Achieving Manageable Security, Why and How?

Kev Hau
Head of Security Engineering, North Asia
Cyber Security Evangelist, Office of the CTO
Kevh@checkpoint.com
Check Point: The Largest Global Cyber Security Company

Global Leader - 100,000+ Customers, 88+ Countries, 6,200+ Partners

Over 25 years of cutting-edge technologies, Industry's most visionary player

Innovation leadership - highest number of real-time prevention techniques

Traded on Nasdaq since 1996 - CHKP

6,000+ Employees worldwide, top talent

TRUSTED BY FORTUNE 500 COMPANIES
27 Years of Recognition

**Network:** 21 times Security Leader in Magic Quadrant

**Network:** Customers' Choice for Unified Threat Management

**Network:** Highest cyber prevention score in Breach Prevention

**Endpoint:** Highest coverage of detected attacking techniques

**Endpoint:** Top Product Scoring: 17.5/18

**Endpoint:** A leader in Endpoint Security

**Mobile:** Highest Mobile security value

**Cloud:** Dome9, a cool vendor in Cloud Security

©2021 Check Point Software Technologies Ltd.
THE EVOLUTION OF IT-OT CONVERGENCE

Source: 5 Industrial Connectivity Trends Driving the IT-OT Convergence (iot-analytics.com)
INDUSTRIAL SYSTEMS IN THE ERA OF CONNECTED DEVICES
NEW EDGE-TO-CLOUD ARCHITECTURES

Edge-to-cloud architectures
New technology is enabling edge-to-cloud architectures that bypass the traditional 5-layer stack

Source: 5 Industrial Connectivity Trends Driving the IT–OT Convergence (iot-analytics.com)
TODAY'S ENTERPRISES ARE HYPER-DISTRIBUTED

Applications are distributed everywhere

Remote user access is the new normal
We need a lot of small army to protect us
CYBER TEAMS ARE FIGHTING THE WAVES

Increasing attack complexity and frequency

Overwhelming amount of alerts

Skillset shortage

Incident detection and handling takes too long

62% of companies are being attacked at least on a weekly basis

11,000+ alerts on average, per day, received by Internal security operations teams.

82% of employers report a shortage of cybersecurity skills.

71% believe this talent gap causes direct and measurable damage to their organizations
SECURITY OPERATION CHALLENGES TODAY

- No central platform to manage security operations
- Explosion of security tools in use that were not designed to work together
- Manual, inconsistent processes
- Alert overload
- Global talent shortage
- Difficulty rising above the daily firefighting to track KPIs and drive improvement
OUR FOCUS
THE BEST SOLUTIONS FOR CUSTOMERS' MOST PRESSING CYBER NEEDS

YOUR NEEDS:
1. SECURE
2. SIMPLER
3. INTEGRATED

OUR PRINCIPLES:
1. BEST PREVENTION
2. GOLD STANDARD MANAGEMENT
3. CONSOLIDATED SOLUTION
WHAT IS CHECK POINT INFINITY?

Cybersecurity Architecture

Secure Your Everything

All Inclusive Consumption Model

Simple and Predictable

Hardware  Software  Subscription

Service  Support

Hardware  Software  Subscription

Service  Support
QUANTUM NETWORK SECURITY
Holistic Network Attack Mitigation Solution

Always-On
On Demand
Hybrid Mode

SCRUBBING CENTER
3.5Tbps
Mitigation Capacity

DDOS PROTECTOR
6 – 400Gbps
Mitigation Capacity

NETWORK THREAT PREVENTION
100Mbps – 1.5Tbps
Threat Prevention Throughput

Check Point Appliance
Bare Metal
Virtualized Security GW
Cloud Service

Micro-Segmentation | Security Service Insertion | Auto-Provisioning | Automation
FIRMWARE SECURITY ASSESSMENT
Identify device security flaw

NANO AGENT SECURITY
On-device runtime self-protection

- Memory corruption
- Shell injection
- Import table hijacking
- Control flow hijacking

Cloud Based Management
INFINITY MANAGEMENT

- Weak/Known Credentials
- Software Misconfigurations
- Known Vulnerabilities (CVEs)
- Suspicious Listed Domains

Linux over ARM32/ARM 64
* Additional OSs coming soon
HARMONIZING SECURITY WITH CHECK POINT HARMONY
MORE THAN SASE….
CloudGuard Unified Security Platform

- Workload Protection
- Security Posture
- Network Security
- Threat Intelligence
- Web and API Protection

CloudBots for Auto remediation

Real-time Alerts

- Code
- Containers
- Vulnerabilities
- CI/CD

Shift-Left
INFINITY-VISION
UNIFIED MANAGEMENT

Manage the Entire Portfolio from a Single Portal

Cloud-Based Management as a Service

Unified Policy, Monitoring, Intelligence
Expose and Shut Down attacks across Network, Cloud, Endpoint, Mobile and IoT

The Most Powerful Threat Intelligence

The Same Tools that are Used by Check Point Research
Check Point IRT
Incident Response Framework - NIST 800-61

- IR Playbook Development
- Table-top Exercise
- IR Team Training
- Compromise Assessment
- Threat Hunting
- Maturity Assessment
- Building Threat Intelligence
- Dark Web Monitoring

Detection & Analysis
- Malware Analysis
- Compromise Endpoint
- Data Leakage
- Website Defacement
- Suspicious Events
- Quarantine infected machines
- Attack Mitigation
- Prevent lateral movement

Containment, Eradication & Recovery

Review Incident
- Root cause/Attack Analysis
- Forensic Investigations
- Service Recovery
- Incident Report
- Threat Hunting
- Playbook Review

INCIDENT RESPONSE TEAM
CHECK POINT

INCIDENT RESPONSE TEAM
CHECK POINT

INCIDENT RESPONSE TEAM
CHECK POINT
Infinity Total Protection Model

- **HARDWARE**: spend for Network Products
- **CLOUD**: spend for Cloud Products
- **CONSULTING**: spend towards Training, Incident Response, and PS
- **WORKFORCE**: Endpoint, Mobile and SaaS protection for all employees
- **SUPPORT**: Threat prevention & 24x7 Premium Support

**SIMPLE, PREDICTABLE - ALL USERS, ALL INCLUSIVE**
Summary

Manage security operations from a single platform

Orchestrate tools to work together

Create consistent, automated processes and slash response times

Reduce alert overload

Focus limited security talent on higher value work

Track, measure and improve SOC performance
THANK YOU