Real-time detection, response and reporting automation of cybersecurity events and incidents

ITAPA 2018, 13-14th Nov

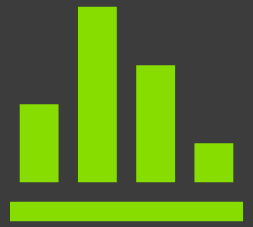
Roman Cupka. Principal Consultant CEE

Flowmon
Driving Network Visibility

Flowmon
Driving Network Visibility

Real-time detection & response

45-250 days in average to detect an incident



Occurs when malfunction of critical service happened (NISD)

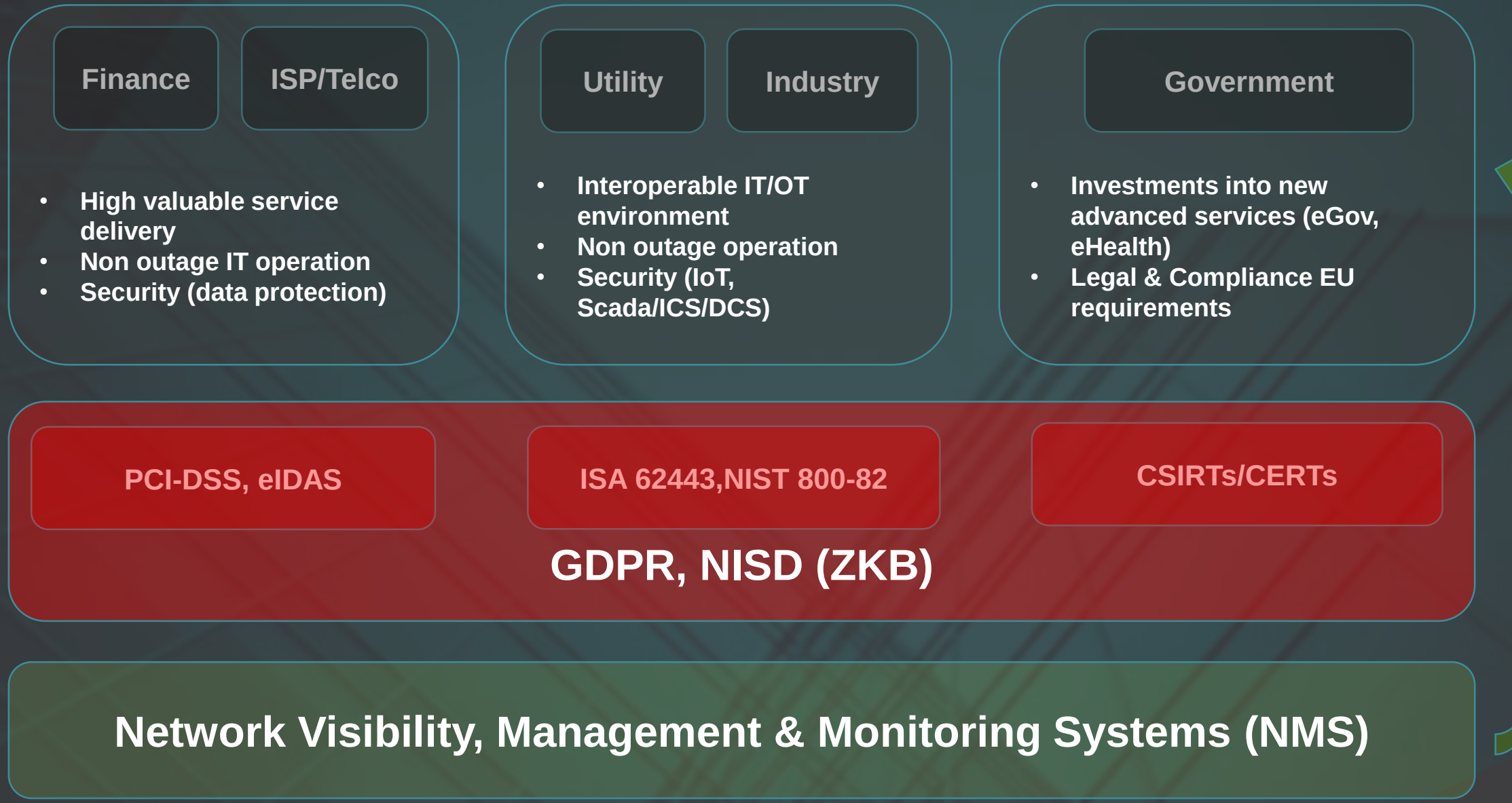
Occurs when sensitive or personal data breach (GDPR)

Detect attack, event or incident in real-time, analyze it in few minutes

Use automation processes for alerting & reporting (3rd parties integration – SIEM etc.)

Classify information automatically (based on manual data predefinition), immediate response

Flowmon
Driving Network Visibility



AGENTLESS & PASSIVE NMS BY FLOWMON

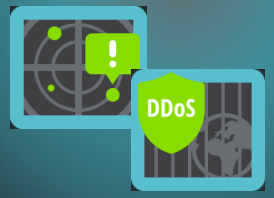
FLOW DATA COLLECTION

ALERTING & REPORTING

DATA ANALYSES (NETWORK, APPLICATIONS & SECURITY)

Security

Early Detection & Response



IT operation

Troubleshooting

IT operation & Security

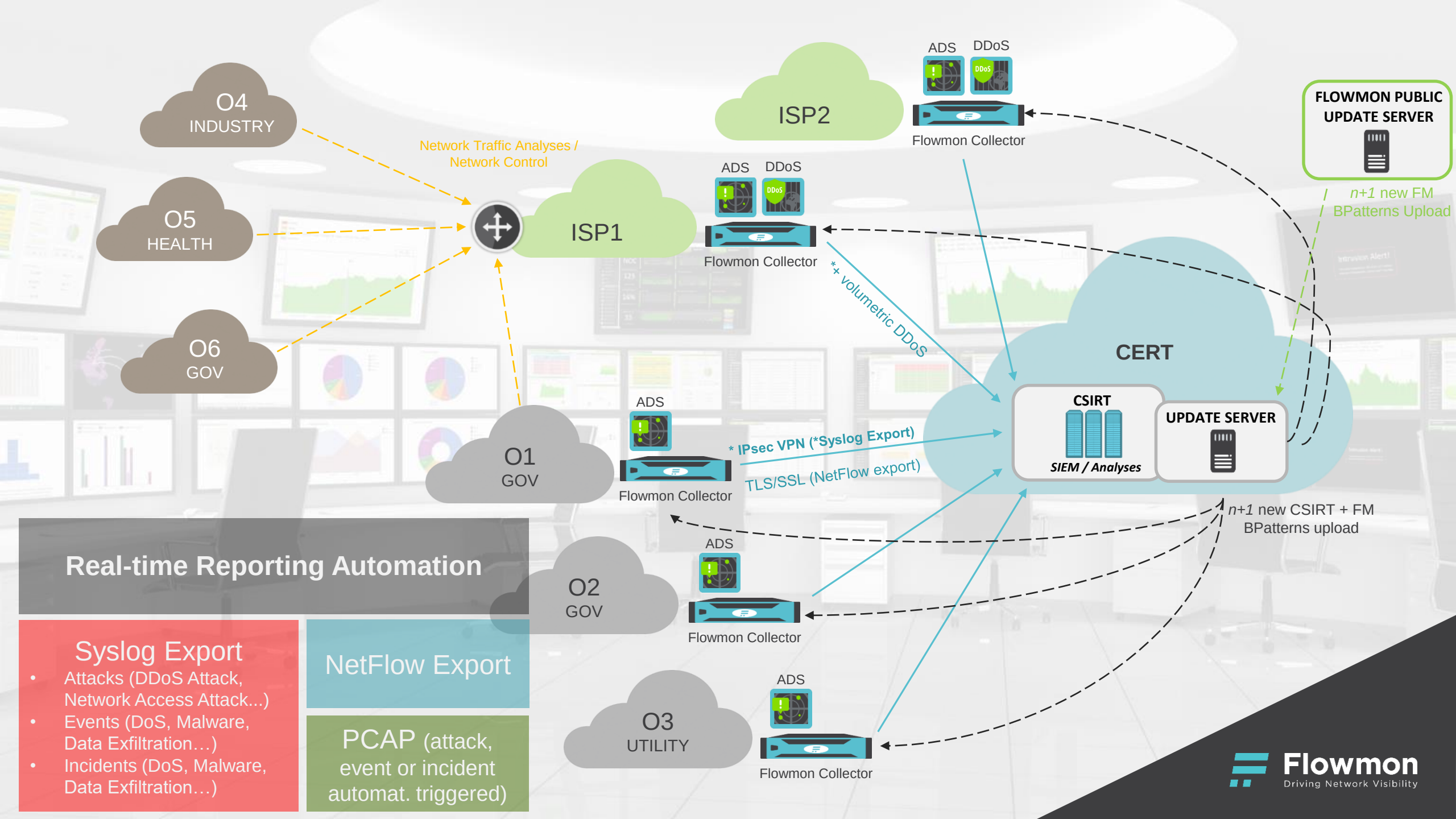
Forensics

Infrastructure

Collector

Probe

Flowmon
Driving Network Visibility


O4
INDUSTRY
O5
HEALTH
O6
GOV
O1
GOV
O2
GOV
O3
UTILITY
ISP1
ISP2
Network Traffic Analyses /
Network Control
ADS
DDoS
Flowmon Collector
*+ volumetric DDoS
* IPsec VPN (*Syslog Export)
TLS/SSL (NetFlow export)
CERT
CSIRT
SIEM / Analyses
UPDATE SERVER
FLOWMON PUBLIC
UPDATE SERVER
n+1 new FM
BPatterns Upload
n+1 new CSIRT + FM
BPatterns upload
Real-time Reporting Automation
Syslog Export
Attacks (DDoS Attack, Network Access Attack...)
Events (DoS, Malware, Data Exfiltration…)
Incidents (DoS, Malware, Data Exfiltration…)
NetFlow Export
PCAP (attack, event or incident automat. triggered)
Flowmon
Driving Network Visibility

Thank you

Performance monitoring, visibility and security with a single solution

Roman Cupka, Principal Consultant CEE

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

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

Flowmon
Driving Network Visibility