

Cybersecurity Emergency Response

Lecture 10

HCIA-Security

Prepared by
Dr. Abdelrhman Ahmed

- **The Internet of Things (IoT), mobile Internet, cloud computing, and big data are booming. Emerging technologies are reshaping the world. However, cyber security incidents are still on the rise, increasing people's concerns about cyber safety.**
- **In 2017, global cyber attacks, such as WannaCry ransomware, occurred at a high rate. It is difficult to effectively monitor and provide alerts for unexpected global security incidents. Furthermore, nations tend to be reactive instead of proactive when it comes to security incidents. This slide provides references for security incident responses.**

Objectives

- **Upon completion of this course, you will be able to:**
 - ❑ **Understand the background of cyber security emergency response.**
 - ❑ **Describe the handling process of cyber security emergency response.**
 - ❑ **Understand new trends in cyber security emergency response.**

Background of Information Security Emergency Response

- **The Morris Worm Incident, which occurred in November 1988, forced over 10% of Internet systems to stop working. This incident shocked the world and deeply concerned computer science professionals.**
- **A Computer Emergency Response Team (CERT) and the CERT Coordination Center (CERT/CC) for Internet security was founded in 1989 following the Morris worm incident. At that time, the Defense Advanced Research Projects Agency (DARPA) tasked Carnegie Mellon University's Software Engineering Institute (SEI) with developing a communication coordination center to connect experts during security emergencies and to help prevent future intrusion**



CNCERT/CC

- Founded in September 2002, CNCERT/CC is a non-governmental and non-profit cyber security technical center. It is a core organization that helps to coordinate the cyber security emergency system in China.
- CNCERT has actively established international cooperation on cyber security. As of 2017, CNCERT had established "CNCERT International Cooperation Partnership" with 211 organizations in 72 nations and regions.



Forum of Incident Response
and Security Teams



Anti-Phishing
Working Group

CNCERT International Cooperation Partnership



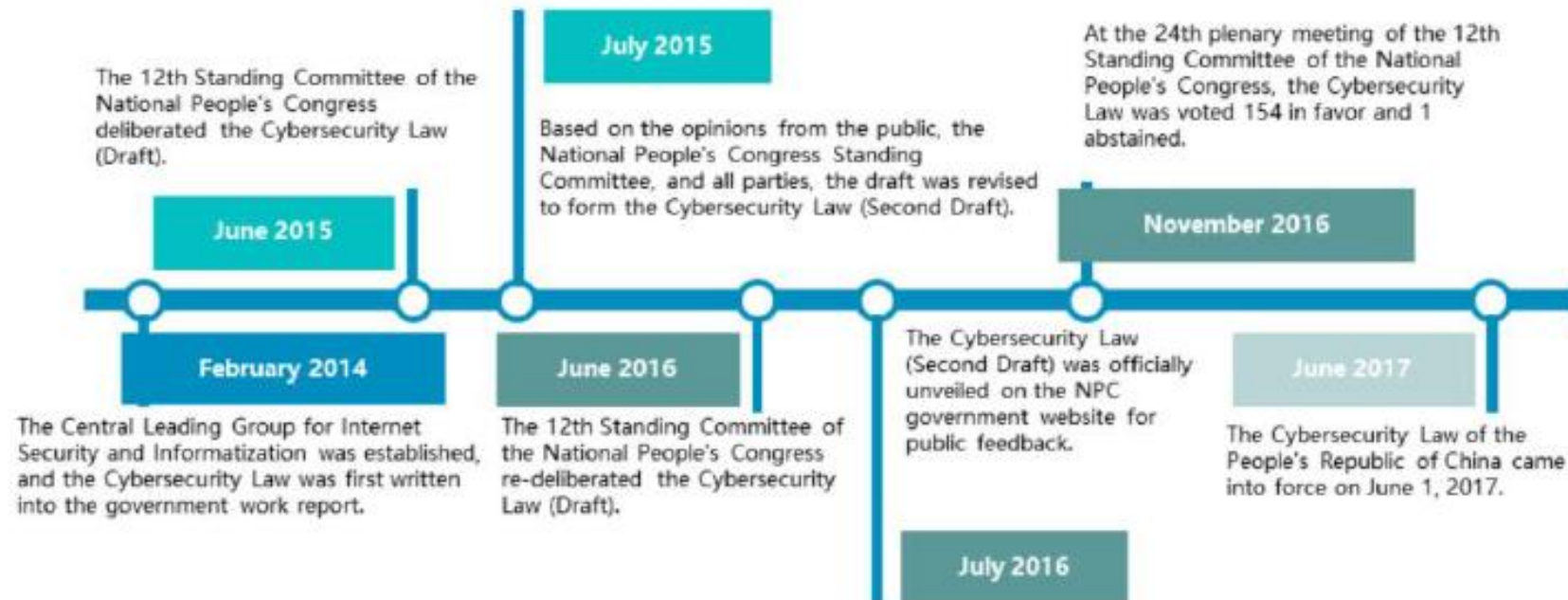
Asia Pacific Computer Emergency Response
Team



Cymru

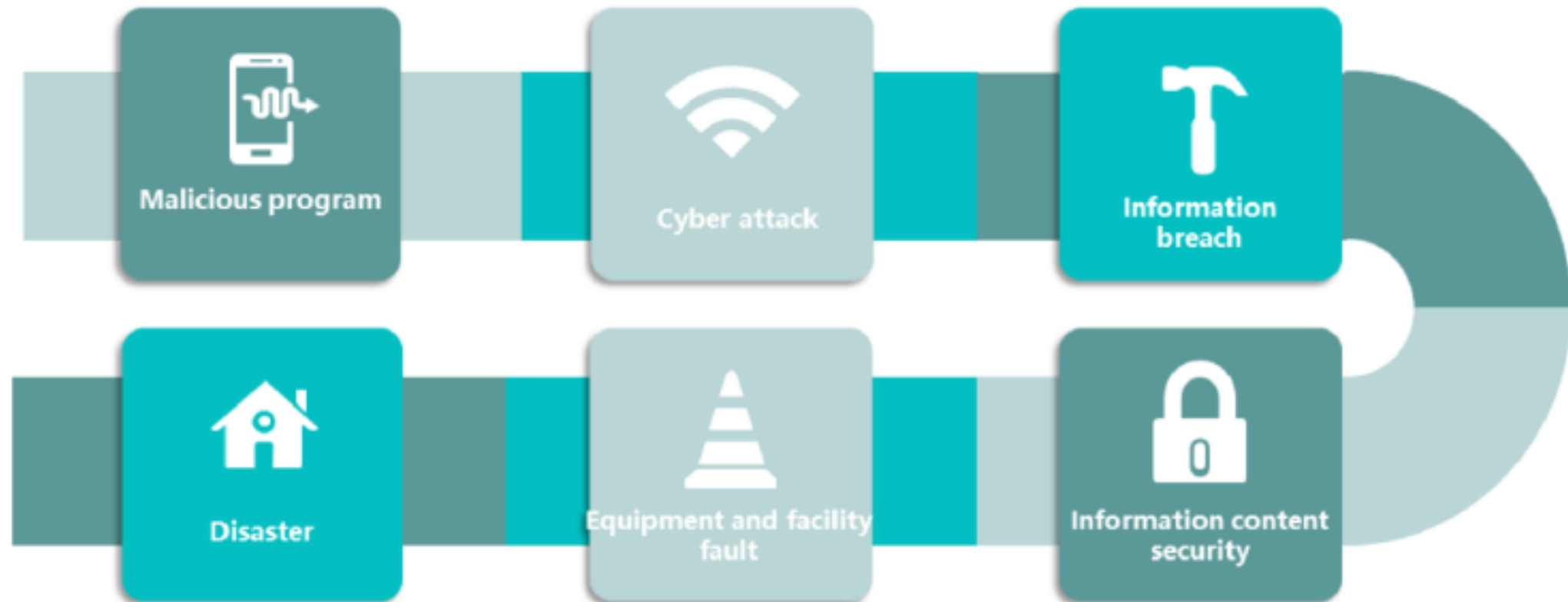
Cyber Security Laws & Regulations in China

- The Cybersecurity Law of the People's Republic of China was adopted by the Standing Committee of the National People's Congress (NPC) in November, 2016 and came into force on June 1, 2017. The Cybersecurity Law is China's first to provide guidelines on cyber security.
- The Cybersecurity Law underwent three years of deliberation before its final release.



Cyber Security Incident Classification

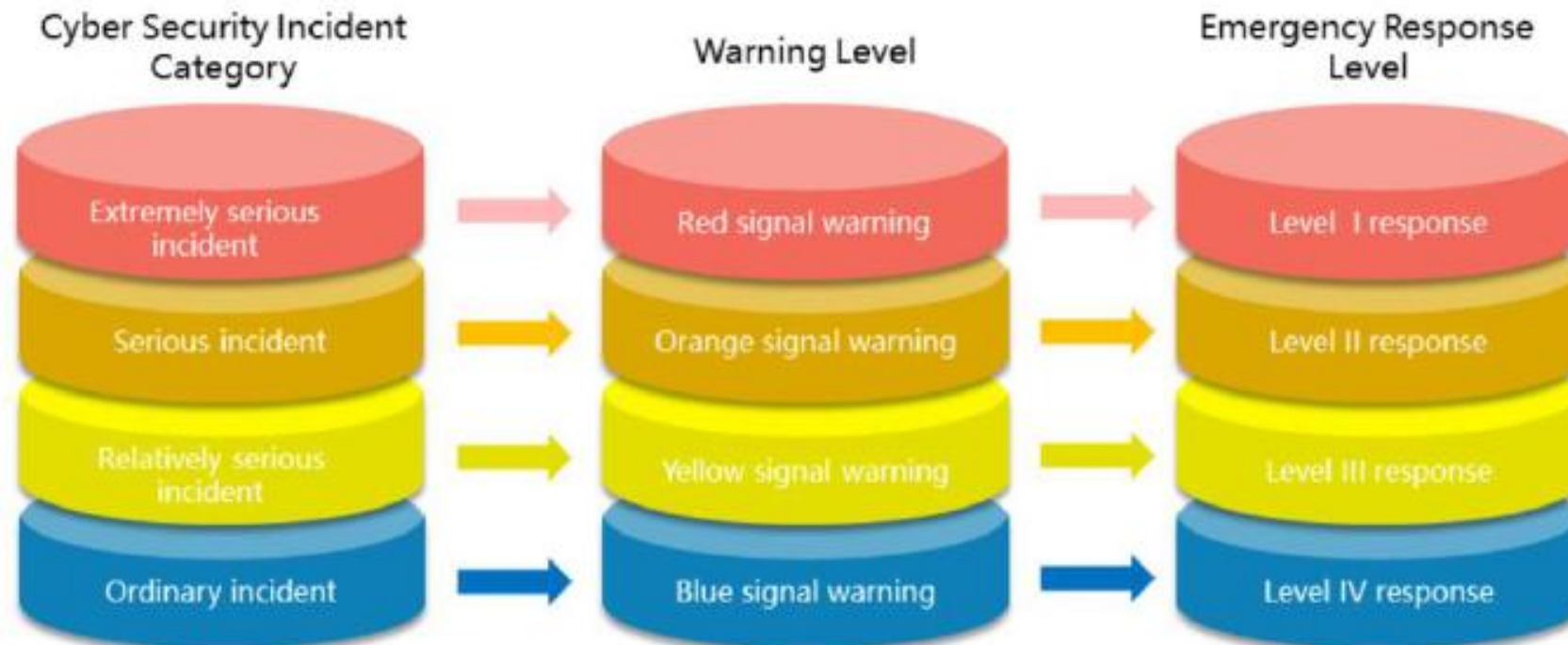
- Cyber security incidents are classified as follows in the National Emergency Plan for Cyber Security Incidents:



Chapter
10

National Cyber Security Incident Categories

- The National Emergency Plan for Cyber Security Incidents clarifies the enforcement solution for Chapter V "Monitoring, Early Warnings, and Emergency Responses" of the PRC Cybersecurity Law. The Plan divides incidents into four categories, which correspond to four warning levels and emergency response levels.



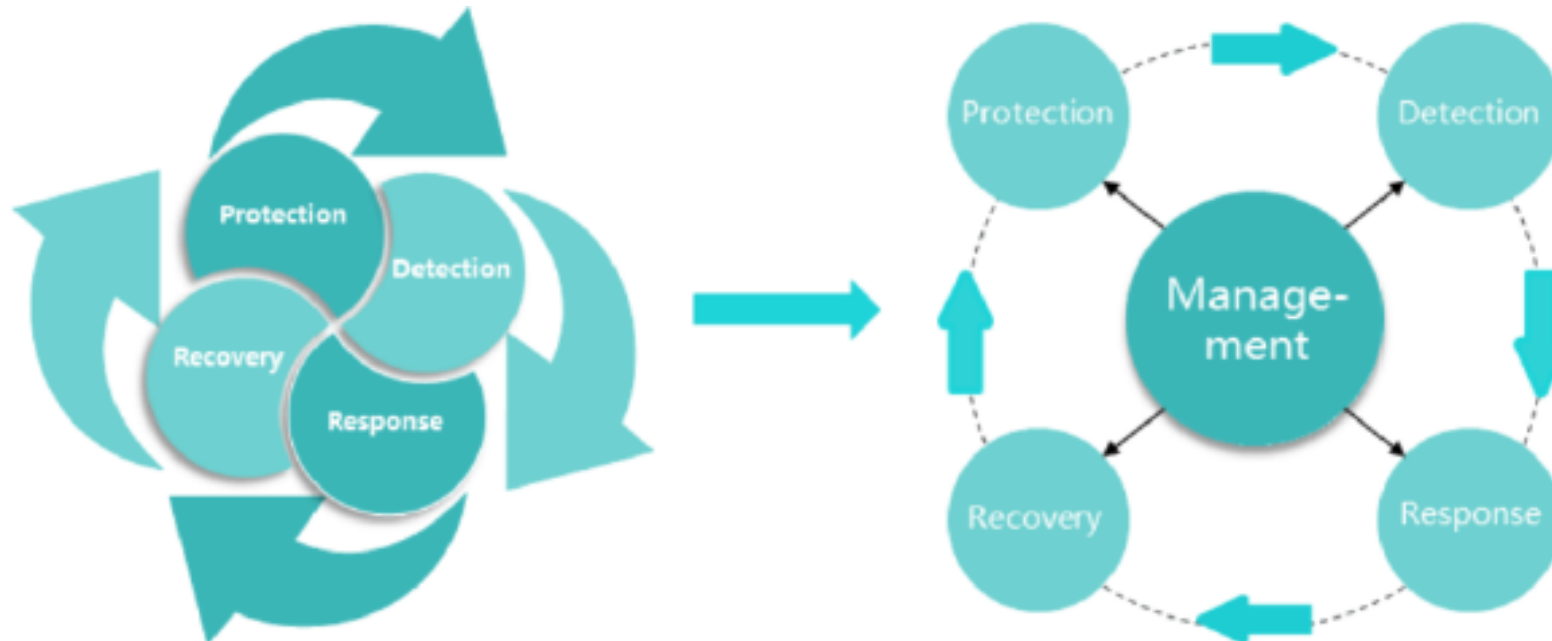
Concept of Incident Response/Emergency Response

- Incident response/emergency response refers to the preparations made by an organization to respond to emergencies and major information security incidents and the measures taken after the incident occurs.
- — GB/T 24363-2009 Information Security Emergency Response Plan Specifications
- The emergency response object of an information system security incident refers to the security incident of the information stored, transmitted, and processed by the information system. The incident subject may be caused by natural events, system faults, or manual attacks from internal or external personnel.
- —GA/T 708-2007 Architecture framework of security classification protection for information system



Cyber Security Emergency Response Model

- MPDRR is an acronym for management, protection, detection, reaction, and recovery. The MPDRR model is a common cyber security model with an in-depth defense system.
- The MPDRR model is developed based on the PDRR (protection, detection, recovery, response) model. It inherits the advantages of the PDRR model and adds security management to security technologies.



Regulations & Standards for Digital Forensics

- **Emergency response types:**

- ☐ **Remote emergency response (preferred):** Emergency response teams handle security incidents by Telephone, email, or fax after receiving incident reports from customers.
- ☐ **Local emergency response:** Emergency response teams shortly arrive at the sites where cyber security incidents occur, locate the causes, resolve the issues, and create detailed emergency response reports.

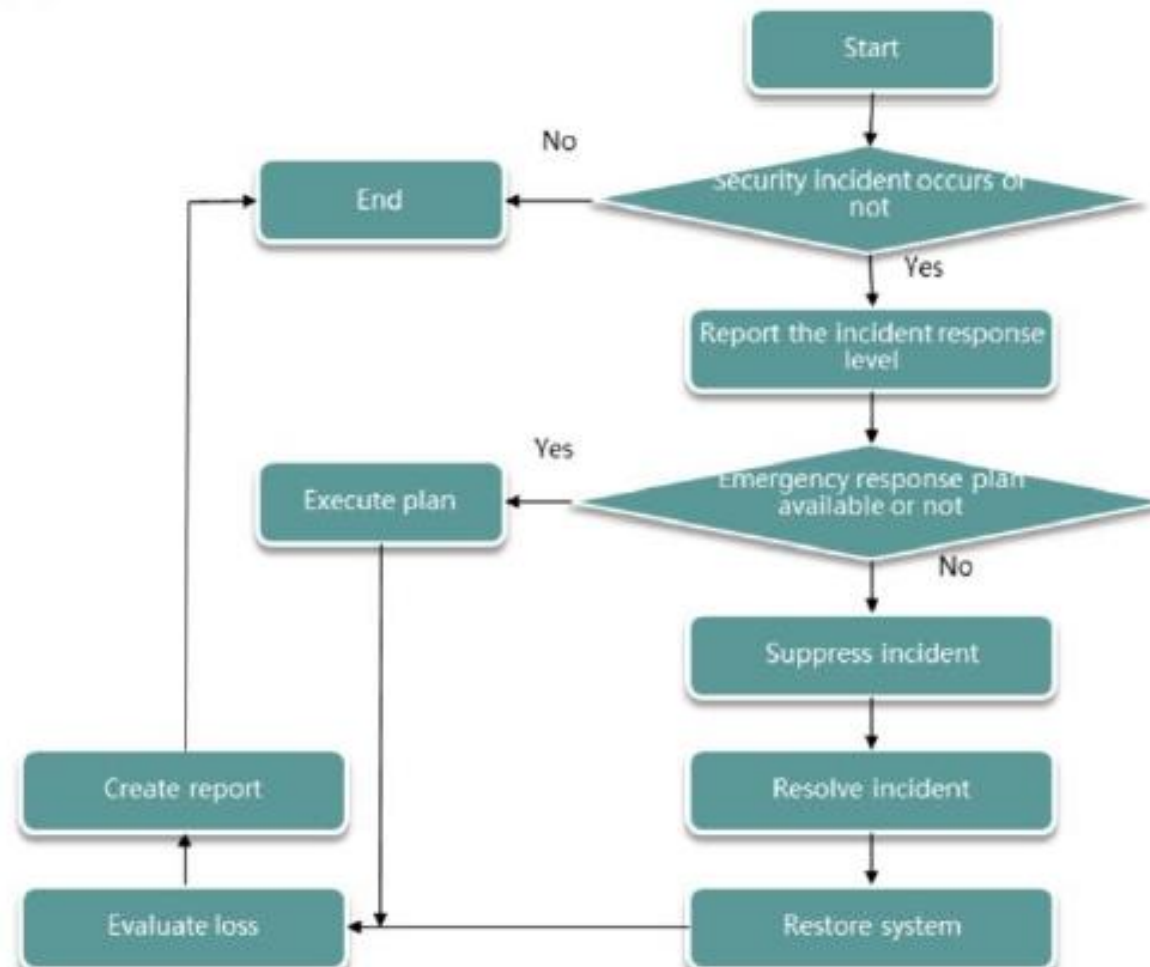


Remote emergency response



Local emergency response

Handling Process of Cyber Security Emergency Response



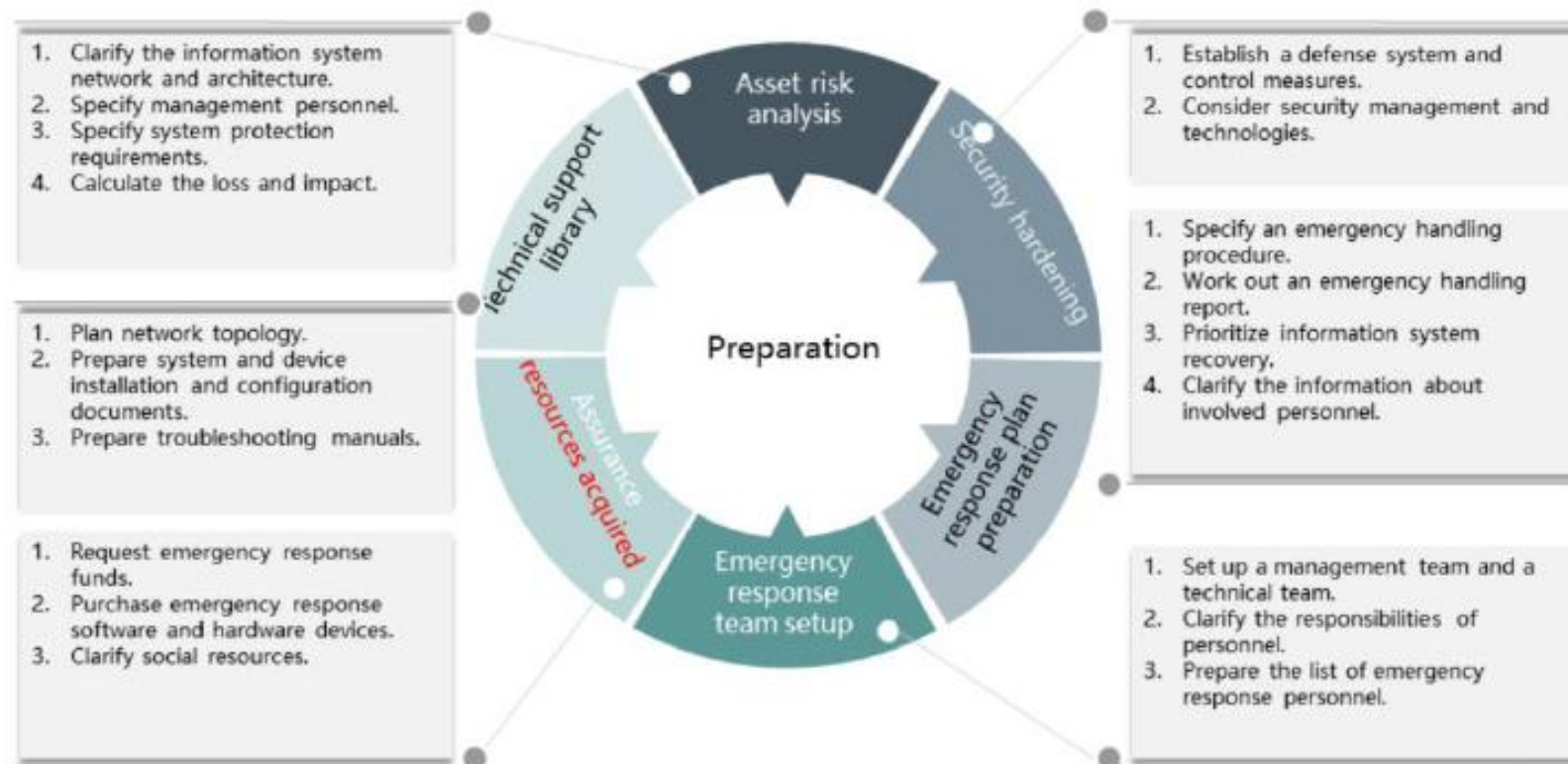
Cyber Security Emergency Response

- Cyber security emergency response plays an important role in tracing, handling, and preventing emerging cyber security incidents to ensure network information security. Currently, emergency response includes:



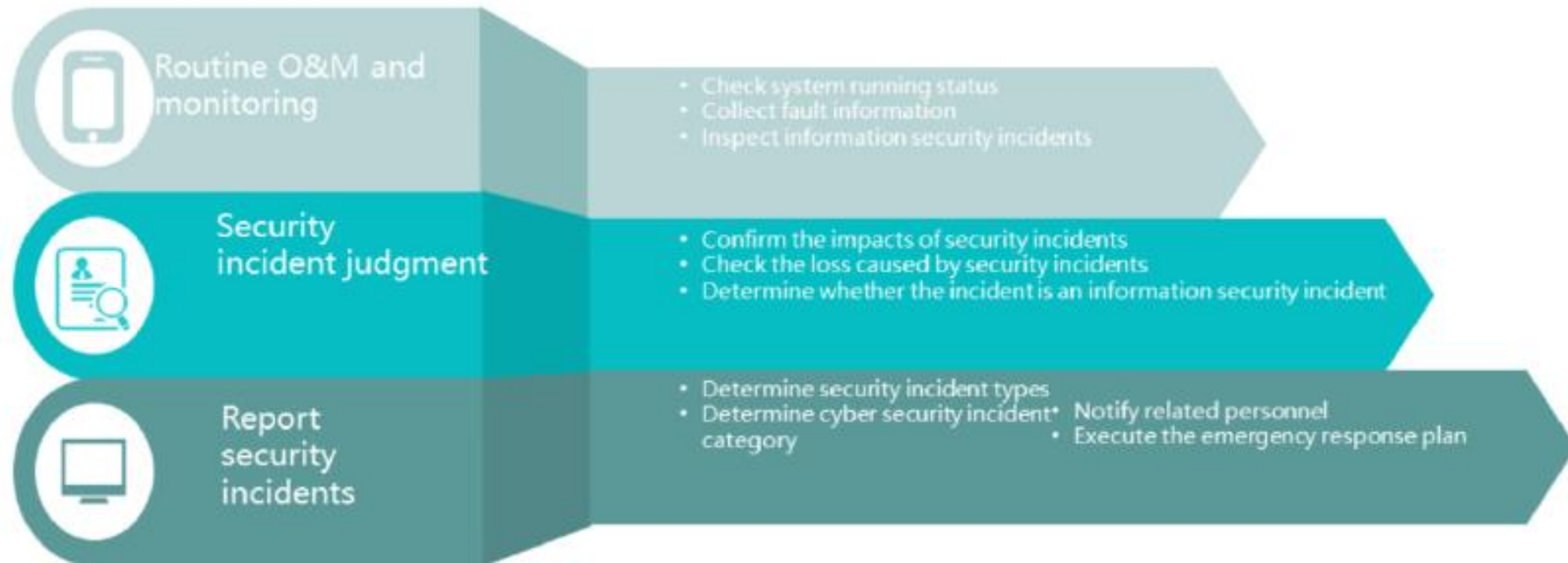
Preparation

Assess potential security incidents and formulate corresponding policies and assurance measures to suppress and resolve security incidents.



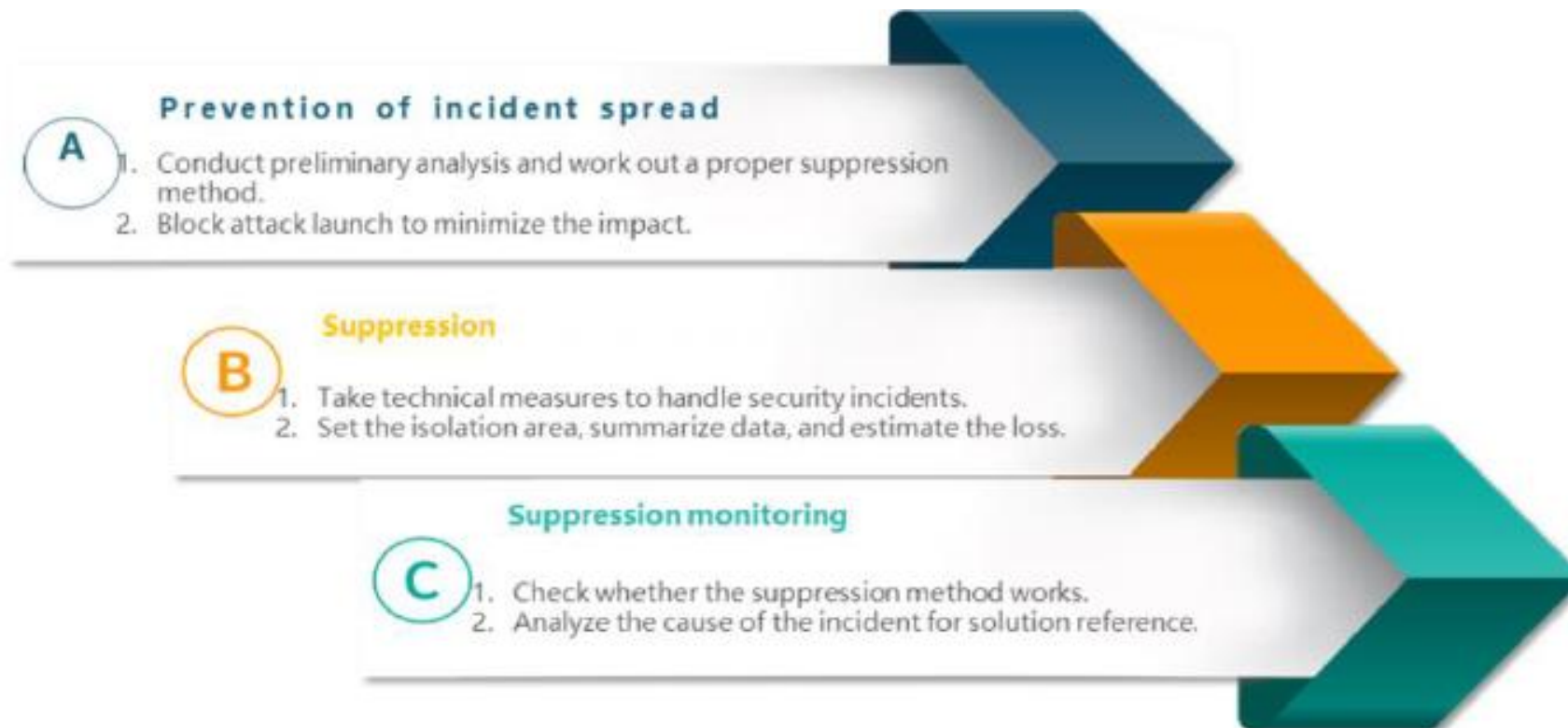
Detection

- Perform routine monitoring and collect system information. If a network security incident occurs, determine its impact and category, and report the incident



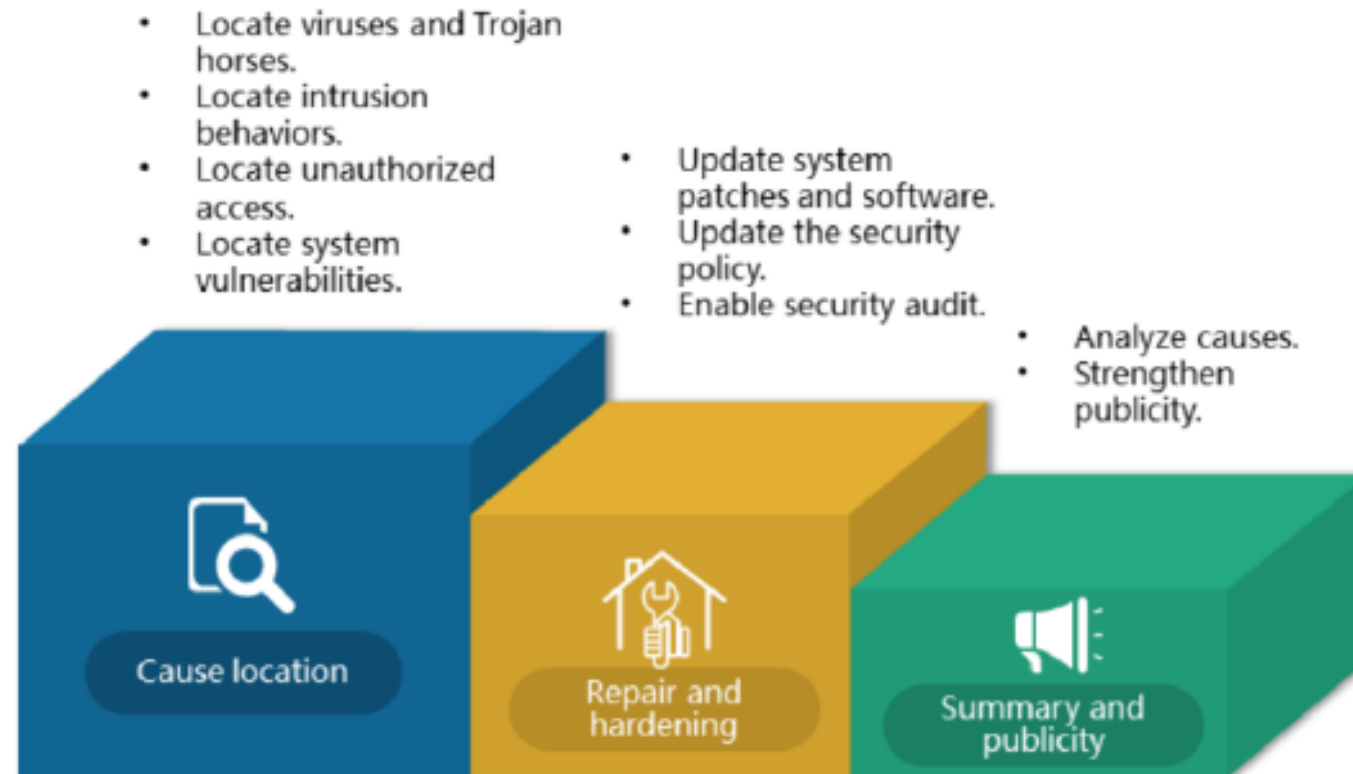
Suppression

- Restrict the scope of attacks and limit potential loss and damage. If an emergency incident is detected, start the emergency response process to minimize the impact of the incident.



Incident Resolving

- After the security incident is suppressed, locate the root cause to resolve the incident.



Recovery

- Restore all the compromised systems, applications, databases, and network devices to normal status.
- ☐ Restore network device configurations.
- ☐ Restore data or systems.
- ☐ Back up all changes.
- ☐ Check running status of the devices that recover.
- ☐ Check whether the isolation measures work. Remove isolation measures or short-term suppression defense measures if site situation improves.



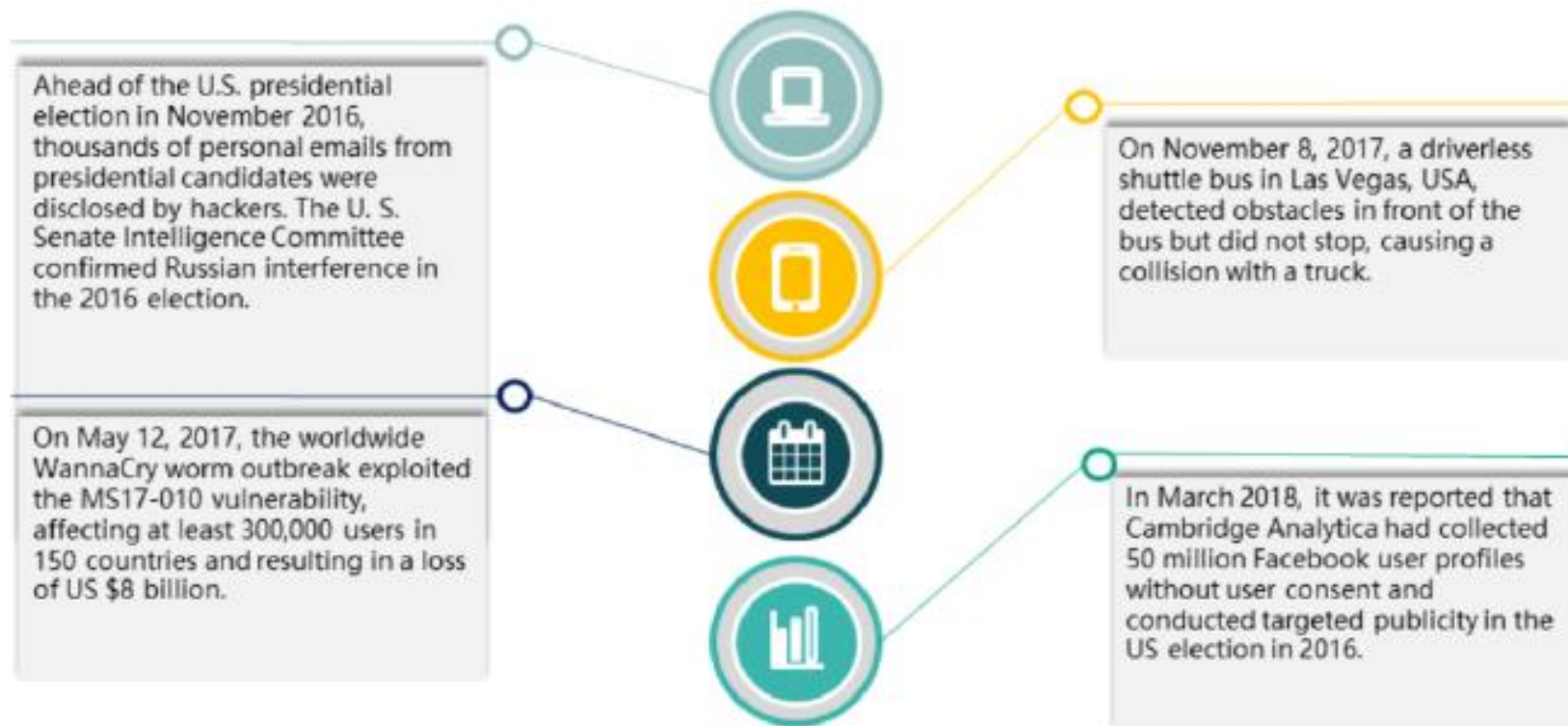
Conclusion

- Learn lessons from security incident responses, and summarize information about security incidents.



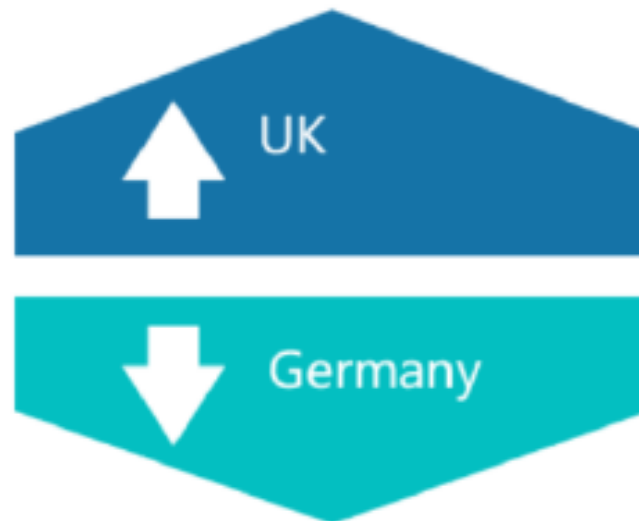
Global Major Security Incidents

- The IoT, mobile Internet, cloud computing, and big data are booming. Emerging technologies are reshaping the world. However, cyber security incidents are still on the rise, increasing people's concerns about cyber safety.



Cyber Security Laws/Regulations

- In 2017, global pilot projects focusing on cyber security laws and regulations were initiated in critical infrastructure, personal data security, and cyber emergency response. As a result, some countries have introduced trial security assurance regulations on autonomous driving.



The core Internet and automobile security principles have enforced cyber security responsibilities on each stakeholder of the automobile supply chain, requiring cyber security throughout the entire automobile lifecycle. Moreover, the principles have set the cyber security bottom line: Ensure basic automobile security even if the automobile is attacked.

The ethics code for autonomous and Internet vehicles gives clear description of controversial automated driving ethics. For example, it prohibits programming to dilemmas. Vendors shall be liable for the damages caused by their automation systems/products.

New Trend in Cyber Security Emergency Response

- In 2017, global cyber attacks, such as WannaCry ransomware, occurred at a high rate. It is difficult to effectively monitor and provide alerts for unexpected global security incidents. Furthermore, nations tend to be reactive instead of proactive when it comes to security incidents. The United States and Belgium, among others, have departed from the existing emergency response mechanism.



Chapter
10

Huawei USG6725F Firewall

This device recently earned the **“Recommended”** rating in the **2025 public evaluation by Wuhan Huanghe Laboratory**, one of China’s important national security testing bodies.

This ranking means the firewall demonstrated:

- High threat detection accuracy
- High performance under stress
- Strong zero-day attack resistance
- Very low false positives

This makes it an excellent model for enterprises and SOC operations.



Positioning of USG6725F in Huawei's Security Portfolio

Huawei's firewall product line:

- **USG6300** → SME
- **USG6500** → Mid-Enterprise
- **USG6700 Series** → Data Center / Enterprise
- **USG6700E** → High-performance data center
- **USG6725F** sits **between 6700E and 6500**, giving:
 - Data-center level features
 - But affordable for large campus & enterprise edge

This model is often used at:

- Internet boundary (north-south traffic)
- Core campus firewall
- Cloud edge security
- Branch-to-HQ secure gateway

Hardware Architecture of USG6725F

The USG6725F is built on Huawei's latest **UniSecurity hardware architecture**:

3.1 Multi-core CPU + Security ASIC

- Multi-core general-purpose processor for control plane + management

- **Dedicated security acceleration chip (ASIC)** for:

- VPN encryption/decryption
- DPI (Deep Packet Inspection)
- Session management
- IPS pattern matching

This achieves high throughput with low latency.

Hardware Architecture of USG6725F

3.2 Hardware Bypass & Redundancy

- Hot-swappable power supplies
- Intelligent fan control
- Hardware-bypass ports to avoid outages if the device fails

3.3 Interface Flexibility

Depending on model variant:

- GE RJ45 / GE SFP
- 10GE ports
- Some models support 40GE/100GE via module

Software Architecture: Security Engines

The USG6725F runs **Huawei's unified security operating system**, and inside it are many security engines.

4.1 Application Awareness Engine

- Identifies 6000+ applications
- Even if they use non-standard ports
- Uses machine learning & payload analysis
- Enables policy like:
“Block TikTok but allow Teams”,
“Allow Facebook browsing but block Facebook video streaming”,
“Allow SSH but only to specific servers”

Software Architecture: Security Engines

4.2 Intrusion Prevention System (IPS)

- Signature-based detection
- Protocol anomaly detection
- Zero-day exploit detection
- Virtual patching:
 - Firewall blocks exploitation attempts before a system is patched

IPS has:

- **Decoding engine** → Understands protocols like HTTP/2, DNS, SMB, TLS
- **Attack detection engine** → signature and behavior
- **Correlation engine** → combines events to reduce false positives

Huawei USG6725F Firewall

4.3 Anti-Malware Engine

Uses:

- File hash reputation
- Sandboxing integration (sending suspicious files to cloud sandbox)
- Static file scanning
- Heuristic behavior detection

Stops:

- Ransomware
- Worm propagation
- Backdoors
- Spyware command/control communications

Huawei USG6725F Firewall

4.4 VPN Engine

Supports:

- IPsec VPN
 - SSL VPN
 - GRE
 - L2TP
 - DVPN (dynamic mesh VPN for large enterprises)
- VPN acceleration runs on ASIC → very high throughput.

Conclusion

Huawei USG6725F is a high-performance NGFW with:

- Deep packet inspection
- AI-driven threat detection
- Advanced IPS and malware defense
- Zero-trust support
- High VPN performance
- SOC-ready visibility



Thank You