Bridging AI and Network Security

From Reactive Defense to Autonomous Resilience

Adrian Yeow

Technical Director, Infoline Tec Group Berhad

KHNOG 2025 Phnom Penh

Abstract & Introduction

As networks evolve into distributed, hybrid, and software-defined environments, conventional security operations are challenged by scale, fragmentation, and the speed of modern threats.

This presentation explores how **AI, automation, and SDN** transform security from reactive response to autonomous resilience.

Key Topics

- The evolving security landscape
- Limitations of traditional approaches
- AI and automation in security operations
- SDN, NFV and network automation
- Intelligent SOC operations

The Evolving Security Landscape

- **Explosive growth** of users, devices, and cloud workloads blurs traditional perimeters
- **Threats grow in scale and velocity**, outpacing human response capabilities
- **Security-tool fragmentation** weakens visibility and creates blind spots

A new model is required: adaptive, predictive, and intelligence-driven

Limitations of Traditional Approaches

- **Reactive posture** — detection only after compromise
- **Manual processes** — slow triage, analyst fatigue
- **Tool silos** — no end-to-end visibility
- **Skill shortage** — high human dependency

Outcome: inconsistent response and poor resilience

AI and Automation in Security Operations

Detection & Response

- **Traffic pattern analysis** identifies anomalies in seconds
- **Behavioral baselines** establish normal activity patterns
- **MTTD reduction** from hours to minutes

Automation

- **SOAR platforms** isolate assets, revoke credentials
- **Automatic blocking** of malicious IPs and domains
- **Closed-loop orchestration**: detection → containment → recovery

80%
MTTD Reduction

60%
MTTR Reduction

Example: AI-assisted DDoS Mitigation

Combining flow analytics with SDN-based rerouting achieves sub-minute containment

SDN, NFV and Network Automation

SDN

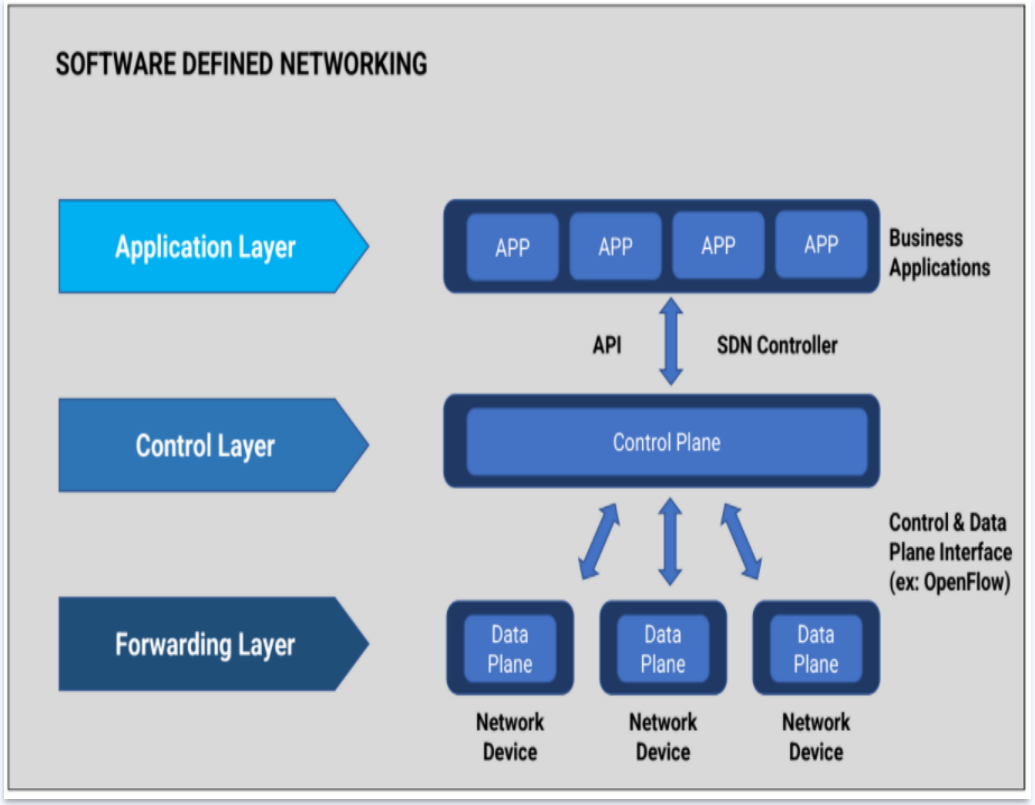
- Centralized policy control
- Dynamic segmentation
- Micro-segmentation

NFV

- Virtualized security functions
- Firewalls, IDS, load balancers
- Elastic scale

Automation

- Infrastructure-as-Code
- Consistent configuration
- Rapid deployment



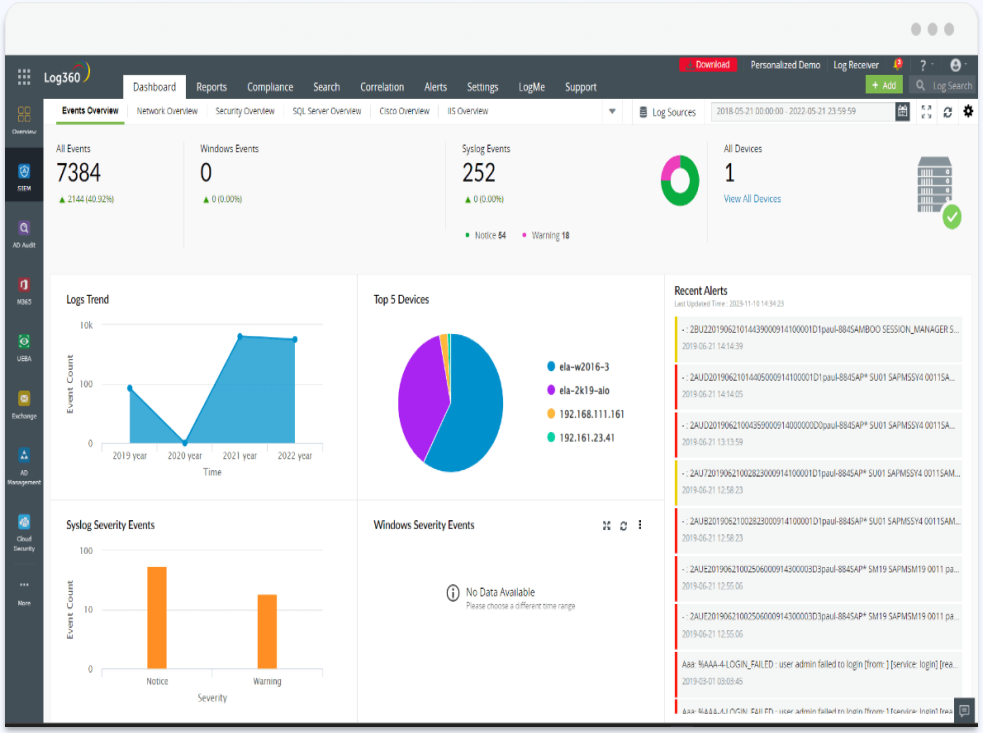
Intelligent SOC Operations

AI-driven SOCs merge analytics, orchestration, and automation

Automated triage reduces false positives by 85%

Machine-learning correlation accelerates incident analysis

Generative-AI summaries speed executive reporting



MTTD reduced from hours to minutes
MTTR cut by automated playbooks

90%
False Positive Reduction

70%
Analyst Time Saved

Challenges and Considerations

Data Quality

AI accuracy depends on **clean**, **diverse** telemetry

Explainability

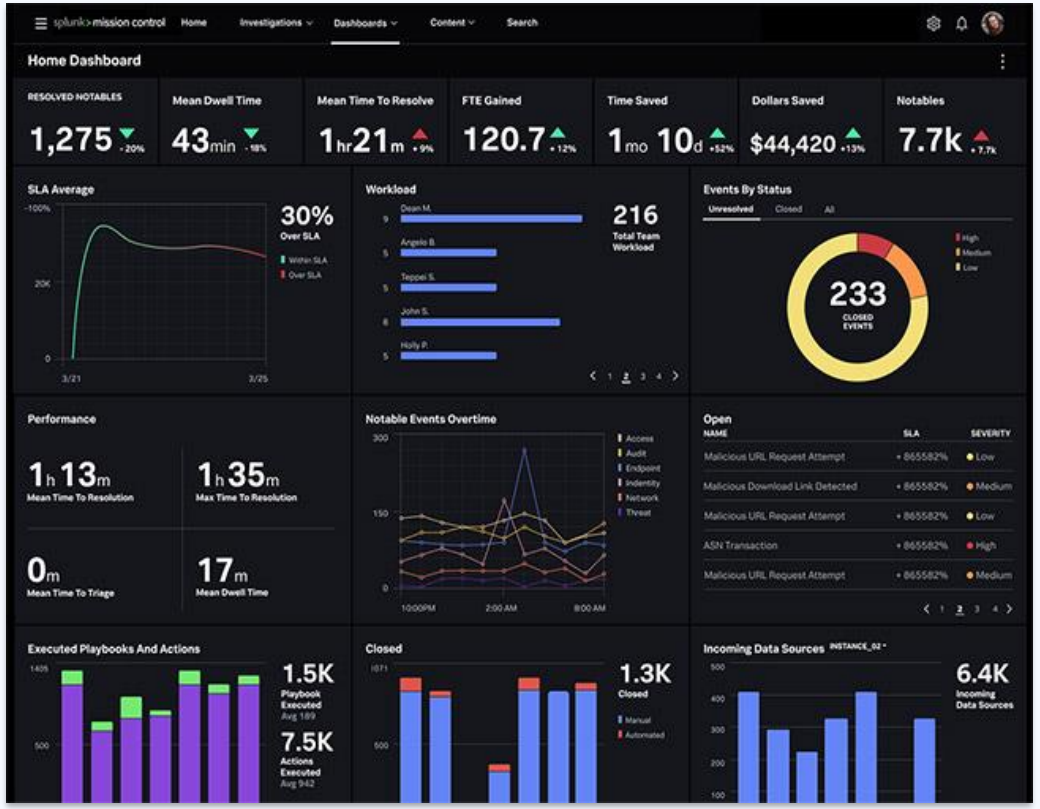
Decisions must be **transparent** for audit

Integration

Legacy tools require **adapters** or phased replacement

Human Oversight

Automation **augments**, not replaces analysts



The Road to Autonomous Resilience

Unified SOC/NOC

Converge **AI**, **SDN** & **Automation** within a single operational framework

Adaptation Focus

Shift from **defense** to **adaptation** and **continuity**

Human-AI Collaboration

Foster **"human-in-the-loop"** collaboration between AI and experts

Business Alignment

Align security objectives with **business resilience** goals

Conclusion

- The convergence of **AI**, **SDN**, and **automation** signals a new security era
- Enterprises that integrate these capabilities gain **agility**, **visibility**, and **trust**
- Building networks that are not just secure but **self-healing**
- By adopting intelligent automation today, organizations prepare for an **autonomous**, **resilient** tomorrow

Thank You

Adrian Yeow | Technical Director, Infoline Tec Group Berhad

KHNOG 2025 Phnom Penh

"The future of network security is not just about defending against threats, but building systems that can adapt and heal themselves."