Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. – Project: 101190180.

Beyond Response

Automation, Orchestration and Integrated Incident Response Ecosystems

February 2026

Digital Innovation Hub
Trakia

Introduction

Sashka Boncheva

Cybersecurity Expert at EDIH Trakia, Bulgaria

Trainer and Consultant

ISO/IEC 27001 Lead Auditor

General Manager – Elegant Systems Ltd.

Women4Cyber Bulgaria, Co-founder

s.boncheva@dihtrakia.org

Co-funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

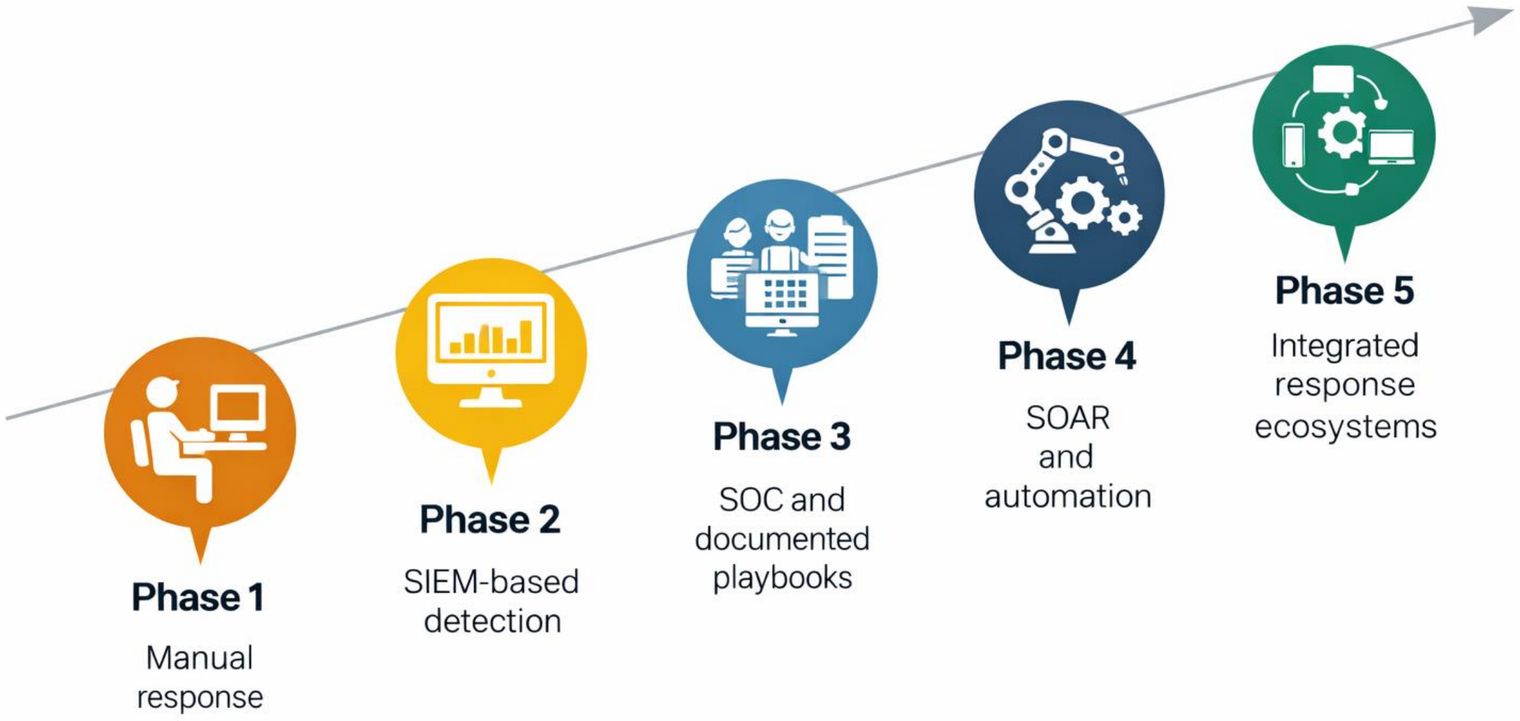
OSCRAT Open-Source Cyber Resilience Act Tools

The Problem

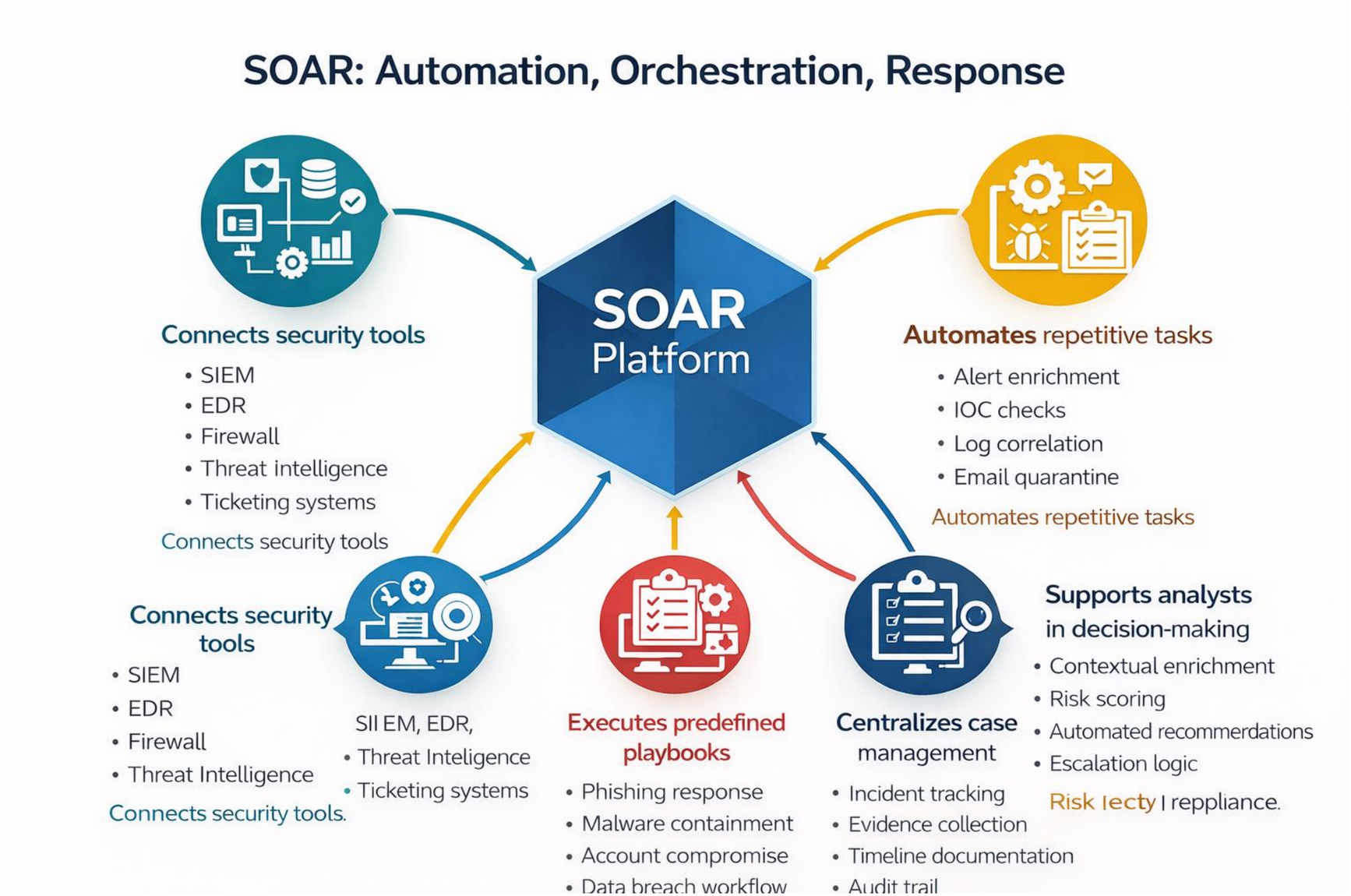
The Reality: Too Many Alerts, Too Little Time

- Thousands of alerts per day
- Multiple disconnected tools
- Manual investigation
- Alert fatigue
- Increasing attack speed

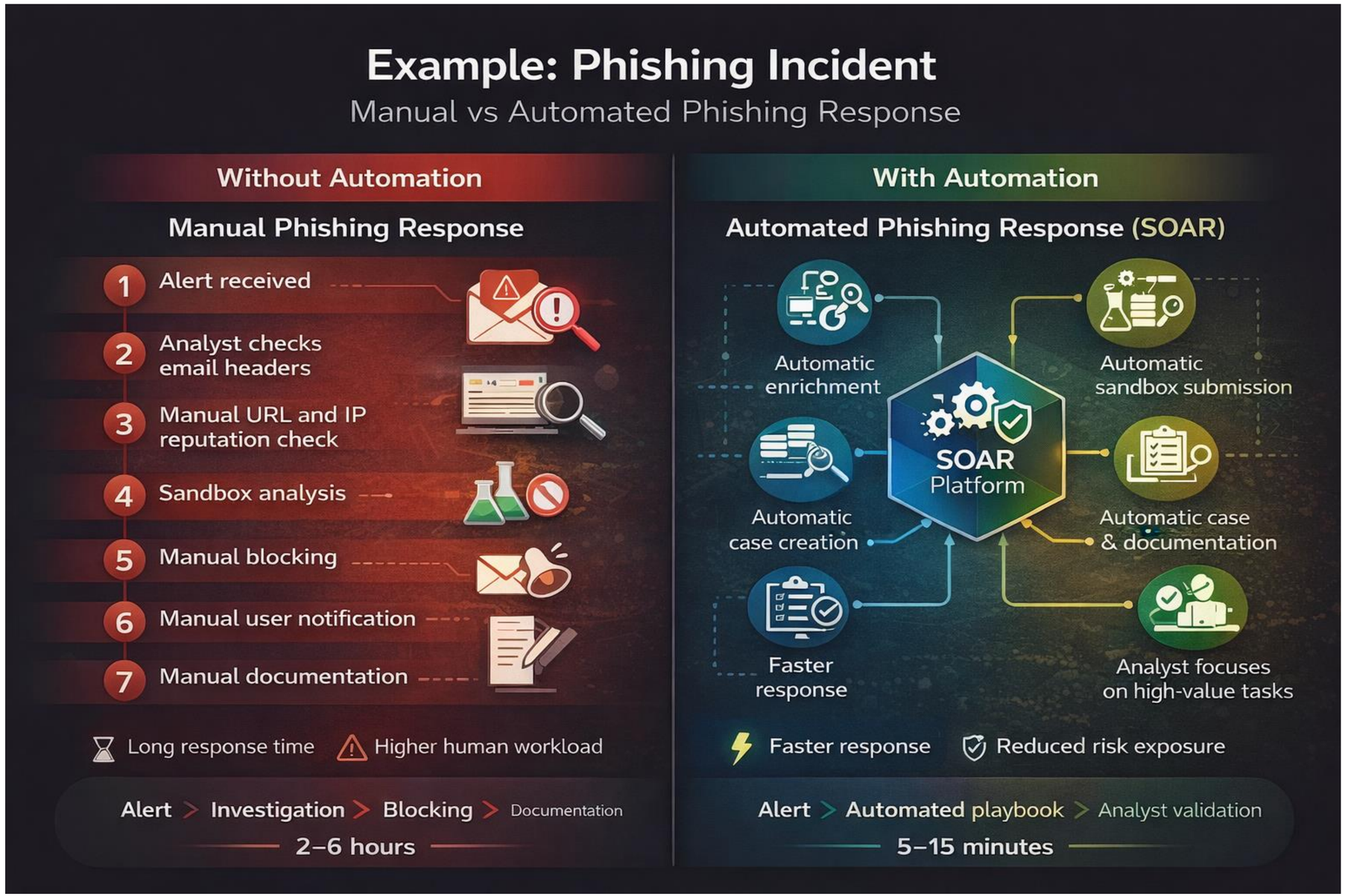
Evolution of Incident Response



What Is SOAR?


SOAR: Automation, Orchestration, Response
SOAR Platform
Connects security tools
• SIEM
• EDR
• Firewall
• Threat intelligence
• Ticketing systems
Connects security tools
Automates repetitive tasks
• Alert enrichment
• IOC checks
• Log correlation
• Email quarantine
Automates repetitive tasks
Connects security tools
• SIEM
• EDR
• Firewall
• Threat Intelligence
Connects security tools.
SII EM, EDR,
• Threat Inteligence
• Ticketing systems
Executes predefined playbooks
• Phishing response
• Malware containment
• Account compromise
• Data breach workflow
Centralizes case management
• Incident tracking
• Evidence collection
• Timeline documentation
• Audit trail
Supports analysts in decision-making
• Contextual enrichment
• Risk scoring
• Automated recommerdations
• Escalation logic
Risk lecty I reppliance.

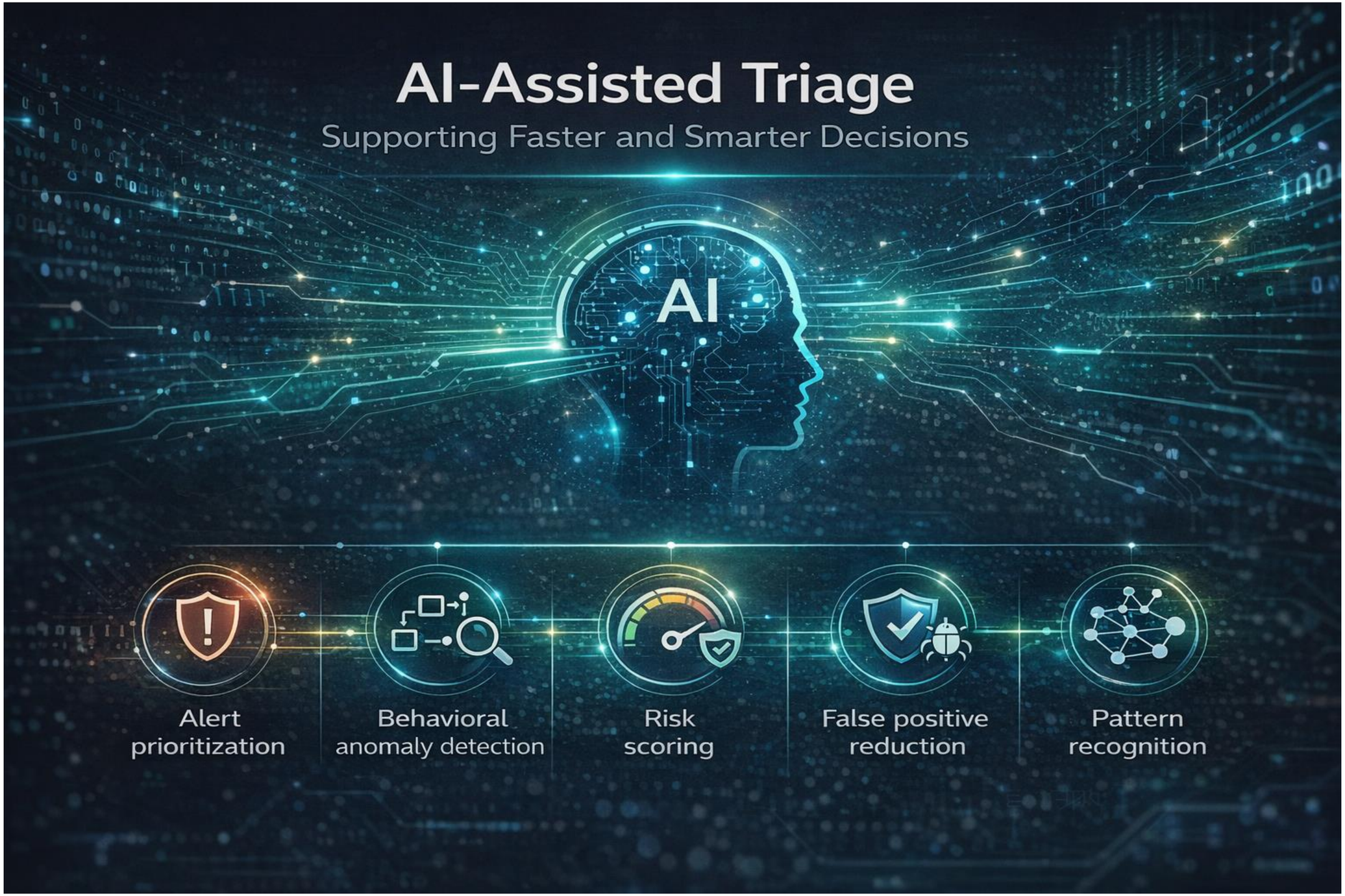
Before and After Automation



Automated Playbooks

Standardized, Repeatable and Controlled Response

- Predefined response scenarios
- Step-by-step automated actions
- Reduced human error
- Faster containment
- Full audit trail


AI-Assisted Triage
Supporting Faster and Smarter Decisions
AI
Alert prioritization
Behavioral anomaly detection
Risk scoring
False positive reduction
Pattern recognition

Threat Intelligence Integration

From Reactive Response to Proactive Defense

- Integration of external threat intelligence feeds
- Indicators of Compromise (IOCs)
- Vulnerability intelligence (CVE, exploit data)
- Sector-specific intelligence sharing (ISACs)
- MITRE ATT&CK mapping


The Integrated Incident Response Ecosystem
Not a Tool. A Connected Operational System.
SIEM
Detection
EDR / XDR
Human Analysts
Detection
SOAR / Case Management
Enrichment
Firewall / Network Security
Ticketing / ITSM
Asset Inventory
Threat Intelligence
Detection
Prevention
Response
Governance
Detection
SIEM / EDR
API / Log Forwarding
Prevention
Firewall / IAM
API Command Execution
Intelligence
TI Feeds
STIX/TAXII
Exposure
TI Feeds
Scan API
Asset Context
ITSM / GRC
Log Forwarding
Governance
ITSM / GRC
Workflow Sync

Automation & Regulation

Regulation Demands Structure.
Automation Enables Execution.

- NIS2 — Incident reporting timelines
- DORA — ICT incident management & resilience
- CRA — Vulnerability handling & reporting
- ISO 27035 / NIST — Structured lifecycle

From Response to Resilience

Reactive → Orchestrated → Predictable → Resiiient

Reactive

Manual, Ad-hoc
Firefighting

Orchestrated

SOAR, Automation
Playbooks

Predictable

Threat Intelligence
Analytics, AI

Resilient

Continuous Monitoring
Governance, Culture

Final Takeaways

- Automation is inevitable
- Integration is critical
- AI is supportive, not sovereign
- Governance remains human

THANK YOU

FOR YOUR ATTENTION

February 2026

Sashka Boncheva

m: +359 888 800 222

s.boncheva@dihtrakia.org

Co-funded by the European Union

CYBER 4 ALL STAR

WOMEN 4CYBER BULGARIA

Digital Innovation Hub Trakia

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

OSCRAT Open-Source Cyber Resilience Act Tools