2025 Cybersecurity Trends

NSTDA Annual Conference 2025 (NAC 2025)

Dr. Montida Pattaranantakul
Researcher, Information Security Research Team (SEC),
Communication and Network Research Group (CNWRG),
National Electronics and Computer Technology Center (NECTEC),
National Science and Technology Development Agency (NSTDA)

Cybercrime is a Growing Threat

As technology advances, cybercriminals are developing more sophisticated attack methods, increasing the risk of financial loss, data breaches, and security threats.

Statistical and Fact in 2025

10%

increase of global cybercrime costs, The global cost of cybercrime is expected to reach $10.5 trillion annually by 2025

Reference: IBM - Cybercrime magazine

Statistical and Fact in 2025

95%

of data breaches happens due to human errors

Types of human errors leading to data breaches

- Weak or reused passwords
- Falling for phishing attacks
- Sending data to the wrong person (Misdirected emails)
- Misconfiguring security settings
- Not updating software (Unpatched vulnerabilities)
- Poorly managed access control & insider threats

Reference: IBM - Top Cyber Security Facts and Statistics for 2025

Statistical and Fact in 2025

88%

of cybersecurity breaches were financially motivated

Most cyberattacks are driven by monetary gain, common financially motivated cyber attacks are;

- Ransomware attacks
- Phishing attacks
- Cryptojacking
- Selling stolen data on the dark web

Reference: IBM - Top Cyber Security Facts and Statistics for 2024

Statistical and Fact in 2025

Malware remains a dominant threat, with over 1.2 billion malware programs in existence.

Meanwhile, The growth of ransomware-related malware attacks is expected to rise by 30% to 40% in 2025 compared to previous years.

Reference: Embroker- Cyberattack statistics 2025

Statistical and Fact in 2025

13%

increase in DDoS (Distributed Denial of Service) attacks in the first half of 2024, totaling over 8 million incidents

Reference: Embroker- Cyberattack statistics 2025

Thailand's Cybersecurity Landscape

10.5$ trillion

The financial impact of cybercrime on the economy and society is expected to surge to 10.5$ trillion by 2025

0.2%

Thailand spends only 0.2% of corporate revenue on cybersecurity systems

1,843 cyber attacks/week

The global average of 1,843 attacks/week/organisation

3,810 cyber attacks/week

The average cyberattacks in Thailand / organization over the last 6 months (Aug 2024 - Jan 2025)

4%

in average compared with the global ransomware incidents

2.8%

of banking malware attacks

6%

of ransomware incidents encountered in Thailand

9.5%

of banking malware attacks in Thailand, which revealed that Thai bank customers suffered losses of more than 60 billion baht to online financial fraud over the last 2 years.

Reference: Fortinet- Thailand Cybercrimbe by 2025

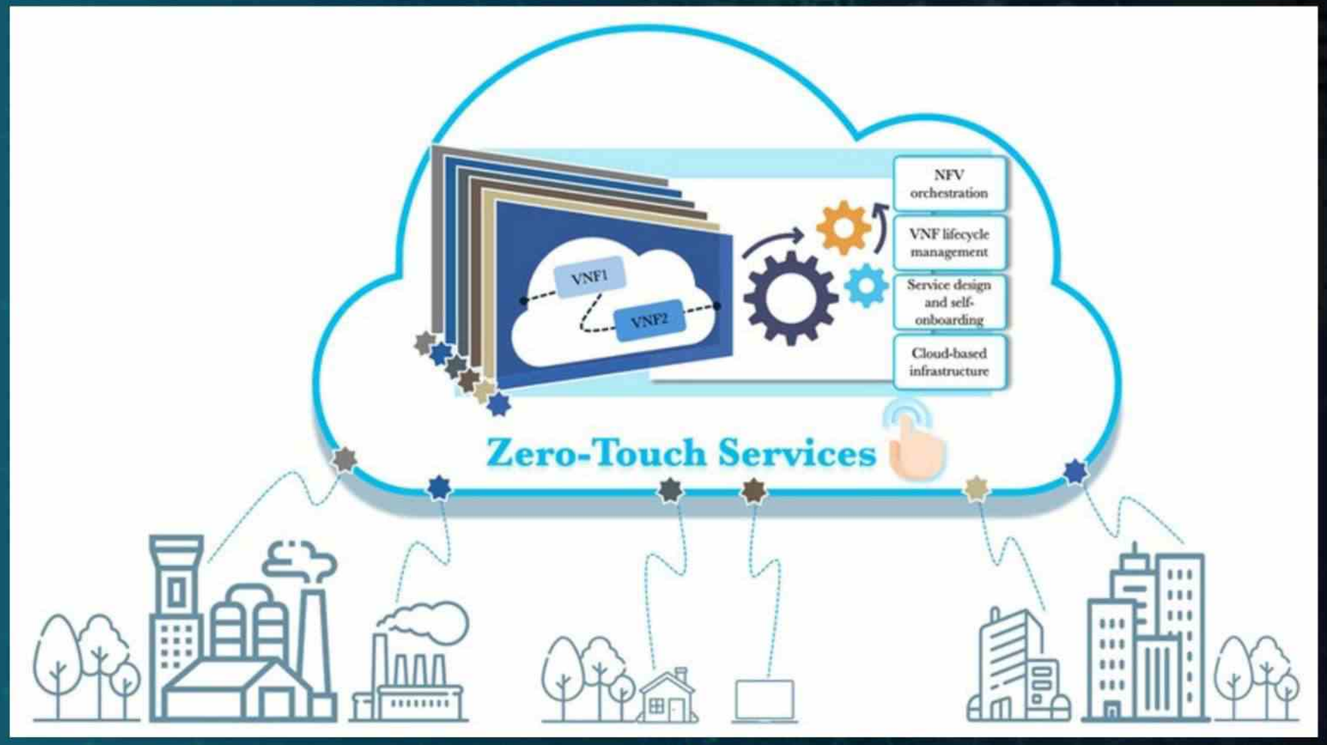
NAC2025
20th NSTDA Annual Conference
การประชุมวิชาการประจำปี สวทช. ครั้งที่ ๒๐

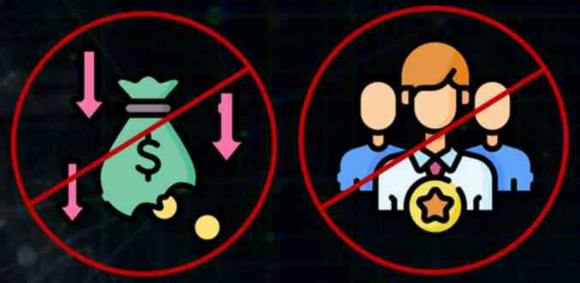
NECTEC a member of NSTDA
กสทช.
กทปส.

Zero-Touch Services

The Future of Automated Cyber Threat Detection and Response

Zero-Touch Services





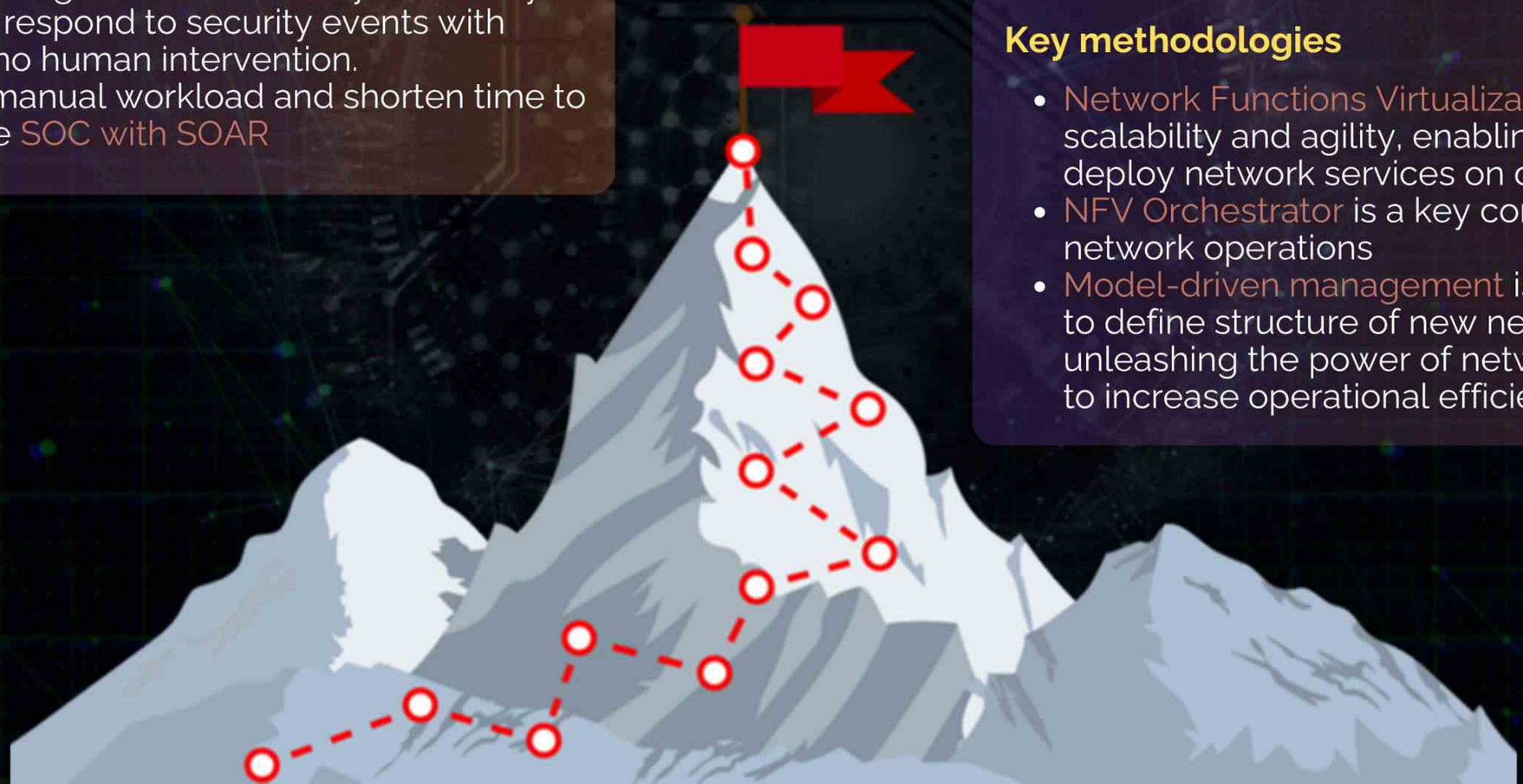
Key observation -- 96% of business in Thailand are SMEs, many of them cannot afford advanced security prevention services

Zero-Touch Services aims to help SMEs the limited expertise and financial resources constraints, by providing scalable and flexible security solution for real-time monitoring and threat detection capabilities with minimal or no human intervention

Our goal

Contributions

- To develop the **"Zero-Touch Services"** platform that enables organizations to analyze security threats and respond to security events with minimal or no human intervention.
- To reduce manual workload and shorten time to action at the SOC with SOAR

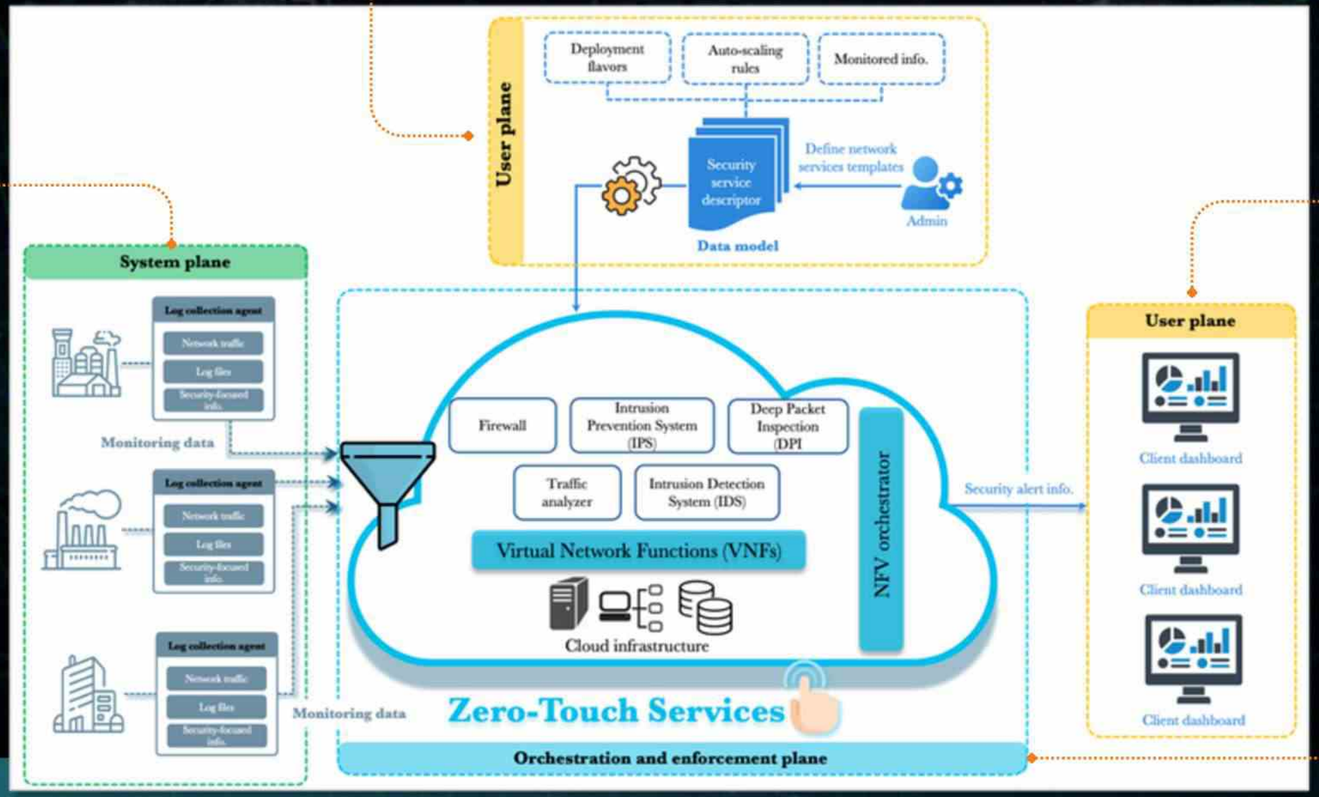


Key methodologies

- Network Functions Virtualization (NFV) enhances scalability and agility, enabling service providers to deploy network services on demand
- NFV Orchestrator is a key component to automate network operations
- Model-driven management is the use of data model to define structure of new network services, unleashing the power of network programmability to increase operational efficiency

Design principles

User plane: serves for two main purposes.
• Web portal allows administrators to interact with the system for creating, configuring, and managing the lifecycle of security services



System plane: in which log collection agents are installed at the endpoint gateway of a particular enterprise network

• Tenant-based threat detection dashboard allows allows each tenant to monitor the detected malicious activities within their enterprise network using our provided security services.

Orchestration and enforcement plane: investigates anomalies by analyzing event data collected from the log collection agents and examines whether any vulnerabilities have occurred within the target enterprise's network.

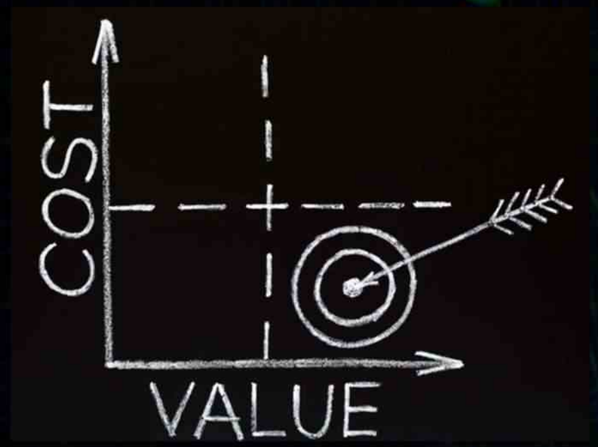
Dashboard

Admin view – Virtualization dashboard shows the operational status (e.g., CPU/memory utilization, VM/VNF status) related to the instantiation of security services

Dashboard

Tenant view – Tenant-specific threat detection dashboard, analysis results from the provided security services (e.g., Snort, Suricata, Zeek)

Key benefits



Security

Cost saving

Efficiency

Achievments

รางวัลความเป็นเลิศด้านความคิดสร้างสรรค์
จากการประกวด
"ผลิตภัณฑ์และบริการในภาคอุตสาหกรรมด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ 2567"
จัดโดย สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)

เนคเทค สวทช. คว้า 2 รางวัล
ผลิตภัณฑ์และบริการในภาคอุตสาหกรรม
ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ประจำปี 2567

Thank you for your attention

ข้อมูลเพิ่มเติม

ติดต่อสอบถาม

Dr. Montida Pattaranantakul, Researcher
Email: montida.pat@nectec.or.th
Phone: 02 564 6900 ext 2520
website: www.nectec.or.th