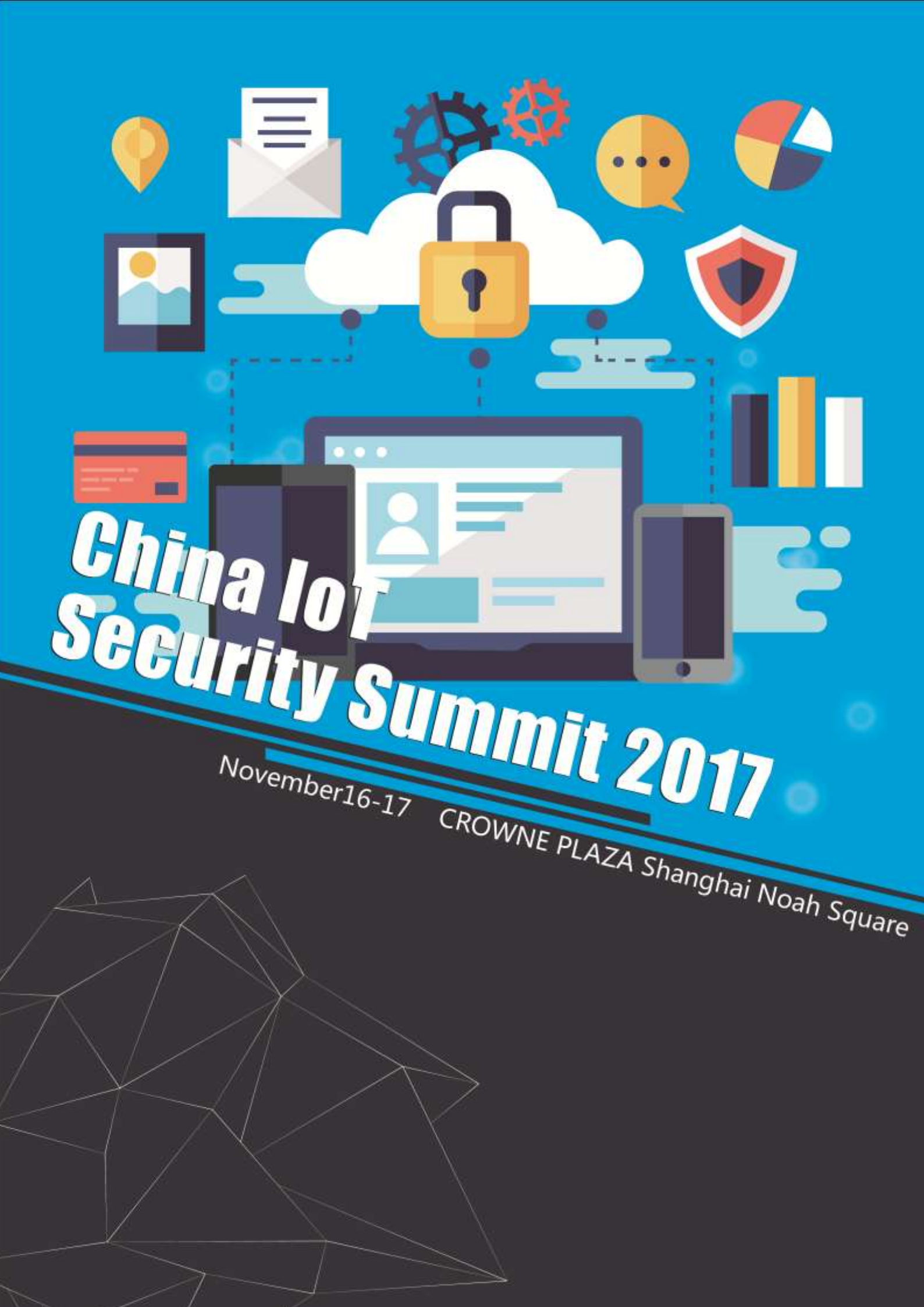

China IoT Security Summit 2017

November16-17 CROWNE PLAZA Shanghai Noah Square

China IoT Security Summit 2017

November16-17 CROWNE PLAZA Shanghai Noah Square

➘Highlights

- ‘Internet Security Law of the People's Republic of China’: Formal Legislation Enhanced Information Security
- Overall Outlook of IoT Security Market and Potential Threats Forecast Analyze
- The Practice of Building an Comprehensive IoT Security Ecosystem
- IoT Gateways Secures Devices’ Communication and Enables a Secured IoT Environment
- Network Operator’s Support to the Protection IoT Security
- IoT Platform’s Security Practice
- Secured IoT Cloud Platform Boost the Development of IoT Industry
- Converge IT and OT to Accelerate Secured IIoT Ecosystem Development
- Industrial Control Systems Security Gap Assessment Engages IIoT Development
- Utilize the Advanced Technologies to Build Security in the Smart Plant
- Panel Discussion: How to Achieve ‘Security’ in the IoT Era
- Designing Automotive Security For Connected Vehicles
- Ensure Security of IoT from Botnet Attacks
- Eliminate Smart Home Appliances Security Risks, Enhance User Safety
- Medical Device in the IoT Era: Prioritize Security Measures
- Binding the User and Devices to Create a Secured Usage Mode
- Blockchain’s Potential of Solving IoT Security Threats
- Machine Learning Helps to Close IoT Vulnerabilities
- Enhance Enterprise IoT Endpoint Security Management System
- IoT-based Smart Grid Security Issues and Challenges

Organizer: ECV we create value and strive for excellence

Media Support: TechWeb www.techweb.com.cn; ZD至顶网; eNet硅谷动力.com.cn; ebrun亿邦动力 www.ebrun.com; 大数据周刊 BIG DATA; 物联网世界 iotworld.com.cn; 数据猿 DataYuan.cn; OFweek 工控网; 广告买卖网 admaimai.com; 前瞻网 qianzhan.com; 贝多罗

China IoT Security Summit 2017

November16-17 CROWNE PLAZA Shanghai Noah Square

Background

IoT means our physical work is connected to the virtual world, and they could affect each other. IoT is no more a word but what is really happening in our daily life and production. The advanced technologies led to IoT developments including: machine-to-human communication, machine-to-machine communication, radio frequency identification, robotics and etc. According to IDC, the IoT market size will reach 170 billion dollars, and there will be 20 billion connected devices in 2020. In another hand, some hackers are also aimed at this huge market, there are many new type of IoT specified attacks, such as Mirai attack in the USA. The difference between IT security and IoT security is that IoT attacks could manipulate some physical devices, and may cause physical damages, the consequence could be not only financial lost, but also affect harm human's safety. IoT security issues are the concerned by all the IoT industry stakeholders. In this case, to build a secured IoT ecosystem is essential to all the IoT business operators and users.

The China IoT Security Summit 2017 aims to bring together about 150+ the most influential experts, business leaders and researchers to analyze the IoT security market situation and the effects of China's new version 'Internet Security Law', share the most popular IoT security technologies, and discuss the possible future of IoT security. This event will be a great platform to get a deep understanding of the market, learn knowledge and business networking.

Attendees

Presidents
Vice Presidents
Chief Executive Officer
Chief Information Safety Officer
Chief Information Officers
Chief Technology Officer
Chief Strategy Officers
Chief Risk Officer
General Managers
Engineering Director
Product Engineer
International Sales
Business Development Directors
Regional Directors
Marketing Directors
Marketing Managers
Partners

Sectors

Network Providers
Cyber Security Solution Providers
Semiconductor Manufacturer
Factories
OEMs
Component suppliers
System Integrators
Distributors
Smart Home Enterprises
Automotive Enterprises
Industrial Companies
IoT Security Research Institute
Healthcare Companies
Mobile Phone Manufactures
Third Party Payment Institution
Medical Device Manufacturers

Guest Speakers

National Research Center for Information Technology Security
Gartner
Huawei
Intel
China Mobile
Aliyun
Siemens
GE
General Motors
Symantec
Midea
Medtronic
Tencent
IBM Security
360
State Grid Corporation of China

China IoT Security Summit 2017

November16-17 CROWNE PLAZA Shanghai Noah Square

Day One

08:30 **Check-in and Registration**

09:00 **'Internet Security Law of the People's Republic of China': Formal Legislation Enhanced Information Security**

- Essential Measurements to Keep Information Security in the IoT Era
- Impacts on Global ICT Enterprises to Operate in China
- In Time Response and Implement the Network Security Risk Contingency Plan

Cao Yue
Deputy Director General
National Research Center for Information Technology Security

09:35 **Overall Outlook of IoT Security Market and Potential Threats Forecast Analyze**

- Current IoT Security Market Size Evaluation
- The Potential Threats Analyze
- Opportunities and Future Trend Forecast

Earl Perkins
Vice President, IoT
Gartner

10:10 **Tea Break and Networking**

10:40 **The Practice of Building an Comprehensive IoT Security Ecosystem**

- Multilayered End-to-End Security System
- IoT Security Practices
- The Challenges During the Process

Jiang Wang Cheng
CEO, IoT Solution Center
Huawei

11:15 **IoT Gateways Secures Devices' Communication and Enables an Secured IoT Environment**

- The Difficulties of Integrate and Secure Different Protocols
- How to Achieve Encryption and Authentication for Devices
- Real Time and Efficient Process Control

Rose Schooler
Vice President, IoT Strategy and Technology
Intel

11:50 **Network Operator's Support to the Protection IoT Security**

- NB-IoT Boost the IoT Development
- Data Transmission Encryption Technology
- Network Operator's Support for IoT Internet Service and Asset Protection

Liu Zi Qian
Chief Scientist, Communication Research Institute
China Mobile

12:25 **Lunch and Networking**

14:00 **IoT Platform's Security Practice**

- Security Challenges within IoT Platform
- Strengthen IoT Network Architecture from Each Layer
- Elements Need to Be Considered For IoT Platform Security

Open for Sponsor

China IoT Security Summit 2017

November16-17 CROWNE PLAZA Shanghai Noah Square

14:35 **Secured IoT Cloud Platform Boost the Development of IoT Industry**

- How to Achieve A Successful and Long-Term IoT Development by Secured Cloud Technology
- Cloud Providers' Standards of Security May Different From Users
- Data Transmission Encryption
- Case Study

Su Jian Dong
Director, Security Solutions
Aliyun

15:10 **Tea Break and Networking**

15:40 **Converge IT and OT to Accelerate Secured IIoT Ecosystem Development**

- Indirect Connectivity Could Exposure the Industrial IoT Devices and Systems' Vulnerabilities
- The Conflicts Caused by Unmatched Advanced Software and Dated Machines
- Extend and Secure the End-point Lifecycle
- Biometrics Application of Device Access

Rajiv Sivaraman
Vice President, Head of Plant Security Services
Siemens

16:15 **Industrial Control Systems Security Gap Assessment Engages IIoT Development**

- The Limitations of Vulnerability Monitoring Tools
- The Potential Threats Caused by Open System
- Measurements of ICS Security Gap Assessment
- Case Study

Open For Sponsor

16:50 **Utilize the Advanced Technologies to Insure Security in the Smart Plant**

- Use Digital Twin Simulation Method
- The Consequences of Legacy Systems
- The Problems Led by New Technology Integration and Application
- New Security Frameworks
- Case Study

Bram Klijsen
Vice President, Software Development
GE Digital

17:25 **Panel Discussion: How to Achieve Security in the IoT Era**

- The Necessity of IoT Security
- What Kind of Malicious Attacks May Affect People in the Next Few Years
- The Most Vulnerable Parts in the IoT Ecosystem
- The Internet Security Regulations' Influences
- Business Model

World Famous IoT Security Industry Companies

18:25 **End of Day One**

Day Two

09:00 **Designing Automotive Security For Connected Vehicles**

- Potential Damages Caused by Connect Vehicle Cyber Security
- Autonomous Driving Security Design Concerns

China IoT Security Summit 2017

November16-17 CROWNE PLAZA Shanghai Noah Square

- Vehicle to X Communication Security Plan

Jeff Massimilla
Chief Cybersecurity Officer
General Motors

09:35 Ensure Security of IoT from Botnet Attacks

- Enhance the IoT Devices Security and Avoid Attacking
- Strong Authentication
- Construction of the Iot Security System

Ameer Karim
Vice President and General Manager of IoT Security
Symantec

10:10 Tea Break and Networking

10:40 Eliminate Smart Home Appliances Security Risks, Enhance User Safety

- Smart Home Appliance Design
- Transmission Encryption
- Problems Caused by System Diversity
- The Limitations of Traditional PKI Encryption System
- The Future of A Secured Smart Home System

Li Qiang
President, Smart Home Research Institute
Midea

11:15 Medical Device in the IoT Era: Prioritize Security Measures

- Maintaining the Privacy of Patient Records
- Threats Detection
- Prevent Remote Hijacking
- Case Study

Matt Russo
Senior Director, Product Security
Medtronic

11:50 Binding the User and Devices to Create a Secured Usage Mode

- User Identification and Mobile Payment Security Issues in the IoT Era
- TUSI Certification Standard for the IoT Industry
- The Emerging Threats during Mobile Payment

Shen Zi Xi
Deputy General Manager, Mobile Security
Tencent

12:25 Lunch and Networking

14:00 Blockchain's Potential of Solving IoT Security Threats

- Makes Trusty, Peer-to-Peer Messaging Possible
- Enables Autonomous Functioning of Smart Devices
- Create a Resilient Eco-system
- Shortcomings of Blokchain in IoT Security

Open for Sponsor

14:35 Machine Learning Helps to Close IoT Vulnerabilities

- Efficiently Malware Detection
- Superior Data Analyzing Abilities
- The Challenges of Applying Machine Learning

Caleb Barlow
Vice President
IBM Security

15:10 **Tea Break and Networking**

15:40 **Enhance Enterprise IoT Endpoint Security Management System**

- Internet Deployment
- Secure Access Systems
- Isolated Network Deployment
- Cascade Control Deployment
- Specialize Security Management System

Zhang Cong
Director, Tian Qing
360

16:15 **IoT-based Smart Grid Security Issues and Challenges**

- Smart Gird Evolution Brings New Challenges
- Potential for Critical Infrastructure Attacks
- Emerging Smart Grid Cybersecurity Technologies

Chen Chun Lin
Deputy Director, Department of Communication
State Grid Corporation of China

16:50 **End of Day Two**

China IoT Security Summit 2017

16-17 November 2017, Crowne Plaza Shanghai Noah Square

Please complete this form and email back to hilaryl@ecvinternational.com

Registration Form

Organization/Company_____

Address _____

Tel_____ **Fax**_____

Name _____ **Job Title**_____

Tel_____ **E-mail**_____

Name _____ **Job Title**_____

Tel_____ **E-mail**_____

Name _____ **Job Title**_____

Tel_____ **E-mail**_____

Authorization

Name_____ **Job Title** _____ **Payment Manager**_____

Registration Fee RMB 12989 /per person

A. More than 3 delegates enjoy 10% discount.

B. The fee is inclusive of two days conference, conference materials, two luncheons and all refreshments. Accommodation and travel is not included.

C. Simultaneous translation (from Mandarin to English and vice versa) for the entire event.

Payment Method

By TT ☐

You will receive a payment notification after we get your Registration Form.
Payment is required within 5 working days on receipt of the payment notification.

By other Method ☐

If TT transfer is not convenient for you, please inquiry us about other payment method.

General Information

A. The Delegate should pay the total Registration Fee to ECV within Five (5) working days upon signing of this agreement by both Parties.

B. Should Delegate cancel the Registration, a charge of 50% of the Registration Fee, plus 10% administrative charge will be billed by ECV to Delegate for the cancellation received by ECV in writing at least FOUR (4) weeks prior to the commencement of the Event.

C. Cancellations by Delegate less than FOUR (4) weeks prior to the commencement of the Event will not be accepted and payments will not be refunded and invoiced sums will be payable in full by Delegate.

D. ECV will refund Delegate the entire Registration Fee if the Event is cancelled FOUR (4) weeks prior to the commencement of the Event. ECV will refund Delegate the entire Registration Fee. If, for any reasons, the Event is postponed, ECV will inform Delegate of the postpone in writing at least FOUR (4) weeks prior to the commencement of the Event or ECV will refund Delegate the entire Registration Fee.

For more detailed information, please contact ECV International.

Ms. Hilary Liu Tel: +86 21 8026 0708-8057 Fax: +86 21 6605 2939 E-mail:hilaryl@ecvinternational.com