Best practices in the detection and response of cyber security incidents

NISD (69/2018 Z.z)

ITAPA 13.11.2019

Roman Cupka. Principal Consultant CEE & Country Manager Slovakia

Flowmon
Driving Network Visibility

NISD / 69/2018 Z.z.

- **Protection** and **security** of **networks** and **information systems** (assets / essential “OES” and digital services “DSP”)
- **Detect**, **solve** and **report** the cyber security **incidents** to national (“based on sector”) CSIRTs/CERTs to avoid penalties (100 - 300.000 EUR)
- An incident is **any event(s)** that **causes service interruption** or **unavailability of service**
- **Application** of **security measurements** (tasks, processes, roles, technologies in organizational, personnel and technical areas)

Cyber & Information Security Assessment

- Assets
- Risk Analyses
- BI Analyses
- Recommendations

Governance

Security Technology

Security Operation

Security Awareness

Reliable Incident Management

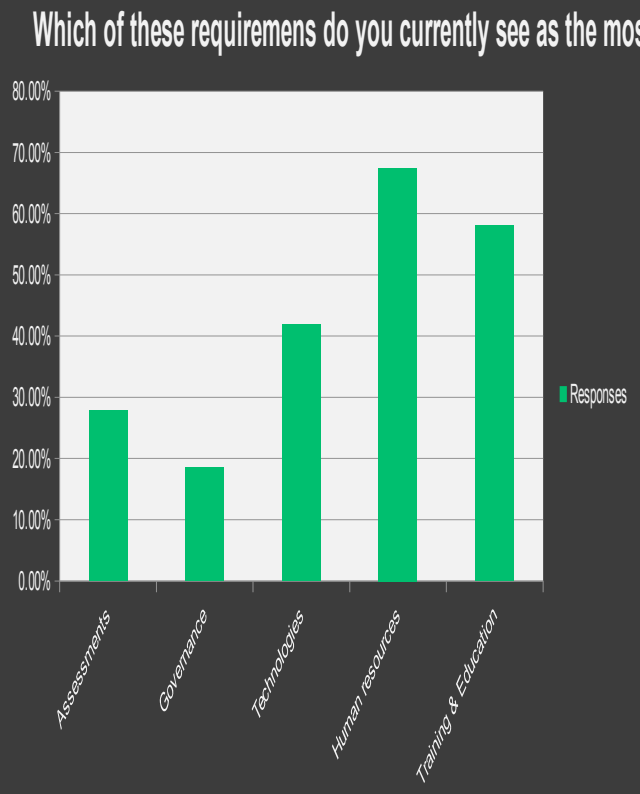
- Detection & Reporting

- Response & Mitigation

- Forensics Analyses

Flowmon
Driving Network Visibility

Flowmon survey 2019 (Slovakia)



Flowmon
Driving Network Visibility

Effective Security Operation

Security Orchestration, Automation & Response

SOAR

Collect security **threats** data and **alerts** from different sources, where incident **analysis** and **triage** can be **performed** leveraging a **combination** of **human** and **machine power**

Incident Response Automation

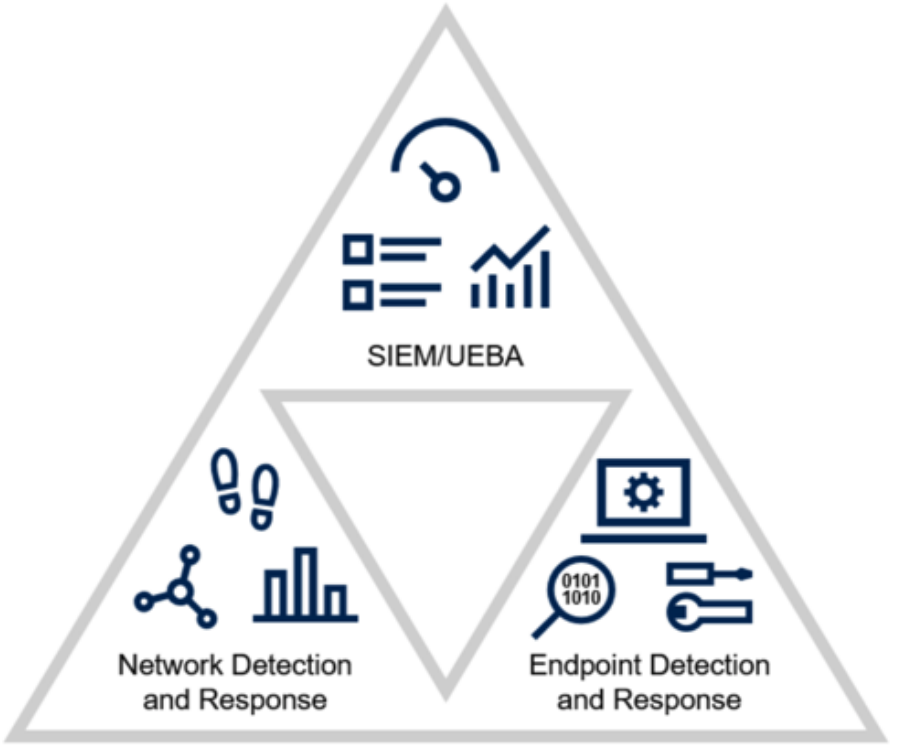
IRA

Routine **relevant alerts/events** that are repetitive and that **do not require** a lot of **human expertise** for immediate **automated analyses** and **response**

Adaptive Security Architecture

ASA

Focuses on **monitoring** for **threats** and **attacks** and dealing with them head-on, **adapting** to **security threats** as they **evolve**



Flowmon
Driving Network Visibility

§ 20 (3g) Security measurements

- **IT Operation** Management
  - **Monitoring** and evaluation of **operational** and **security events**
  - Act. of NBU 362/2018 Z.z. § 11 (h)
    - **Network** and information system **performance monitoring** and **diagnostics**
    - **Detection** of operational and security **anomalies**
    - **Application performance** monitoring

DDoS & Anomaly Detection Network & Application Performance

Flowmon
Driving Network Visibility

§ 20 (4a) Security measurements

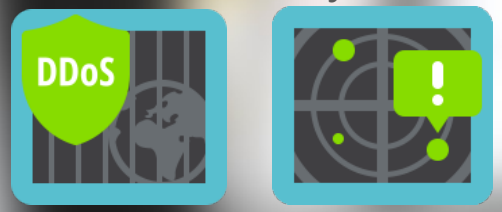
- **Detection** of cyber security **incidents**
- Act. of NBU 362/2018 Z.z. § 14 (4) - **collection** and continuous **evaluation** of cyber security **incidents**
  - Rule-based, corellation
  - **Blacklisting** / Shadowlisting
  - **Anomaly detection**
  - **Signature** based „text mining“
  - **Patterns** comparision
  - **Heuristic** analyses
  - **Cognitive** analyses

Flowmon
Driving Network Visibility

§ 20 (4b) Security measurements

- **Evidence** of cyber security **incidents**
  - **Incident** mitigation
  - Essential and digital services **recovery**
  - **Digital tracks** archiving
  - **Forensics** and **root cause analyses**

DDoS & Anomaly Detection



Traffic & Data Recorder

Collector

Probe

Flowmon
Driving Network Visibility

Storage requirements
for Flow vs. Packet Analysis

	Packet Analysis	Flow monitoring
1 minute	75 GB	0,15 GB
1 hour	4 500 GB	9 GB
1 day	108 000 GB	216 GB

Flow is ready for the future dynamics

Flowmon
Driving Network Visibility

§ 19 (6) the obligations of the essential service operator

- Cyber security **incident resolution**
- **Reporting a** significant cyber security **incident**
- **Provide cooperation** and **information** to the **Central Authority** (U/UO)
- **Archive all evidence** at the time of the incident
- **Report suspected crime** in connection with the incident

DDoS & Anomaly Detection / Network & Application (Data Recording)

Collector

Probe

Flowmon
Driving Network Visibility

Important Steps 69/2018

OES & DSP
Registration
- Central Authority
- Registration of essential services (OES)

Network & Information
Classification
- Network Categorization
- Information Classification

Security Measures
Adoption & Implementation
- Tasks, processes, roles, technologies
- Organizational, personnel and technical areas

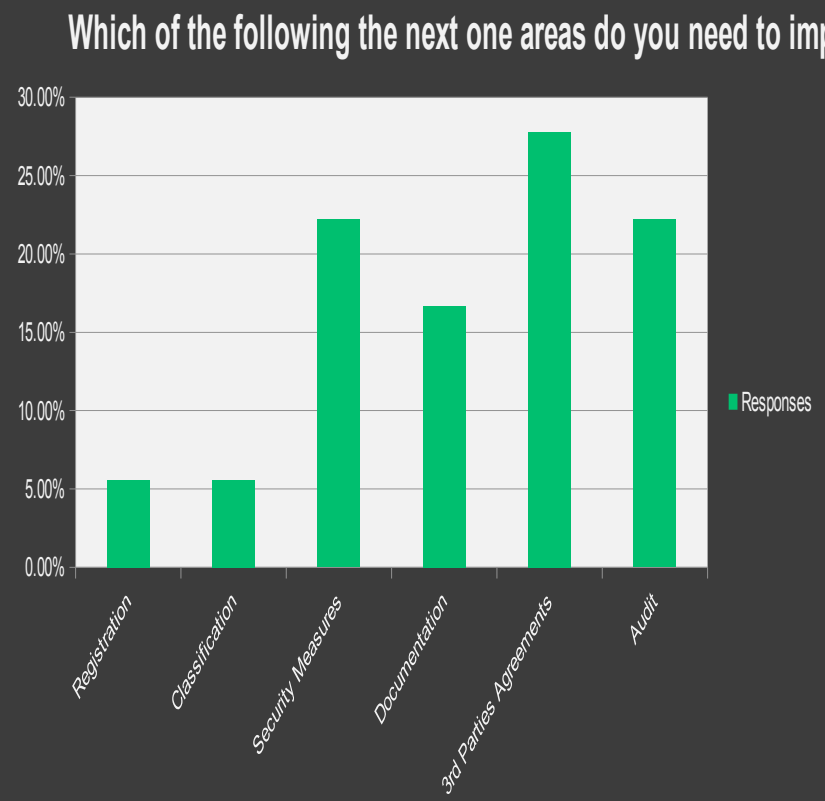
Documentation
Preparation
- Adoption of Sec documentation according measures

3rd Parties
Agreements
- Concluding a contract with a 3rd parties based on Categorization, Classification & Measures

Audit
Internal/External
- Cyber Security Audit by accredited Auditor
- Avoiding the penalties

Flowmon
Driving Network Visibility

Flowmon survey 2019 (Slovakia)



Flowmon
Driving Network Visibility

Thank you

Performance monitoring, visibility and security with a single solution

Roman Cupka, Principal Consultant CEE & Country Manager SK

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