

# The amendment to the Cyber Security Act calls for automation

ITAPA 2021

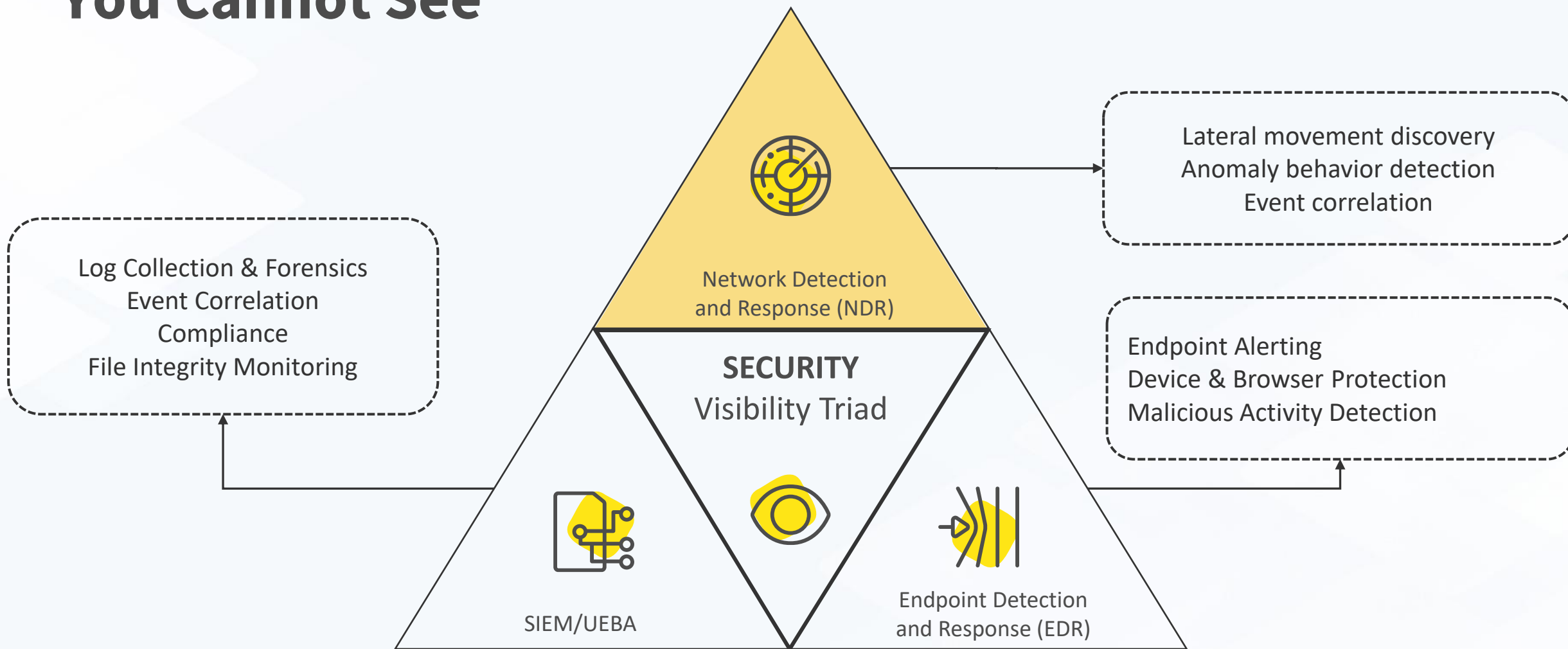
Roman Cupka  Progress® | **Flowmon**

Senior Principal Consultant


10.11.2021



# You Cannot Manage and Protect What You Cannot See





  
**Data Processing Automation**  
 (§24a)

**IoC**  
 (Indicators of Compromise)

<- API (Webhook, Rest) Syslog (CEF)

---

Parsers (hash, IPs, domain, url, CVE...)

---

API (Webhook, Rest) Syslog (CEF) <-


---

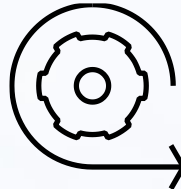
Plain Text, Xml, Json


---

Alerts based on predefined incident type filters

  
**OES**



  
**Cyber Incidents and Security Events**

  
**Security Measures §20 (4a)**

- Rule-based, correlation
- 
- Blacklisting/Shadowlisting
- 
- Anomaly detection
- 
- Signatures based "mining"
- 
- Patterns comparison
- 
- Heuristic / Cognitive analyses





**Thank you for attention**

