Future Security for Future Networks

Sam Barker

VP, Telecoms Market Research

Juniper Research


MWC24

Senthil Ramakrishnan

Assistant VP, Product Management & Development, Cybersecurity

AT&T

State of Cybersecurity 2024

Vendor Sprawl	**3K+** cybersecurity vendors in US	**Increasing Complexity**
Alert Fatigue	**75+** separate cyber tools managed	**Limited Integration**
Talent Shortage	**3M+** cyber personnel shortfall	**Lack of In-House Expertise**
Regulation	**280+** cyber bills in US	**Sprawling Compliance Requirements**
Cybercrime	**$1T+** cost of cybercrime	**Growth in Malicious Activity**

Top Priorities:

- **Security is #1** concern for Customers
- Threat landscape is intensifying
- Cost of cyber breach is **>$1B in 2023**
- Security Controls are vastly distributed and complex
- **43% of attacks target Small Business & Mid Market**

*Source : Gartner 2023 Global Security and Risk Management Survey

Customers and challenges

Cloud-first approach is fueling internet connectivity

As 5G and fiber are growing, your threat surface is also expanding

Digital transformation is top of mind

Need solutions that support growth strategies and the ability to scale quickly

Attacked from all sides*

The cyberthreat landscape is ever-evolving and expanding

Limited resources available to manage and maintain policies and controls

*Gartner 2021 Global Security and Risk Management Survey

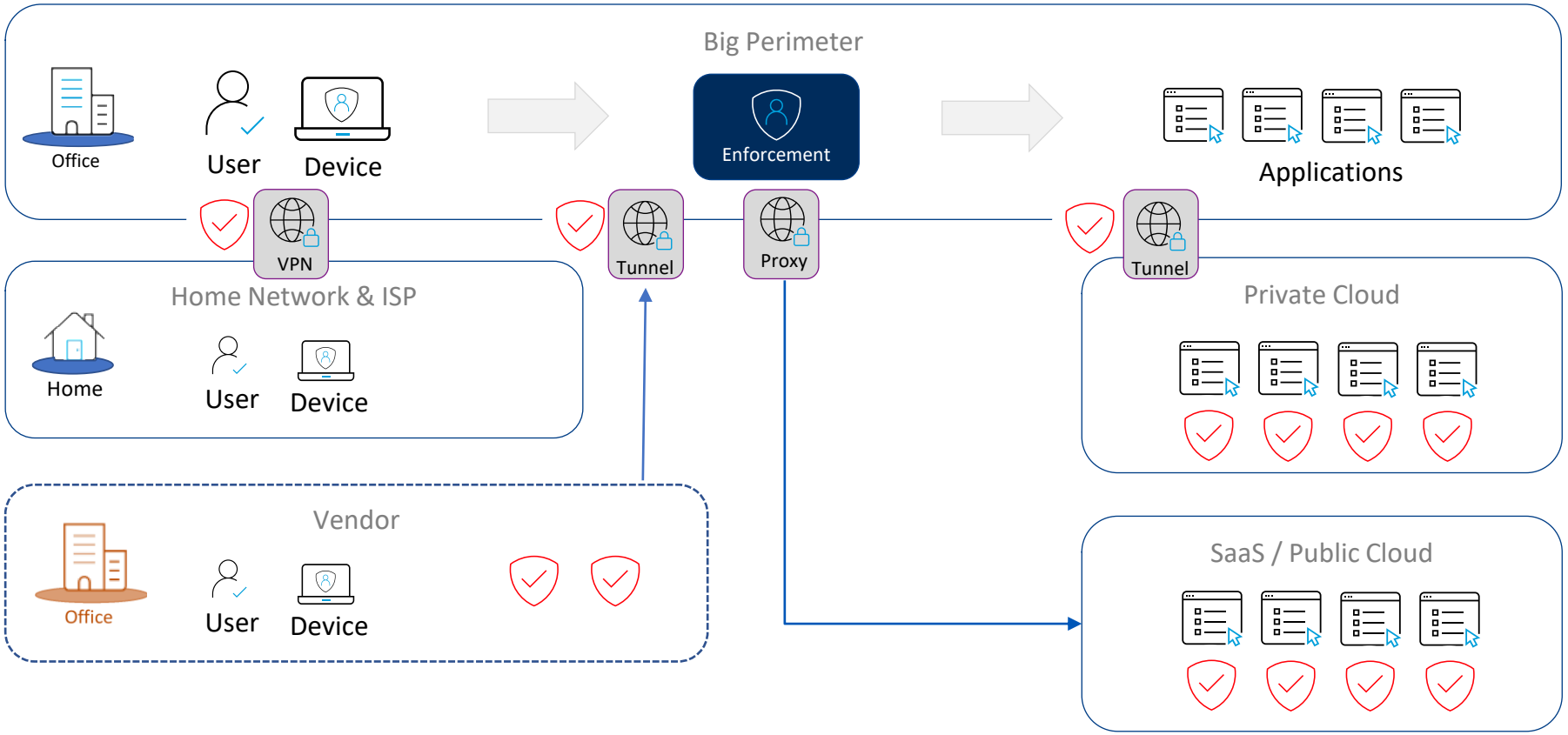
Complexity is a challenge

Lack of expertise to manage and maintain multiple security solutions from multiple vendors

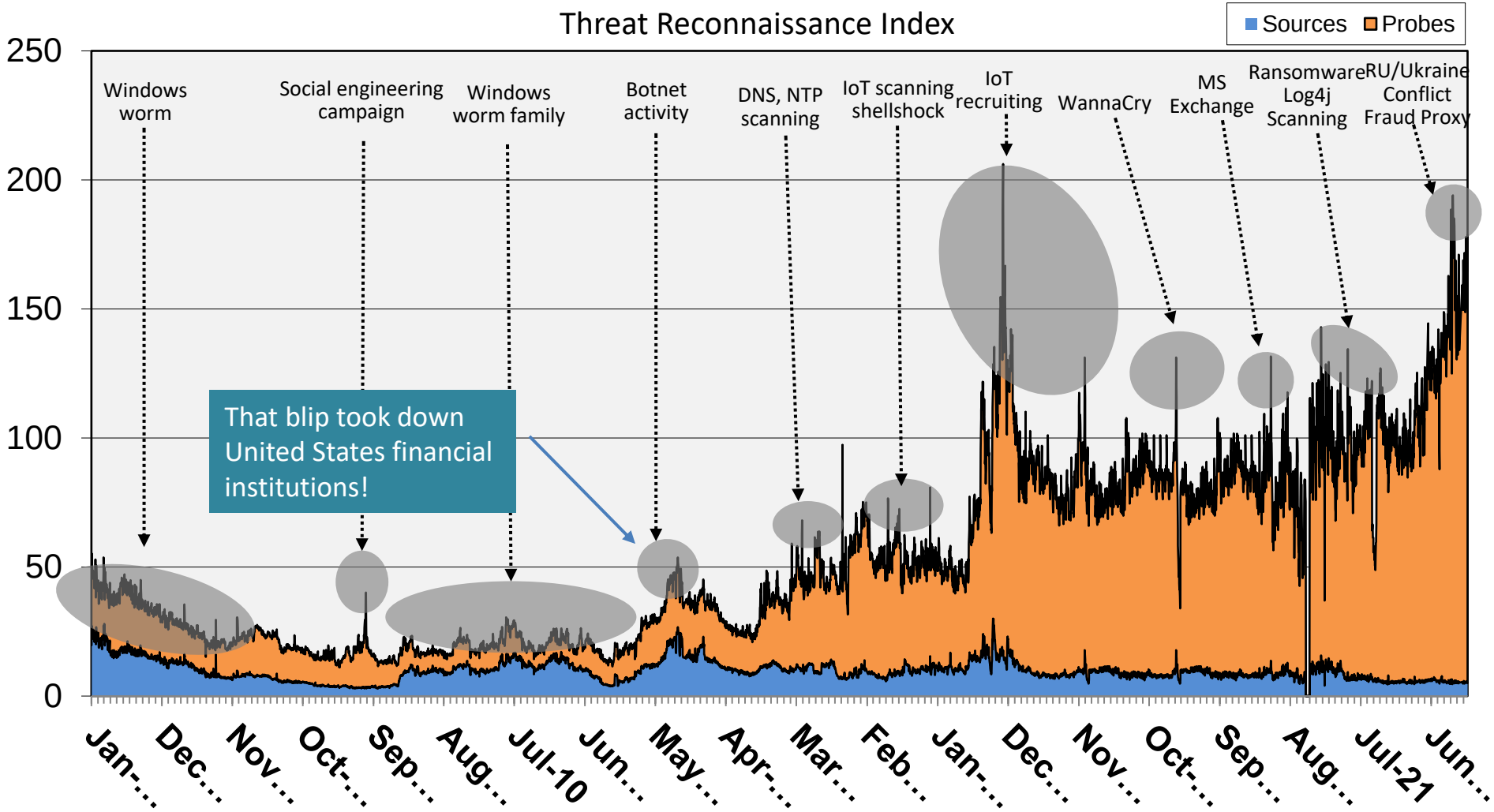
Budget constraints make multiple security solutions too costly

Remember when life was Simple….

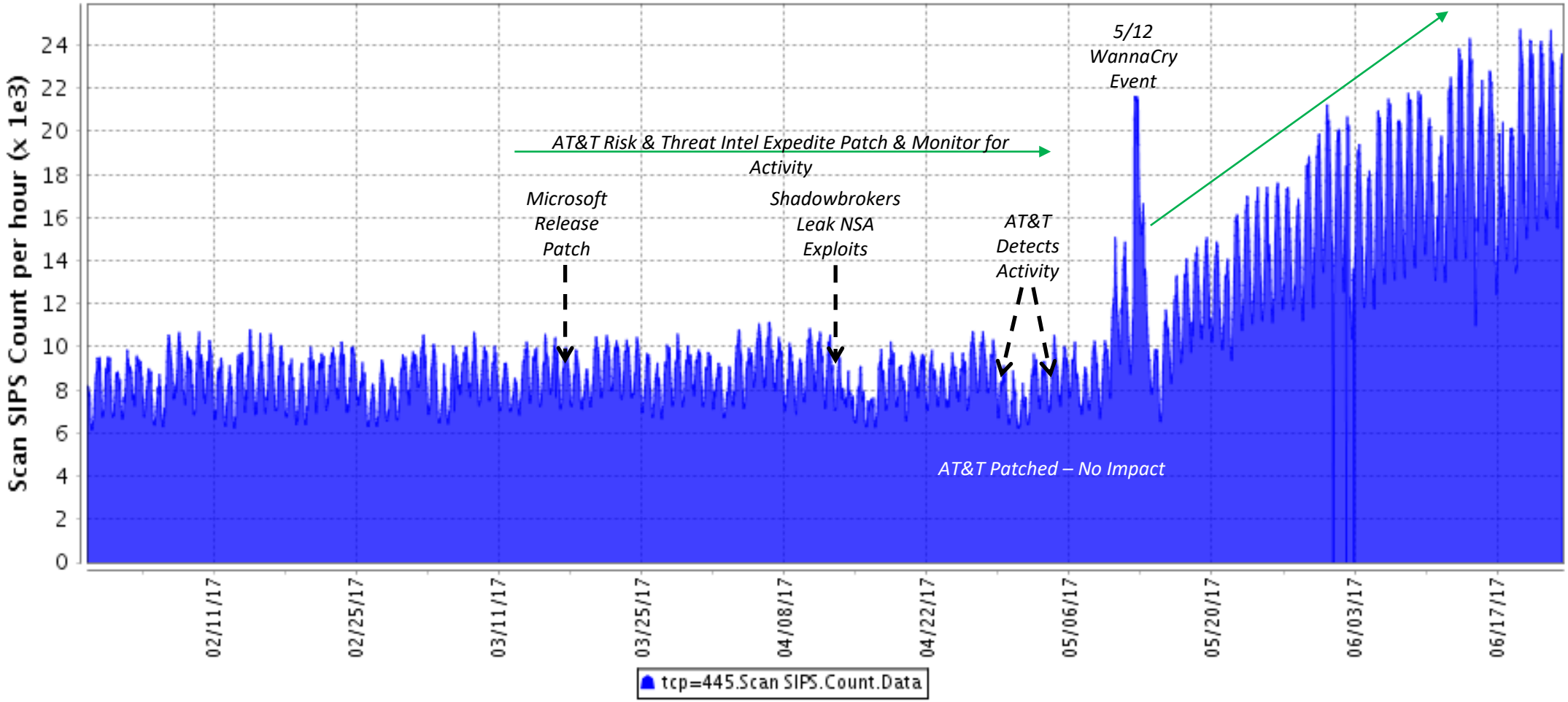
Security Has Become Complex and Hard to Manage



Visibility generates Valuable Insights



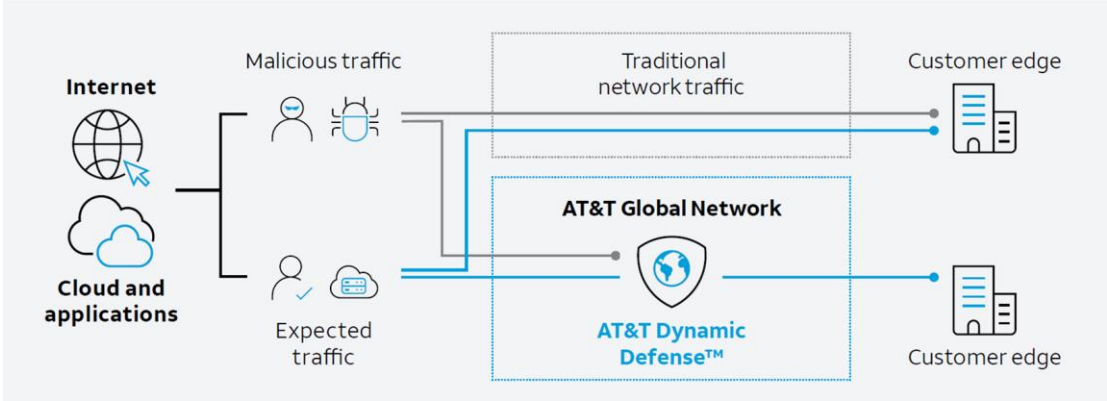
A deeper look at Exploit Activity - WannaCry



What is Network Embedded Security?

AT&T Network Embedded Security

a security platform embedded in AT&T's global network infrastructure that customers can utilize to detect threats, filter traffic, and execute security controls before the data reaches their network.



Unprecedented visibility

We see it first

Embedded security controls

Built in, not bolt on, included with AT&T Connectivity

Effortless

Better security at a better value

Near-real time

Same-day deployment in minutes, 24/7/365 network monitoring

AT&T Network Security – MITRE ATT&CK

Dynamic Defense

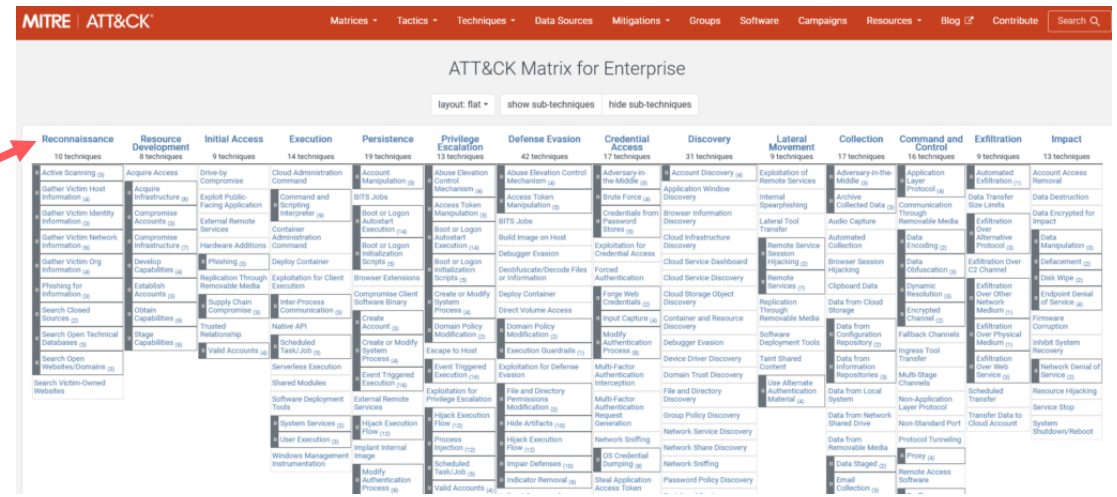
Filt

Detects threats BEFORE they reach customer

Defeat Reconnaissance and Initial Access Techniques

Executes security controls to mitigate threats

Impacted MITRE ATT&CK techniques are highlighted



AT&T Business


MWC24

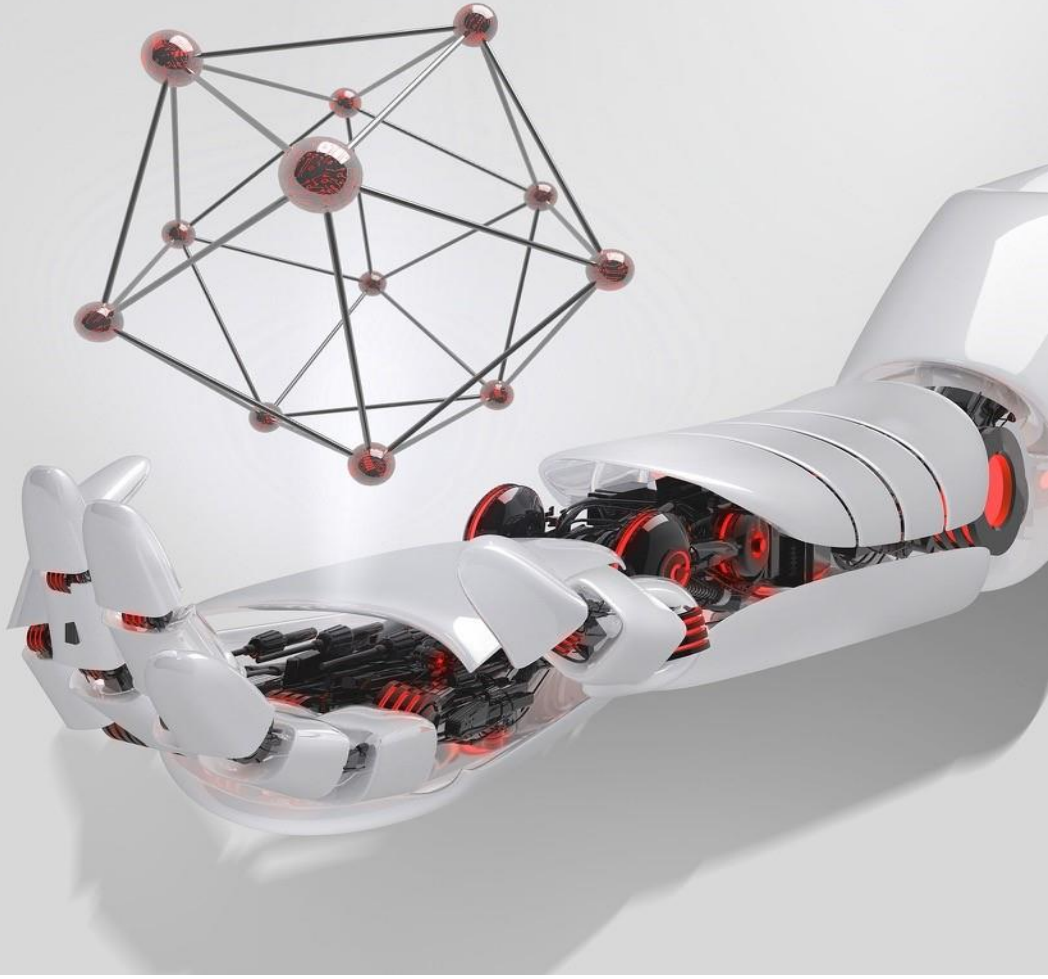
Louis Lou

Executive Assistant Director, Global Cyber Security & Privacy

Huawei

FUTURE SECURITY

FOR FUTURE NETWORKS



Louis Lou

Executive Assistant Director for Global Cyber Security & Privacy

HUAWEI

Future Security Challenges | More Cyber Attacks and EDTs bring new challenges

Cyber Attacks

Ransomware Attack

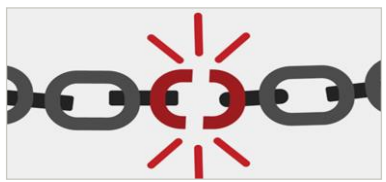
Ransom attacks occur every 11 seconds

It can cause losses of billions of dollars to enterprises.

DDoS attack

More than 10 million DDoS attacks per year

398 million RPS attack



Supply chain attacks

45% of organizations worldwide have experienced one or more software supply chain attacks

Data breach

The average cost of a data breach is up to $4+ million.

According to Cybersecurity Ventures, the global economy is expected to lose up to $10.5 trillion by the end of 2024.

Emergent Disruptive Technologies (EDTs)

AI/Large Model

AI Security

AI for Attack (Attacker)

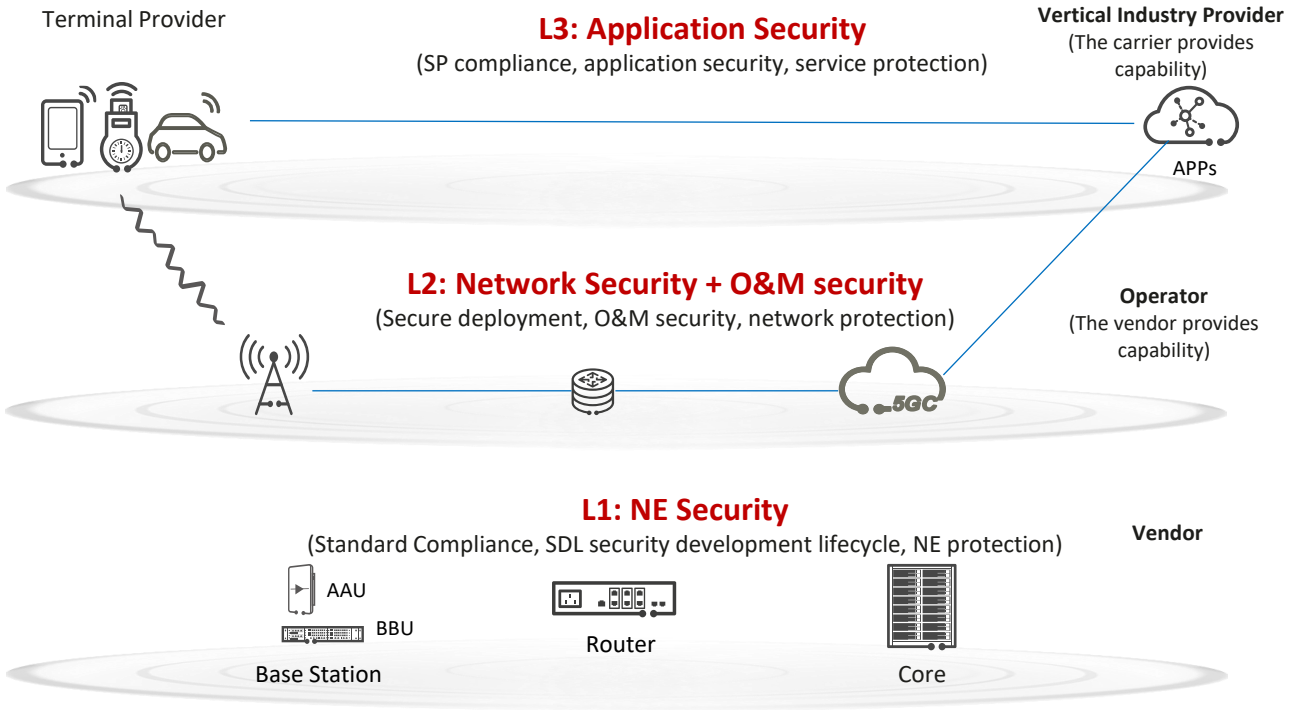
AI for Security

Quantum Computing

Quantum computing breaks asymmetric cryptosystems and subverts existing cryptosystems.

HUAWEI

Future Security Technologies and Applications | AI integrated development environment, AI network O&M, and AI malicious content identification



Application Layer

AI identifies malicious content and security traps.

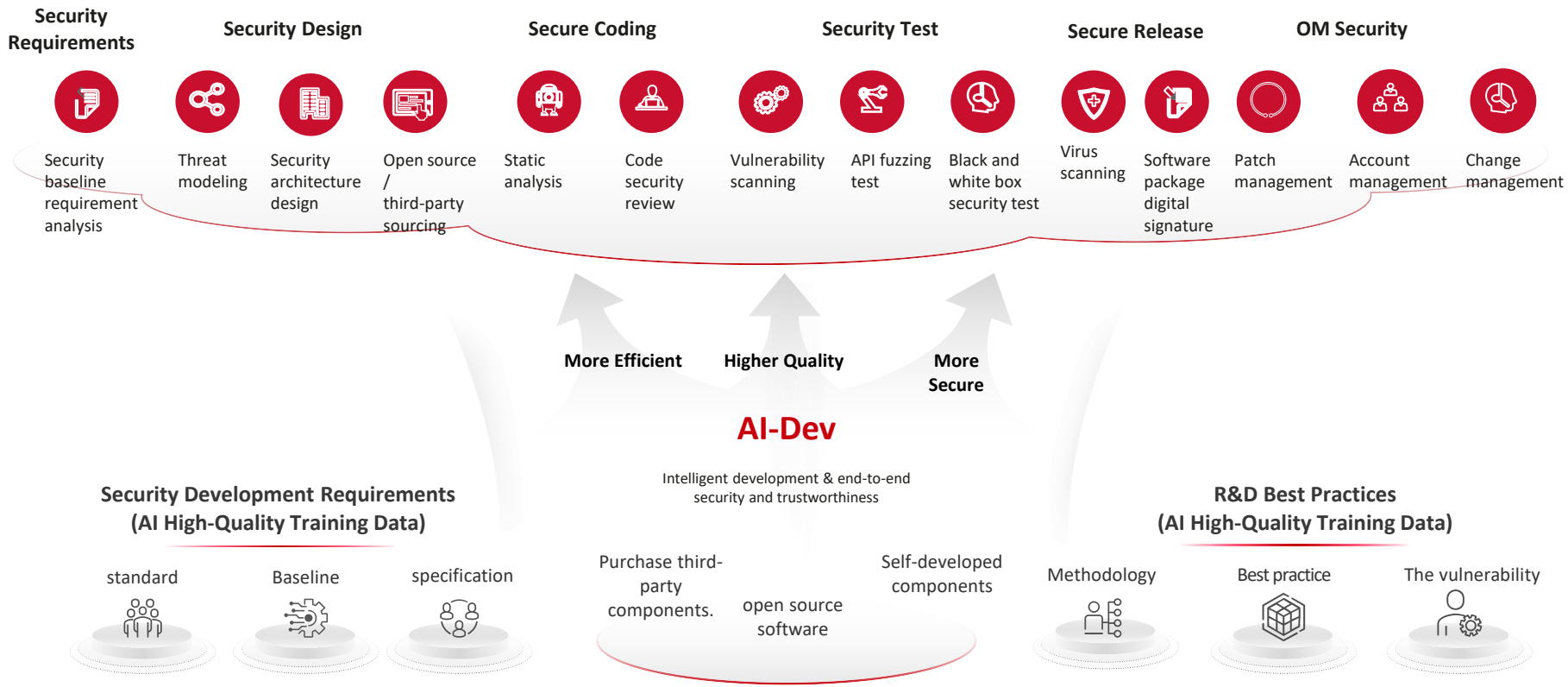
Network Layer

AI + IPDRR, AI network deployment/O&M, monitoring, and situational awareness

Product Layer

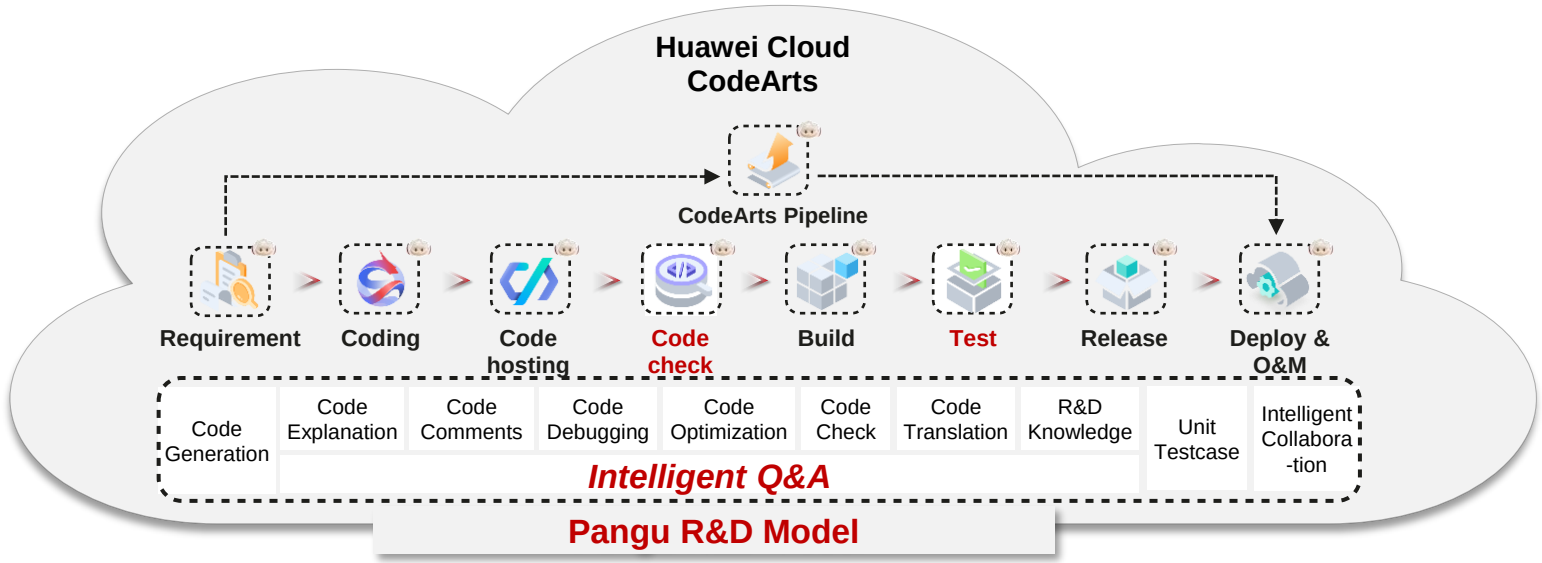
The AI integrated development environment ensures product design, development, testing, and vulnerability management.

AI-enabled Product Development | AI-DEV Integrates the Tool Chain to Ensure Product Design, Development, Testing and Vulnerability Management, Helping Suppliers Develop More Secure Products



AI-DEV | CodeArts Absorbed Huawei R&D Engineering/Tool Capabilities, and is Offered to Business Customers to Improve their Product Quality and Development Productivity

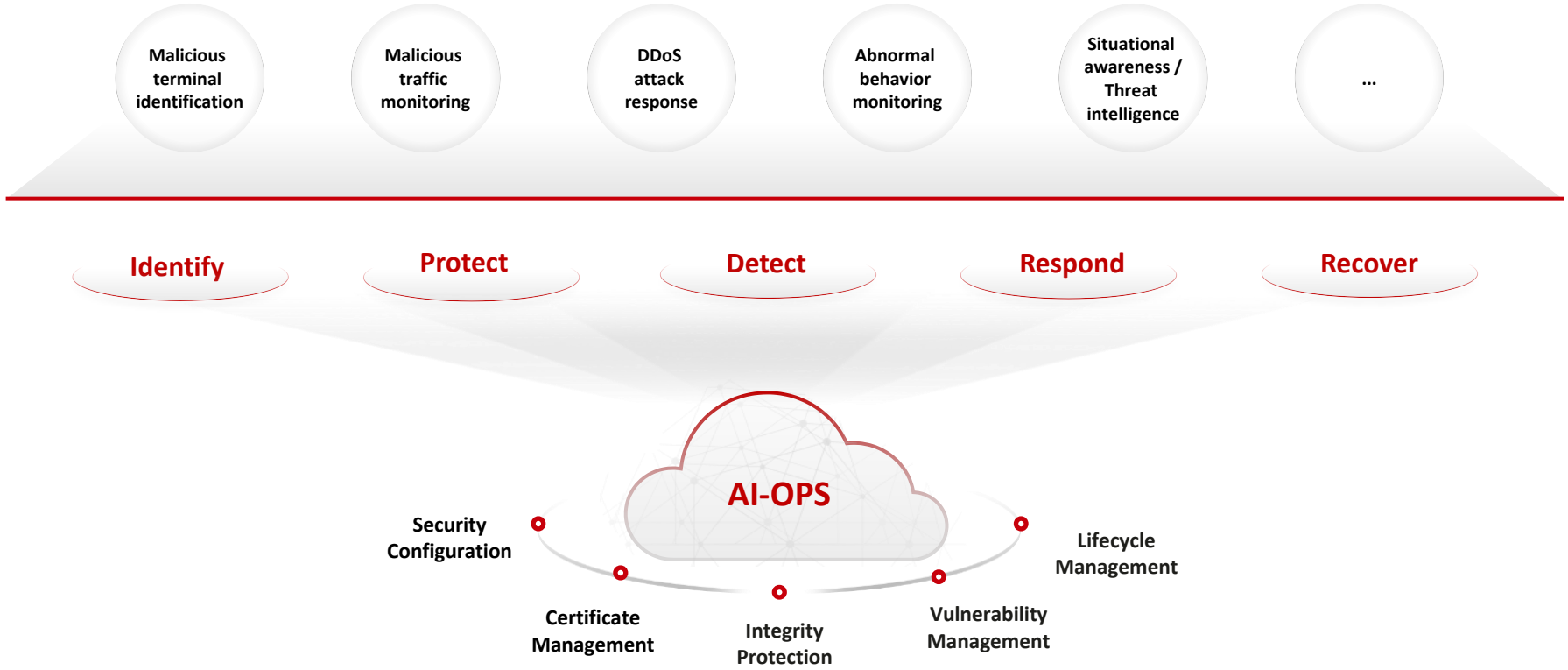
Case 1: Security Development and Test Assistant



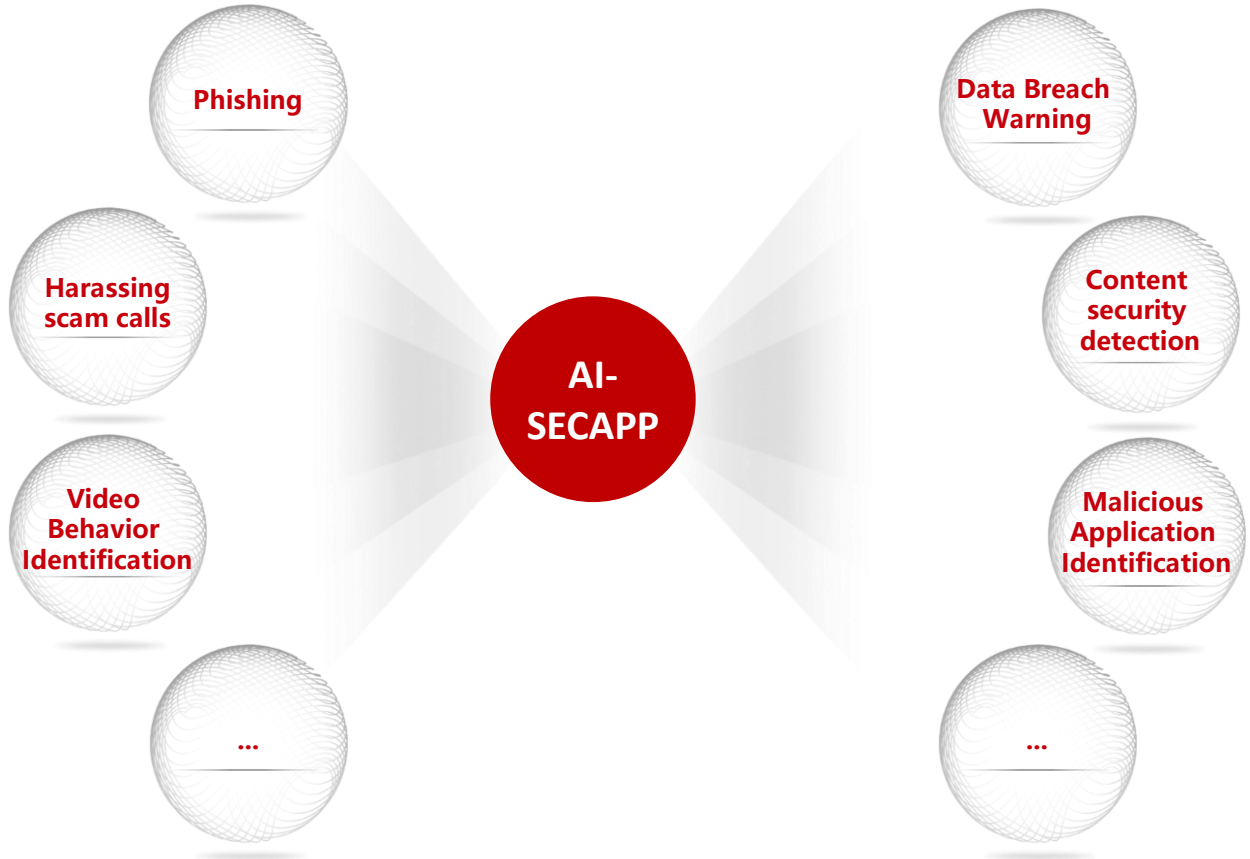
AI assisted software development

- Enabled by Pangu R&D Model, supports mainstream IDEs and programming languages
- ***Automatic generation*** of code/test cases/test scripts, ***efficiency increased by 20%+***
- ***Intelligent Q&A & Collaboration*****,** one-stop application deployment

AI-based Network Deployment and O&M | AI-OPS Helps Enterprises Deploy and Operate Resilient Networks

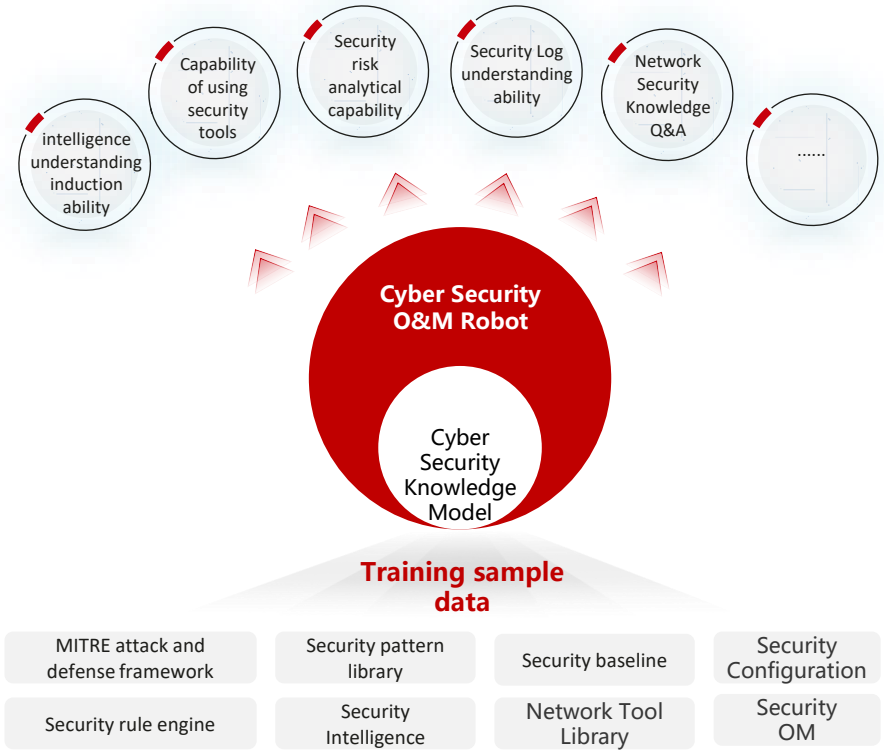


AI application security | AI Identifies Malicious Content and Security Traps, Helping Users Identify Phishing Emails and Internet Fraud

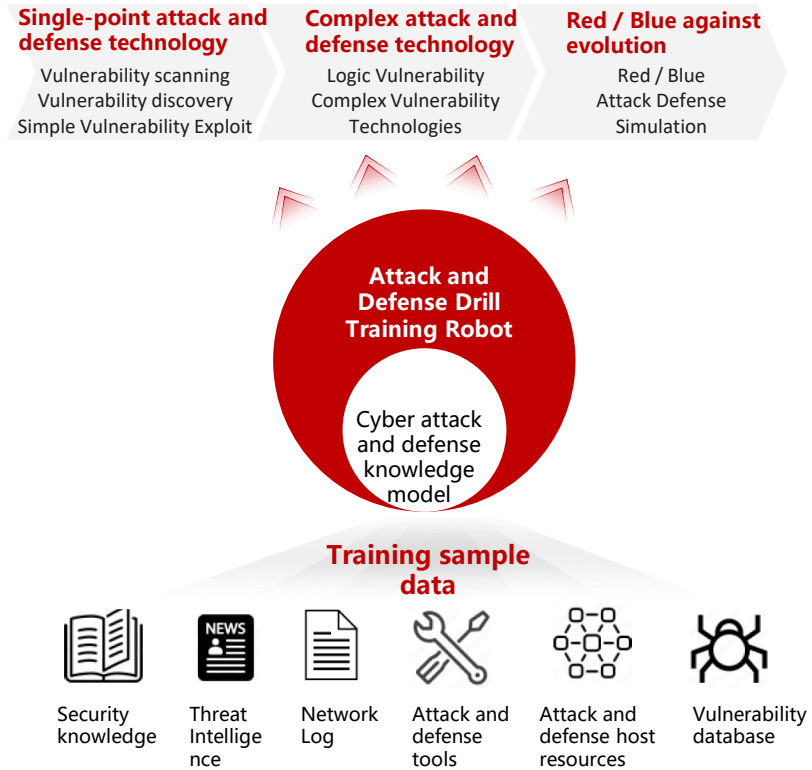


AI for Security Case Study

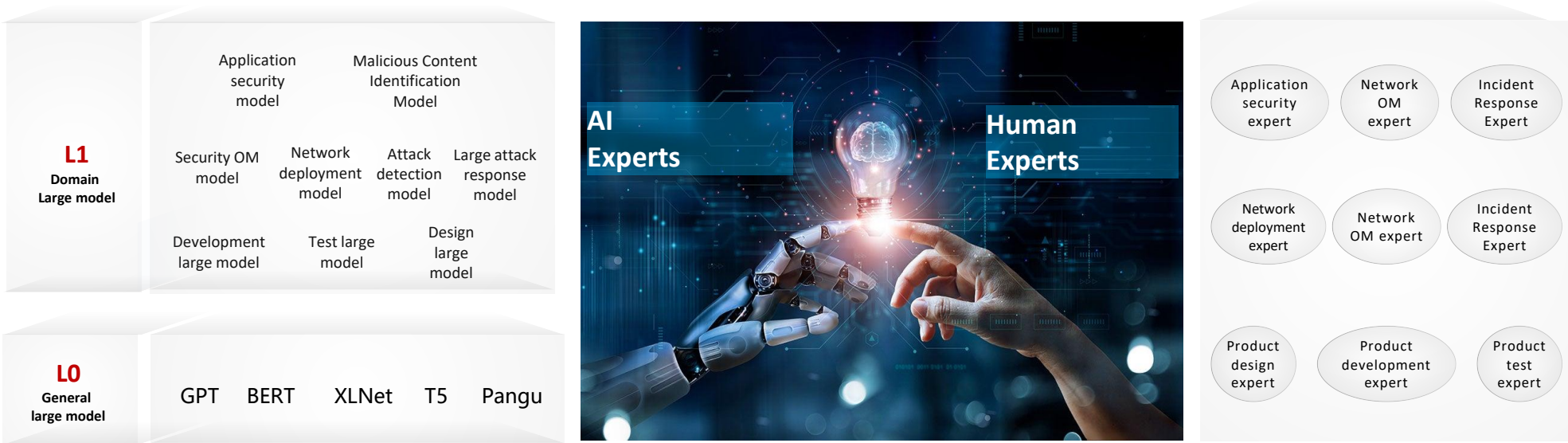
Case 2: Network Security O&M Robot



Case 3: Attack-defense Drill Training Robot

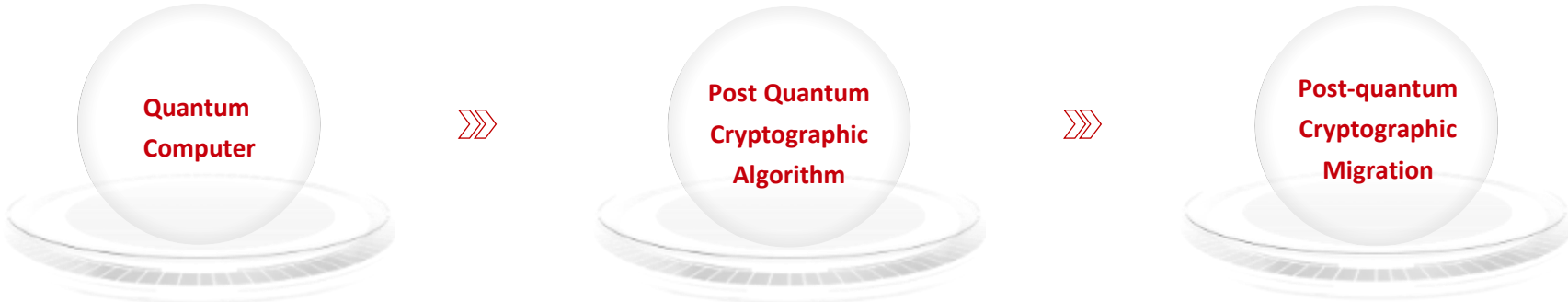


AI for Capability Improvement | AI Experts and Human Experts Improve Each Other's Capabilities



AI experts and human experts learn from each other and improve each other. Human experts train better domain expert models, and AI experts help human knowledge learning and capability improvement.

Post-quantum Cryptographic Algorithm & Migration | Building a Trust Foundation for the Digital World in The Post-quantum Era



Thank you.

把数字世界带入每个人、每个家庭、
每个组织，构建万物互联的智能世界。

Bring digital to every person, home and organization for a fully connected, intelligent world.

HUAWEI


MWC24

Moderator: Sam Barker

Juniper Research

Mikko Karikytö

Ericsson

Dr Galina Pildush

Palo Alto Networks

Nagendra Bykampadi

Rakuten Symphony


MWC24