Cisco & IBM Security
SECURING THE THREATS OF TOMORROW, TODAY, TOGETHER

Nicky Choo
Head, Routes to Market & Business Partners, Asia Pacific, IBM Security & Cloud
Disconnected security capabilities

- Criminal detection
- Fraud protection
- Application security management
- Vulnerability management
- Device management
- Access management
- Identity governance and administration
- Privileged user management
- Malware protection
- Endpoint detection and response
- Malware analysis
- Transaction protection
- Application scanning
- Mainframe security
- Network visibility and segmentation
- Network forensics and threat management
- Incident response
- Security analytics
- Indicator of compromise
- Malware analysis
- Threat sharing
- Threat hunting and investigation
- Disconnected security capabilities
Traditional security practices are unsustainable

- 85 security tools from 45 vendors
- 1.8 MILLION unfilled security positions by 2022
- 68 PERCENT of CEOs are reluctant to share incident information externally

How do I…

- Improve real-time visibility across the diverse threat landscape and disparate technologies
- Effectively detect and respond to malware and advanced threats
- Integrate risk, compliance and security analytics to increase security efficiency
- Streamline security operations against a backdrop of talent and funding shortage
- Focus on regulatory compliance
We exist to protect the world, freeing you to thrive in the face of cyber uncertainty

Largest enterprise cybersecurity provider

Leader in 12 security market segments

3,700+ security patents

20+ security acquisitions

60B+ security events monitored per day
Disconnected security capabilities are failing us

Security analytics

Privileged user management

Access management

User behavior analytics

Data access control

Incident response

Data protection

Endpoint patching and management

Fraud protection

Identity governance and administration

Network visibility and segmentation

Vulnerability management

Network forensics and threat management

Mainframe security

Threat sharing

Application scanning

Malware protection

Criminal detection

Device management

IDaaS

IoCs

Threat and anomaly detection

Content security

Endpoint detection and response

Transaction protection

Endpoint patching and management

Application security management

Malware analysis

Transaction protection

Threat hunting and investigation
Build an integrated security immune system

- **DATA**
  - Data protection
  - Data access control
  - Security analytics
  - Vulnerability management
  - Threat and anomaly detection

- **IDENTITY & ACCESS**
  - Privileged user management
  - Identity governance and administration
  - Access management
  - IDaaS
  - Mainframe security

- **APPLICATIONS (APPS)**
  - Application scanning
  - Application security management

- **MOBILE**
  - Transaction protection
  - Device management
  - Content security
  - Transaction protection

- **ENDPOINT**
  - Endpoint detection and response
  - Endpoint patching and management
  - Malware protection

- **NETWORK**
  - Firewalls and intrusion prevention
  - Network forensics and threat management
  - Network visibility and segmentation

- **THREAT INTELLIGENCE (THREAT INTEL)**
  - Threat sharing
  - Malware analysis
  - IoCs

**Main Features**
- Criminal detection
- Fraud protection
- Application security management
- Application scanning
- Device management
- Content security
- Endpoints protection
- Endpoints patching and management
- Malware protection
- IoCs
- Threat sharing
- Malware analysis
IBM Security Immune System

SECURITY ORCHESTRATION & ANALYTICS
- Guardium
- Key Manager
- Multi-cloud Encryption
- Critical Data Protection Services

DATA
- QRadar
- Resilient
- Watson
- i2

IDENTITY & ACCESS
- Identity Governance & Access
- Cloud Identity
- zSecure
- Identity Management Services

ADVANCED FRAUD
- Trusteer
- Financial Malware Research

NETWORK
- QRadar Incident Forensics
- QRadar Network Insights
- Managed Network Security
- Secure SD-WAN

MOBILE
- MaaS360
- Mobile Device Management

ENDPOINT
- BigFix
- Managed Detection & Response
- X-Force IRIS

APPLICATIONS (APPS)
- AppScan
- Application Security on Cloud
- SDLC Consulting
- X-Force Red

PLATFORMS
- X-Force Command Centers

THREAT INTEL
- X-Force Exchange
- Malware Analysis
- X-Force IRIS

SECURITY ECOSYSTEM
- App Exchange
- Hybrid Cloud Security Services

ON PREM | CLOUD | HYBRID
- Products
- Services
Why Are IBM Security & Cisco Partnering?

- Better serve the large number of mutual customers that both companies share
- Joint portfolio of industry leading, complementary solutions that leverage each organization’s strength to deliver more effective security
- Market leaders in respective segments, industries with a 360° alliance
- Highest levels of executive sponsorship and engagement
Two Trusted Advisors: IBM Security & Cisco

- **Simple**
  Breakdown siloes and reduce complexity via a collaborative approach, self-deployed or turnkey via IBM services

- **Open**
  Feature rich extensions and integrations that deliver security outcomes across the diverse threat landscape

- **Orchestrated**
  Rapidly detect and respond to advanced threats via a drillable dashboard of key Cisco threat telemetry from a single pane of glass
Cisco Security and IBM Security Together

Ingest
Cisco threat and networks telemetry

Apply
IBM QRadar Security Analytics & Watson AI engine

Identify & Prioritize
Capture & classify threats for faster response

Orchestrate & Respond
To prioritize incidents with IBM Resilient

QRadar supports over 25 Cisco product families out of the box

Advanced analytics for threat prevention, detection, and response

Orchestrate incident response across people, process and technology
IBM X-Force Threat Management & Cisco Partnership
A Smarter Security Solution to Manage the 360 degree Threat Lifecycle, Aligned to the NIST Framework

**Insight**
- Cisco Firepower (Network Discovery), AMP for Endpoints, Security Online Visibility Assessment (SOVA)
- Cisco AMP IR Package and Umbrella
- Cisco Stealth Watch & Firepower
- Cisco Talos Threat Intelligence

**Prevention**
- Cisco StealthWatch Cloud, CloudLock, AMP, Umbrella, FirePower, ISE, ESA, WSA, AnyConnect
- Cisco ISE and FirePower

**Detection**
- Cisco Umbrella Investigate, AMP Visibility, Threat Grid, Talos

**Response**
- Cisco Security Services (augmentation & special domain expertise)
- Cisco Rapid Threat Containment
- Cisco AMP IR Package, Umbrella, Talos

**Recovery**
- Cisco FirePower Mgmt Console
- Cisco, Security Online Visibility Assessment (SOVA)
- Cisco Security BU engineering
- Dedicated Security Consulting Engineer

**Metrices & Reporting**
- Issue Management
- Change Management
- Enhancements

**Governance**
- Programmatic Framework:
  - Maturity Approach
  - SOC Use Case Library
  - Response Playbooks
- X-Force Expertise:
  - Security Testing
  - 24x7 Command Centers
  - Incident Response
- Smarter Platform:
  - QRadar analytics and Watson AI
  - Resilient intelligence orchestration
  - Mobile App
Security Hub – Zero Trust Security – Cisco Firepower is the heart of the IBM Security Architecture

**Zero Trust Security**
- Secure Application Access to Simplify the Network and Enable Virtualized Cloud & Data Center Services
- Strong Security for users
- Secure Multi-Cloud Application Protection

**Software-Defined Security Benefits**
- Programmable Security
- End-to-End Segmentation
- Agile Security Services

**IBM Security Hubs**
- High Feature Security Services
- Maximized Network Availability with Any Network Transport.
- Secure and resilient high availability Network with Strong Encrypted Zero Trust Security

**Integrated Security**
- Network and Security Integrated together
- Proactive Analytics
- Secure Guest Access

**Any Person, Anywhere, Any Department, Any Device**

**Strong Security for all locations:**
- Firewall, IDS, IAP, DDoS, Malware-AV, DNS Firewall, Ransomware, Anti-Spam, URL Filtering, SSL VPN, IPSec, User FW Machine ID
IBM Security and Cisco Join Forces to Tackle Cybercrime

Offering integrated technologies, services and threat intelligence collaboration

<table>
<thead>
<tr>
<th>Products</th>
<th>Threat Intelligence</th>
<th>Managed and Consulting Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Analytics</td>
<td>Incident Response</td>
<td></td>
</tr>
<tr>
<td>IBM QRadar SIEM, UBA &amp; Watson for Cyber Security</td>
<td>IBM Resilient</td>
<td>X-Force Threat Management Security Hub</td>
</tr>
<tr>
<td>Cisco Firepower, Cisco Cloud (Umbrella, Cloudlock), Stealthwatch</td>
<td>Cisco Identity Services Engine (ISE)</td>
<td>Services above based on wide variety of Cisco Security products</td>
</tr>
<tr>
<td>Cisco Threat Grid, ASA, ESA, WSA, Netflow, Routers, Switches, IOS</td>
<td>Cisco Threat Grid, Cisco Umbrella Enforcement &amp; Investigate</td>
<td></td>
</tr>
<tr>
<td>Cisco Threat Grid, ASA, ESA, WSA, Netflow, Routers, Switches, IOS</td>
<td>Cisco Threat Grid, Cisco Umbrella Enforcement &amp; Investigate</td>
<td></td>
</tr>
<tr>
<td>Cisco Threat Grid, ASA, ESA, WSA, Netflow, Routers, Switches, IOS</td>
<td>Cisco Threat Grid, Cisco Umbrella Enforcement &amp; Investigate</td>
<td></td>
</tr>
</tbody>
</table>
WannaCry Ransomware

- Leverages known exploits
- Infiltrates endpoints, encrypts all files, demanding a $300 USD ransom in bitcoin
- Exploits a known Windows vulnerability that enables remote code execution (patch available since March)
- Crippled at least 100K organizations across multiple industries in over 150 countries
- 300k+ infected endpoints
- Cisco TALOS and IBM X-Force IRIS teams collaborated in support of our mutual customers, and continue to work together on leading threats

X-Force Exchange integrates with Cisco Threat Grid
Ecosystem of Collaborative Defenses: IBM Security App Exchange

Share and download apps based on IBM security technologies

- 175+ IBM and partner Apps
- 100K+ app downloads
Cisco Apps for IBM Security

Better and deeper integrations via out-of-the-box extensions and apps between Cisco, QRadar and Resilient that remove integration costs from your business

Detect and respond to threats faster via deep visibility and actionable insights into the most critical threats (based off of Cisco’s threat telemetry) from a single dashboard

Improve SOC effectiveness via simple and streamlined operations including drillable dashboards and workflows direct from QRadar and Resilient vs toggling between disparate views
Stop Threats at the Edge with Cisco Firepower and IBM QRadar

**Before the App**

- Firepower sends large volumes of event types to QRadar in most environments, and customers need to tune their SIEM accordingly.

- QRadar SIEM prioritizes threats, but didn’t always deliver full depth of Firepower insights.

**After the App**

- The Firepower App for QRadar streamlines investigations into critical security event information.

- The App provides a new drillable QRadar dashboard that delivers a consolidated view of key Firepower metrics and easy, direct access to underlying data.

- Prioritizes information about intrusion activity through easy to understand graphs and metrics.
Cisco Firepower App for QRadar: Stop Threats at the Edge

INCIDENT ALERT

- **Firepower intrusion, advanced threat, or IoC event** happens against high profile asset
- **Firepower “Impact Assessment”** determines asset is vulnerable to this attack and sends a Severity 1 event to QRadar
- **Network analytics detects abnormal behavior**
- **Firepower detects outbound connection to a known ‘bad’ site based on IP, URL or DNS threat intelligence**
- **Watson reveals wider campaign, Malware, other IOCs**

**Asset Database**
**Fully Qualified Event**
**Network Behavior Analytics**
**IP/URL/DNS Threat Intelligence**
**Cognitive Analysis**
Expedite Threat Investigation with Cisco Threat Grid and IBM QRadar

Before the App

• Threat Grid provides automated malware analysis and integrated threat intelligence, from samples submitted by Cisco and 3rd party security products, including IBM Resilient and X-Force Exchange.

• Time consuming to investigate threats and understand the full scope and veracity in context.

• Alert fatigue with the potential of missing alerts in the noise of event data.

After the App

• **Streamlines investigations** into critical security event information, identified by submitting source.

• **Reduce time to detect and respond** to threats on a single interface.

• **Understand the scope and veracity** of threats with right click functionality from QRadar to Threat Grid for deeper malware analysis (ex. hash values, IPs)
Cisco Threat Grid App for QRadar: Expedite Threat Investigation

**INCIDENT ALERT**

1. **Unknown Threat**
   - QRadar generates a security offense, including a suspicious file.

2. **Submit Sample to Threat Grid**
   - File is submitted to Threat Grid for dynamic and static malware analysis.

3. **Automated Malware Analysis**
   - Threat Grid analyses the behavior of the sample and determines a threat score, 70+ displayed in QRadar App.

4. **Alert and Pivot to Report**
   - Analyst alerted to samples with high threat to network, and single click to view analysis report in Threat Grid.

5. **Intelligence and Response**
   - Threat Grid provides integrated behavior and threat intelligence to take incident response action with Resilient or other remediation.
Address these concerns:

• Unmanaged or unknown users on the network
• Limited contextual awareness of users & devices
• Non-compliant devices with expired or invalid antivirus software
• Unable to enforce consistent security policies inside the network
• Inability to segment and contain threats on the network
The App Now Accelerates...

- **Policy enforcement everywhere** in complex security deployments from the network to the endpoint and cloud.

- **Streamlining threat containment** by invoking quarantine actions on ISE pxGrid from the QRadar console.

- **Time to identify** unknown or unmanaged devices roaming on the network, including Internet of Things devices.

- **Understanding the scope and veracity** of “at-risk” users and devices through a single, aggregated QRadar dashboard, drilling down into targeted endpoints.
Incident Response: How Can Organizations Address these concerns:

• Understand step by step what happened in a security incident and breach

• Respond quickly and effectively to a security incidents

• Maintain compliance with breach and security incident response requirements

• Understand what threats the organization is experiencing and the effectiveness and cost of response and management

• Be ready to respond to a breach or the next major zero day
Orchestration Goes Beyond Incident Response

**ORCHESTRATION** is the coordination of activities, both human and automated (people, process, technology)

**AUTOMATION** is taking action without human intervention.
Resilient Intelligent Orchestration

Orchestrate IR With Dynamic Workflows

**Components**

**People**
Identify tasks that require human action

**Process**
Enforce order and dependencies to perform correct tasks

**Technology**
Leverage technical integrations and automation

**Initiate response to ransomware attack.**

- Verify affected assets
- Identify affected assets
- Identify ransomware variant
- Determine scope and recoverability
- Recover data from backdrop
- Ban hash via AV utility
- Isolate backup media from network
- Block IP addresses & URLs
- Alert legal department
- Determine value if unrecoverable
- Post-incident review, update playbook

Response completed.
Cisco Threat Grid & Resilient: Orchestrate Incident Response

- Incident analysis and root cause
- Orchestrated response with best practice playbooks and automated response
- Endpoint activity visibility and action
- Network data forensics gathering additional evidence
- Coordinated response across Sec Ops, IT, Legal and Comms

Cognitive Analytics
Orchestration & Playbooks
Endpoint Integration
Network Insights & PCAP
Built-in Compliance Intel

RESPONSE SPEED
What Makes Cisco & IBM Security A Better Option….

Eliminate blind spots created by unknown or unmanaged devices roaming on the network, including Internet of Things devices.

Gain full visibility of all users, devices, network activity and see authentication and remediation data in a single dashboard vs toggling between disparate tools.

Prioritized set of alerts based on QRadar advanced analytics applied to Cisco event/threat data including offense chaining that correlates malicious activities around asset, user, domain…. into a single incident.

Enforce policies and contain threats everywhere from the network to the endpoint to users and cloud.

Simplify and expedite incident response by taking immediate remediation actions (ex. quarantine) directly from the QRadar interface and orchestrating incident response directly from Resilient based on Cisco threat telemetry.
Cisco and IBM
Join Forces to Fight Cybercrime
Integrated Solutions At-a-Glance

Applications
Cisco integrated security portfolio with IBM QRadar and Resilient for rapid analysis and remediation

Threat Intelligence
Facilitate collaboration between two leading threat research teams: IBM X-Force and Cisco Talos

Services
IBM Consulting and Managed Security Services team collaborating with Cisco to deliver new services to further reduce complexity for customers
THANK YOU

FOLLOW US ON:

- ibm.com/security
- securityintelligence.com
- ibm.com/security/community
- xforce.ibmcloud.com
- @ibmsecurity
- youtube/user/ibmsecuritysolutions