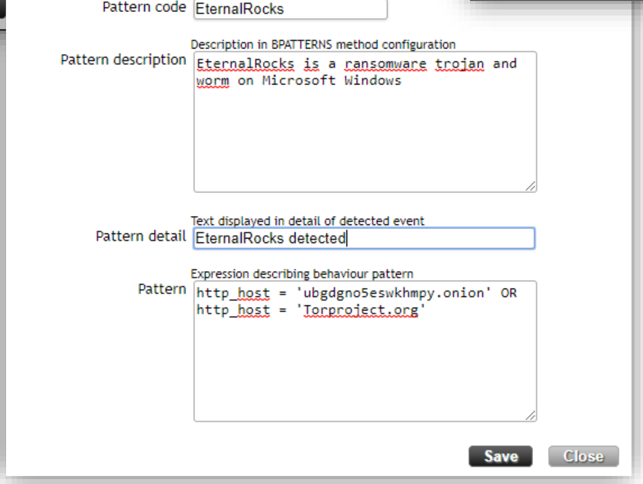
```
Detect Petya ransomware communication
from compromised hosts in network.
```

Text displayed in detail of detected event
Pattern detail: Petya ransomware detected

Expression describing behaviour pattern
Pattern:

```
destination_ip_address =
Tools.ip_to_int('95.141.115.108') OR
destination_ip_address =
Tools.ip_to_int('185.165.29.78') OR
destination_ip_address =
Tools.ip_to_int('84.200.16.242') OR
destination_ip_address =
Tools.ip_to_int('111.90.139.247')
```

Petya



Add new custom pattern

Unique identifier in BPATTERNS method configurat
Pattern code: EternalRocks

Description in BPATTERNS method configuration
Pattern description:

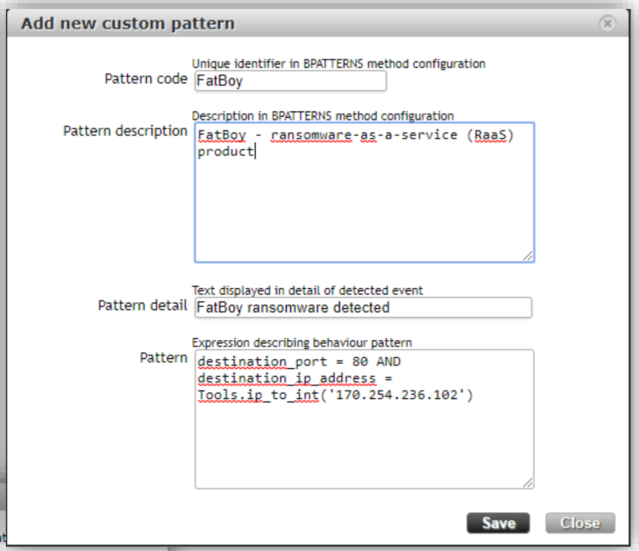
```
EternalRocks is a ransomware trojan and
worm on Microsoft Windows
```

Text displayed in detail of detected event
Pattern detail: EternalRocks detected

Expression describing behaviour pattern
Pattern:

```
http_host = 'ubgdgno5eswkhmpy.onion' OR
http_host = 'Torproject.org'
```

EternalRocks



Add new custom pattern

Unique identifier in BPATTERNS method configuration
Pattern code: FatBoy

Description in BPATTERNS method configuration
Pattern description:

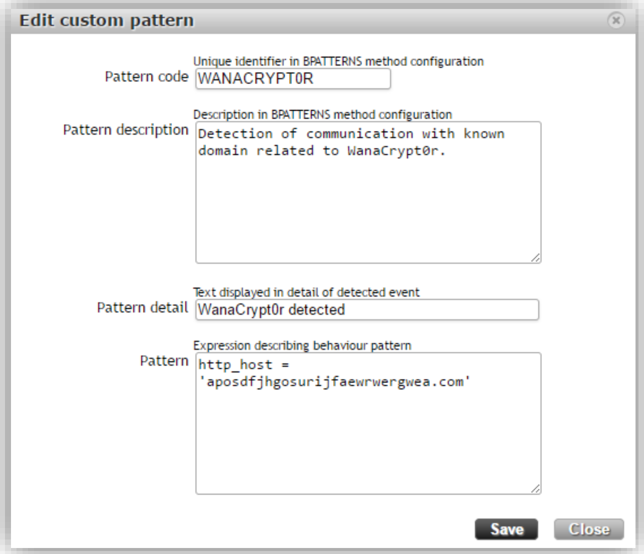
```
FatBoy - ransomware-as-a-service (RaaS)
product
```

Text displayed in detail of detected event
Pattern detail: FatBoy ransomware detected

Expression describing behaviour pattern
Pattern:

```
destination_port = 80 AND
destination_ip_address =
Tools.ip_to_int('170.254.236.102')
```

FatBoy



Edit custom pattern

Unique identifier in BPATTERNS method configuration
Pattern code: WANACRYPT0R

Description in BPATTERNS method configuration
Pattern description:

```
Detection of communication with known
domain related to WanaCrypt0r.
```

Text displayed in detail of detected event
Pattern detail: WanaCrypt0r detected

Expression describing behaviour pattern
Pattern:

```
http_host =
'aposdfjhgosurijfaewrwergwea.com'
```

WannaCry

Flowmon
Driving Network Visibility

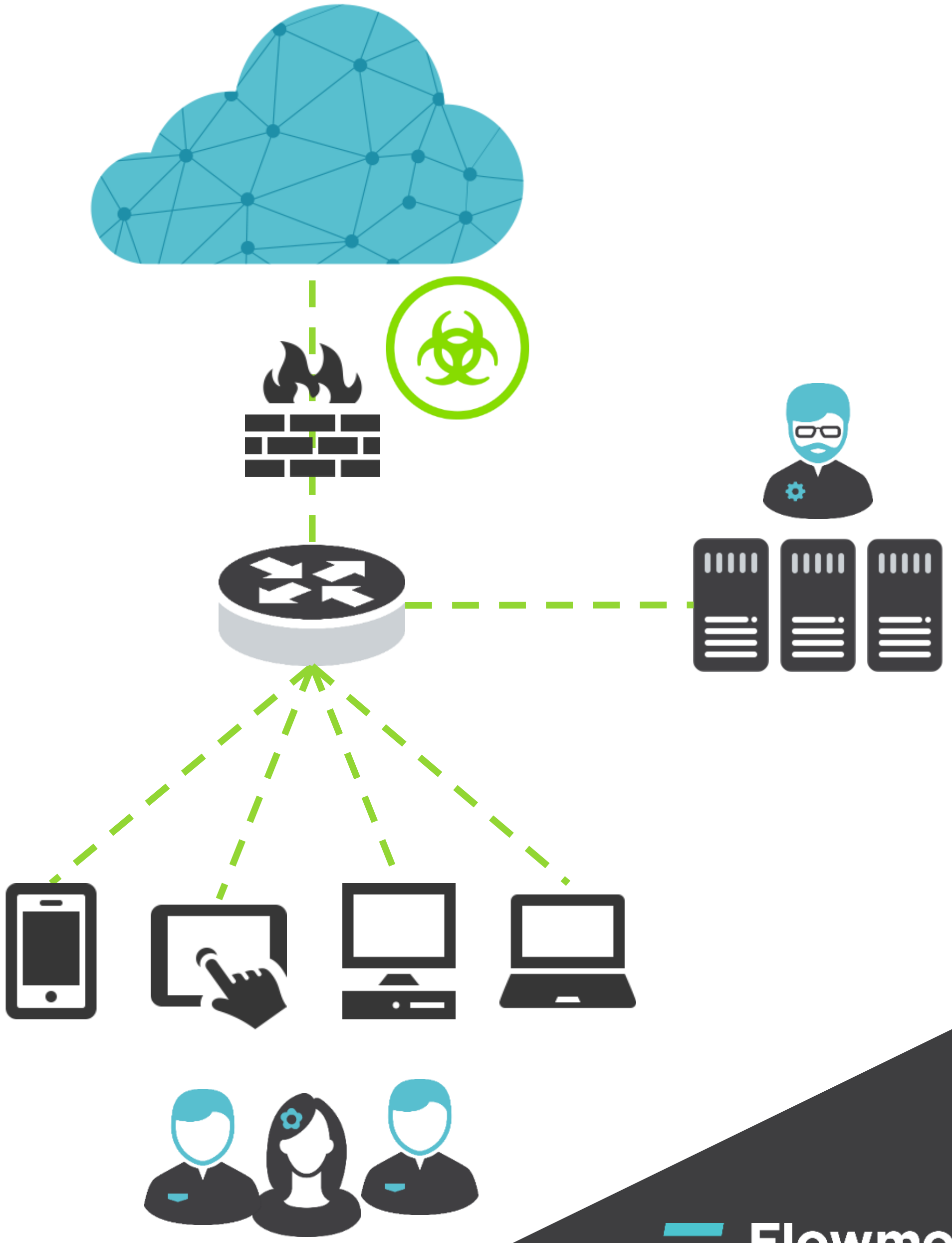
Flow-Based Behavior Patterns

- Detection method designed to unveil rising threats
- Updates new behavior patterns for rising threats
- Provides information about detected event
- Standard event pipeline

Flowmon
Driving Network Visibility

90% OF SECURITY BUDGET IS SPENT ON PERIMETER

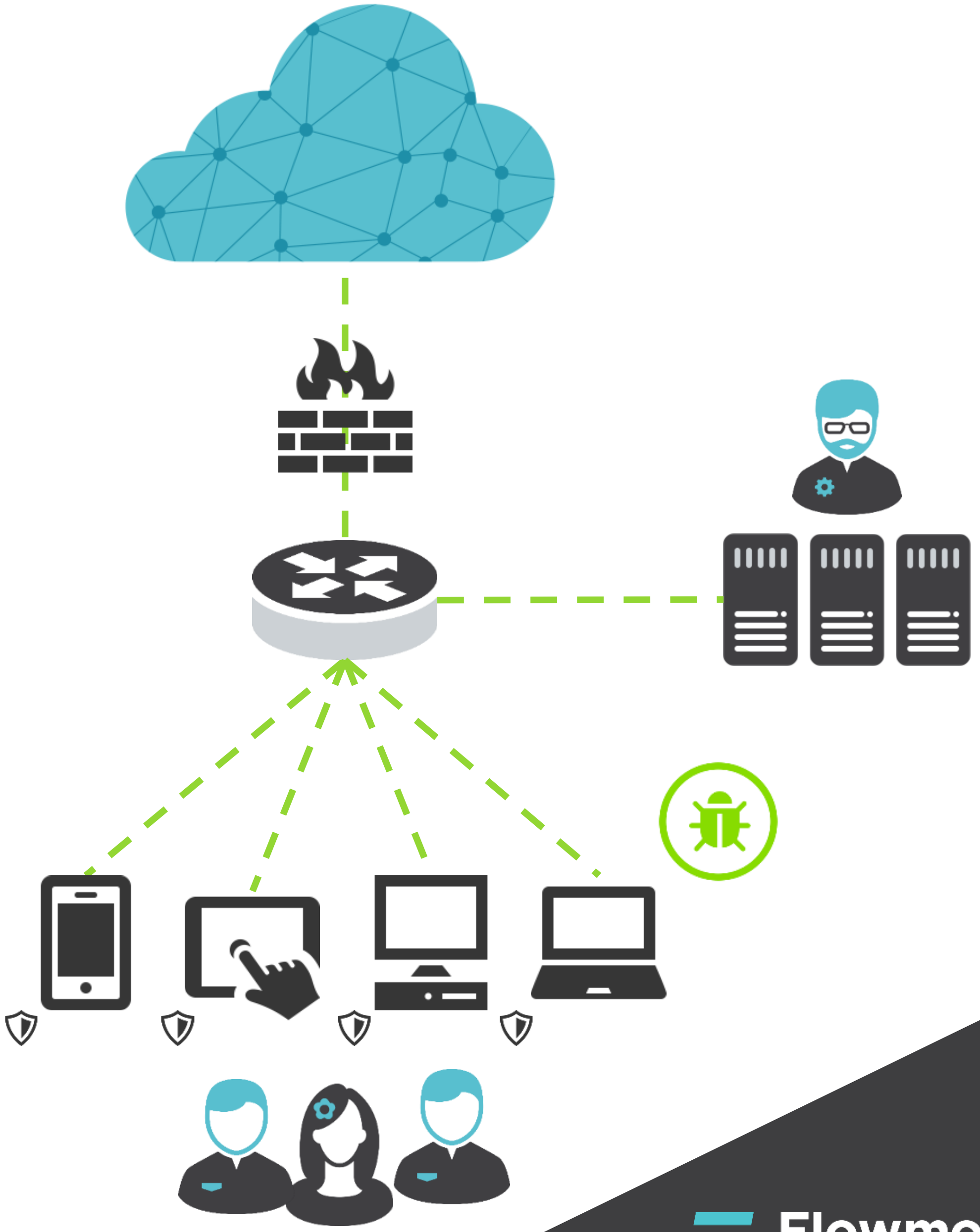
WHILE ONLY 25% TARGET IT INSIDER THREATS ARE THE BIGGEST WORRY



Flowmon
Driving Network Visibility

ANTIVIRUSES SEARCH FOR KNOWN AND DOCUMENTED ATTACKS

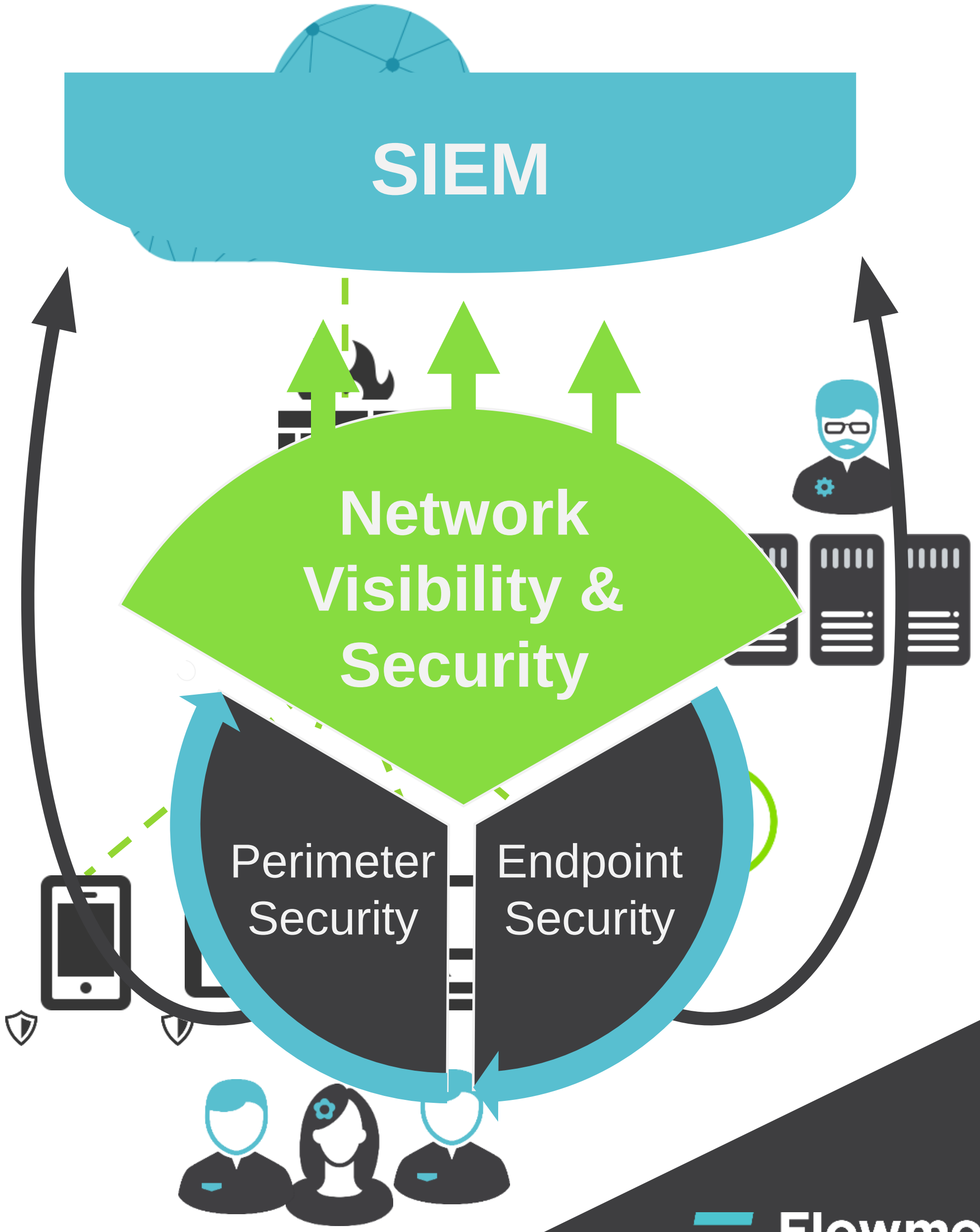
TO DISCOVER AND DOCUMENT A NEW TYPE OF ATTACK MAY TAKE MONTHS



Flowmon
Driving Network Visibility

SIEM's ARE A MUST HAVE BUT THEY ARE ONLY AS STRONG AS THEIR DATA SOURCES

EARLY DETECTION INSIDE LAN, NON-DEPENDENT ON SIGNATURE IS THE MISSING LINK



Flowmon
Driving Network Visibility

Inline vs. Out-of-band

Intrusion prevention systems (IPS)

Firewalls and next-generation firewalls (NGFWs)

Data loss prevention (DLP) systems

Unified threat management (UTM) systems

SSL decryption appliances

Web application firewalls (WAF)

Intrusion detection systems (IDS)

Behavior analysis systems

Forensic tools

Data recording

Packet capture (PCAP) tools

Malware analysis tools

SIEM and Log Management

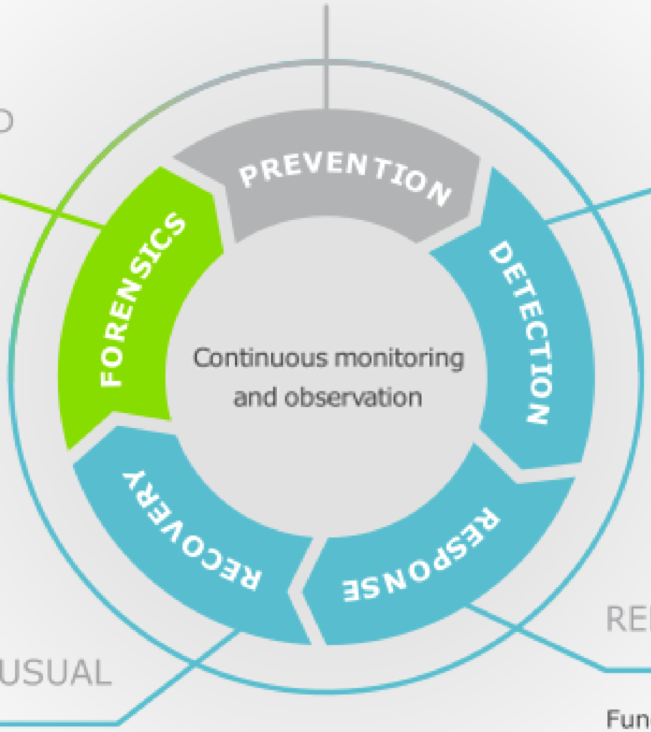
Flowmon
Driving Network Visibility

BUILDING WALLS AND CHECK POINTS

90% of the security budget – mainly perimeter security - where only 25% of attacks target this point in the network.

ENSURING YOUR INVESTMENTS TO PREVENTION DO NOT GO WASTED

Flowmon stores the full statistical history of communication and provides on-demand and auto-triggered recording of detected incidents. It is a reliable source-of-truth and enables you to understand the characteristics of an attack and to discover bottle-necks, predict upcoming attacks and to insure better prevention.



LAYING CLEVER TRAPS

Early detection with Flowmon Anomaly Detection System covers gaps left by standard prevention technologies and represents the people, time, skillset which are lacking to identify a problem before it causes major impacts on company productivity.

RESTORING BUSINESS AS USUAL

Eliminate unnecessary costs on IT operations and insure time-efficient disaster recovery with Flowmon, which helps you to conduct an assessment of the scope of the attack. This includes understanding what parts of the network have been compromised, what needs to be re-installed, recovered, and adjusted. Flowmon enables effective collaboration between all IT teams.

REDUCING MEAN-TIME-TO-RESOLVE

Fundamental network and security tools that many of us already use in day-to-day operations have the capabilities necessary to block or restrict suspicious traffic. Use the whole potential of such technologies you have already implemented with Flowmon to provide a flexible incident response at no additional costs.

Network Information System Security Directive

New EU legislation

Flowmon
Driving Network Visibility

NISD – Network and Information Security Directive

- *The **Directive** on security of network and information systems from **adopted** by the **European Parliament** on **6 July 2016***
- ***Member States (**BG, ES, CS, DA, DE, ET, EL, EN, FR, HR, IT, LV, LT, HU, MT, NL, PL, PT, RO, SK, SL, FI, SV) will have **21 months to transpose** the Directive **into** their **national laws** and **6 months** more to **identify operators** of essential services*
- *The laws and guidelines that have evolved in this area are associated with **safeguarding critical infrastructure** – energy, transport, water, banking, financial market infrastructures, healthcare and digital infrastructure.*

The NIS Directive and National CSIRTs

ENISA looks into the provisions of the upcoming Directive and how it may translate for CSIRTs.

Published on February 26, 2016

Tagged with CSIRT

http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016L1148

NISD – Network and Information Security Directive

- *„Article 14“: **Operators of essential services** are required to **take** “appropriate and proportionate **technical** and **organisational measures** to **manage the risks** posed to the security of network and information systems.*
- ***Requirement** (under penalties) to **report**, **without** undue **delay**, significant **incidents to** a Computer Security Incident Response Team or **CSIRT**.*
- *„Article 16“ **Digital service providers**, which is the EU’s way of saying **ecommerce**, **cloud computing**, and **search services.***
- ***CSIRTs** - **center** of the **NIS Directive**, **collecting incident** data, responsible for **monitoring** and **analyzing threat** activity at a national level, **issuing alerts** and **warnings**, and **sharing** their **information** and threat awareness **with other CSIRTs**.*

The NIS Directive and National CSIRTs

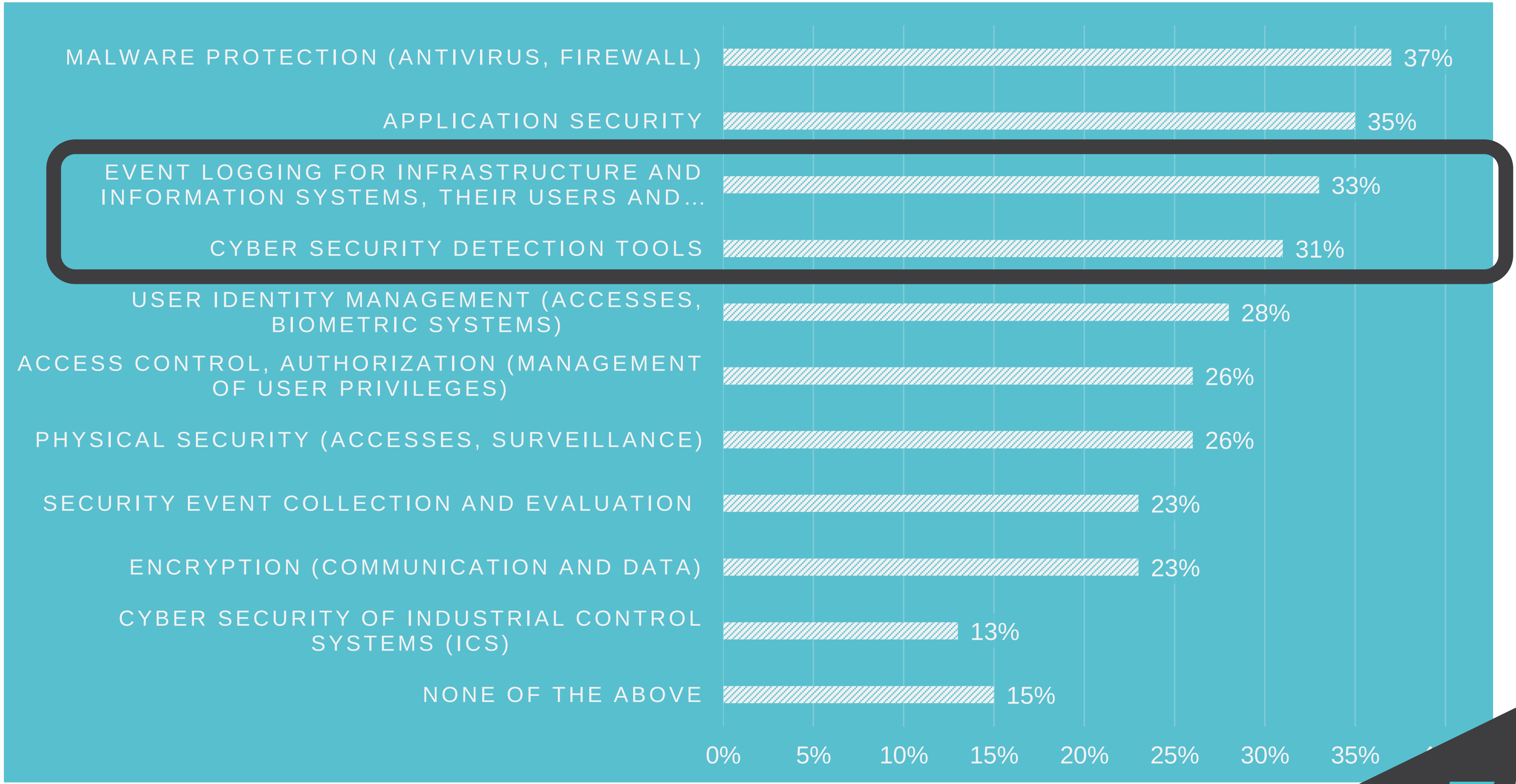
ENISA looks into the provisions of the upcoming Directive and how it may translate for CSIRTs.

Published on February 26, 2016

Tagged with CSIRT

http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016L1148

Planned IT security investments (3-5 years)
Article 14, 16 of NISD (and Article 25, 32, 33, 35 of GDPR) technical measures



GfK Research for Infotrendy 2017

Flowmon
Driving Network Visibility

Thank you

Performance monitoring, visibility and security
with a single solution

Roman Cupka, Country Manager SSE

roman.cupka@flowmon.com, +421 948 464 123

Artur Kane, Technology Evangelist

artur.kane@flowmon.com, +734 754 449

Flowmon Networks a.s.
Sochorova 3232/34
616 00 Brno, Czech Republic
www.flowmon.com