中華電信研究院
Chunghwa Telecom Laboratories

An Integrated Security Monitoring System for Digital Service Network Devices

Wen-Lin Cheng, Ting-Che Chuang, Chien-Wen Yang,
Yueh-Hsien Lin, Min Liu, Chuan Yin
Network Management Laboratory, Chunghwa Telecom Laboratories

2017,Sep.

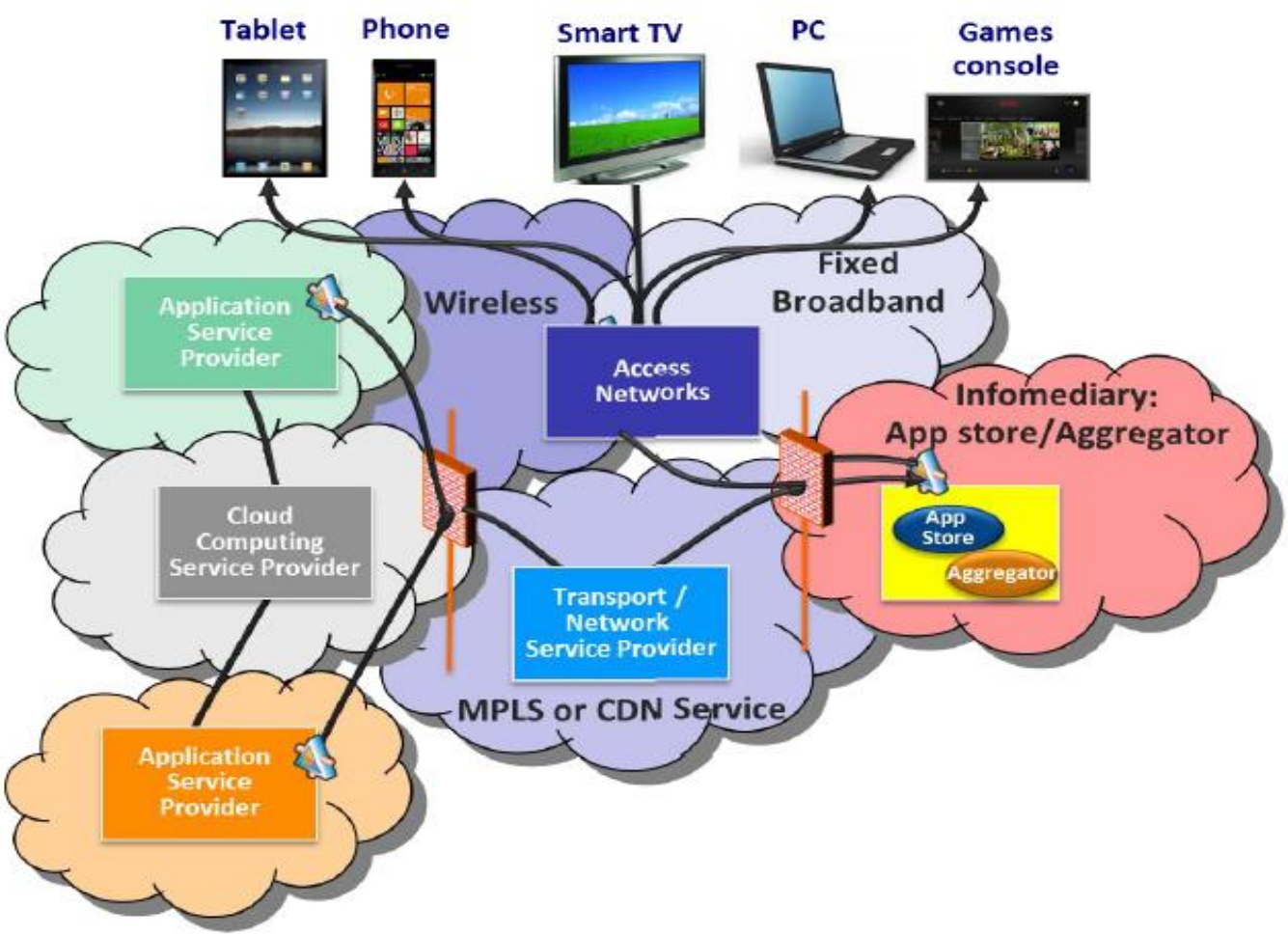
Outline

- Introduction
- Related Work
- Methodology
- System Implementation
- Conclusion

Introduction-Digital Services(1/2)

- New ICT (Information and Communication Technology) services are booming quickly.
- In digital service ecosystem, almost all services are composed by multiple micro-services.
- Building composite digital services is more complicated for service providers.

Introduction-Digital Services(2/2)



The Multi-Service Nature of Service Delievery

Introduction-Digital Service Security

- **How to ensure digital service security?**
  - System security
  - Network security

Network Device Security

- **What do we take care?**
  - Service providers focus on anti-virus, anti-hacking, service performance.
  - Telecom operators focus on stable and robust network.
- **How about Network Device Security?**

Integrated Security Monitoring System

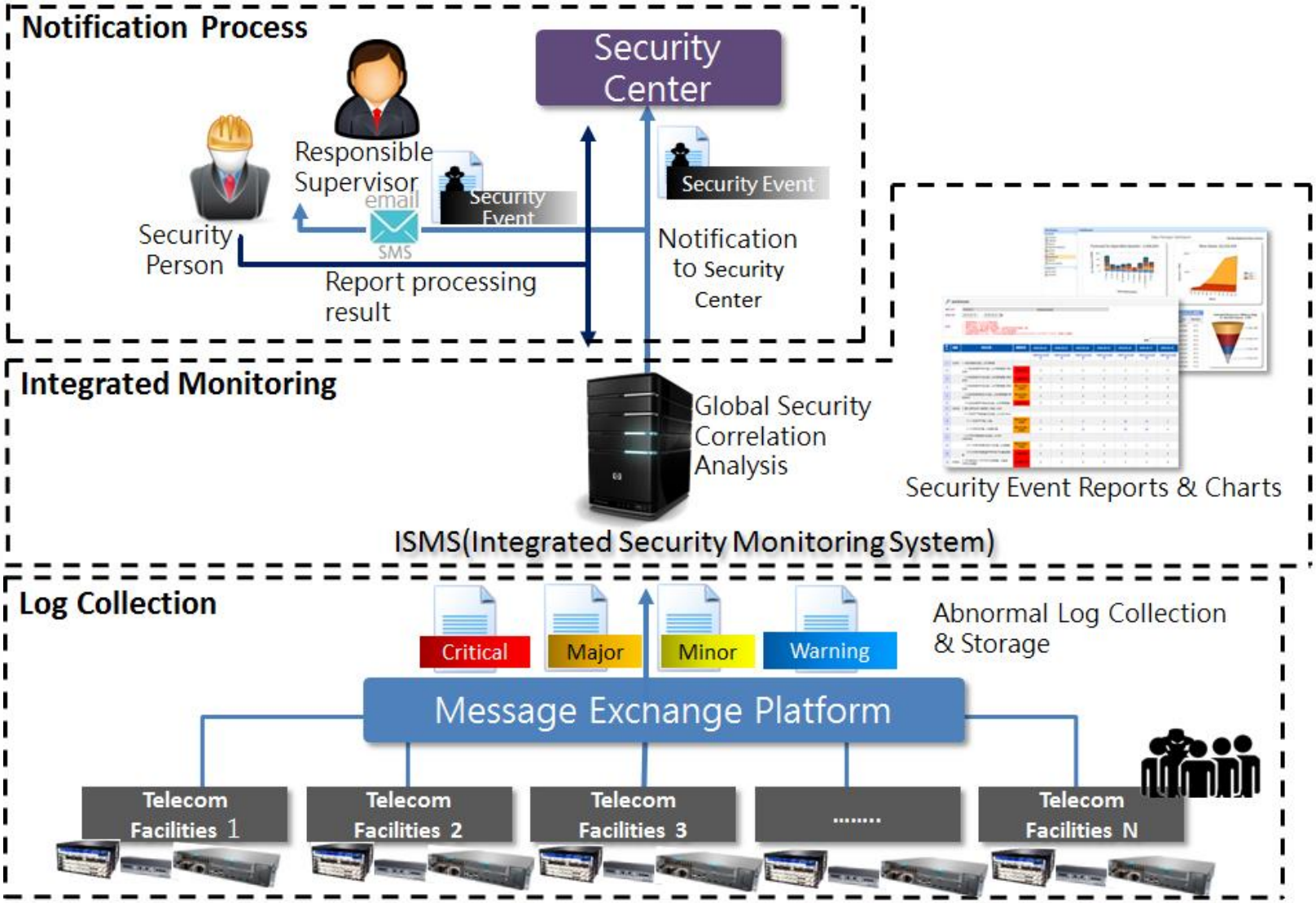
- **The system aggregates all security data under heterogeneous network architecture.**
- **The system present analyzed information in a single panel.**
- **The system consists of three building blocks**
  - Device log collection architecture
  - Global security alarm correlation analysis
  - Security event notification

Related work

- **Network Operation Management**
  - Expert system
  - Intelligent Network Fault Diagnosis
  - QoS
- **Network Security Management**
  - Packet analysis
  - Traffic analysis

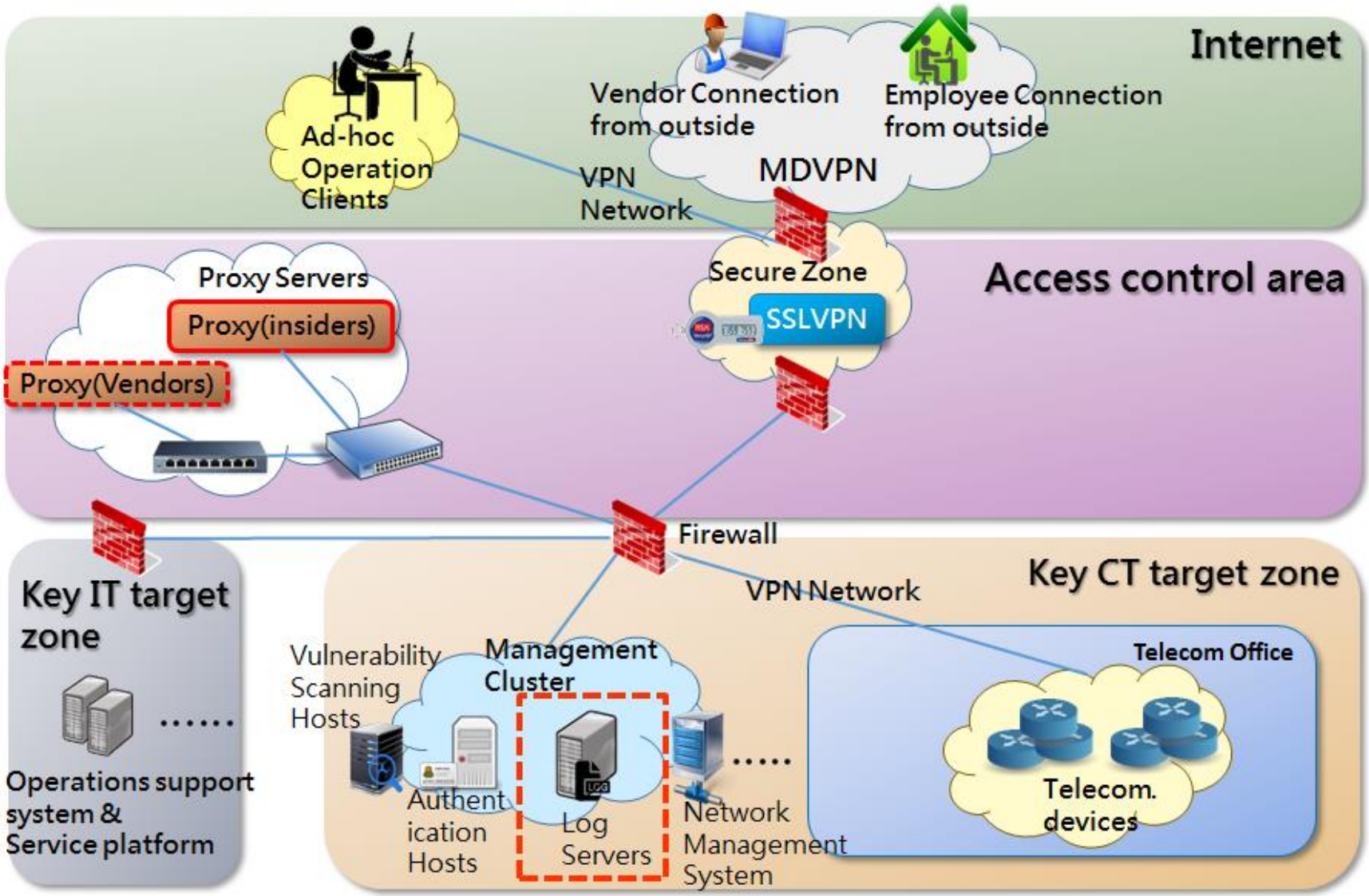
Methodology(1/3)

Integrated device security monitoring process



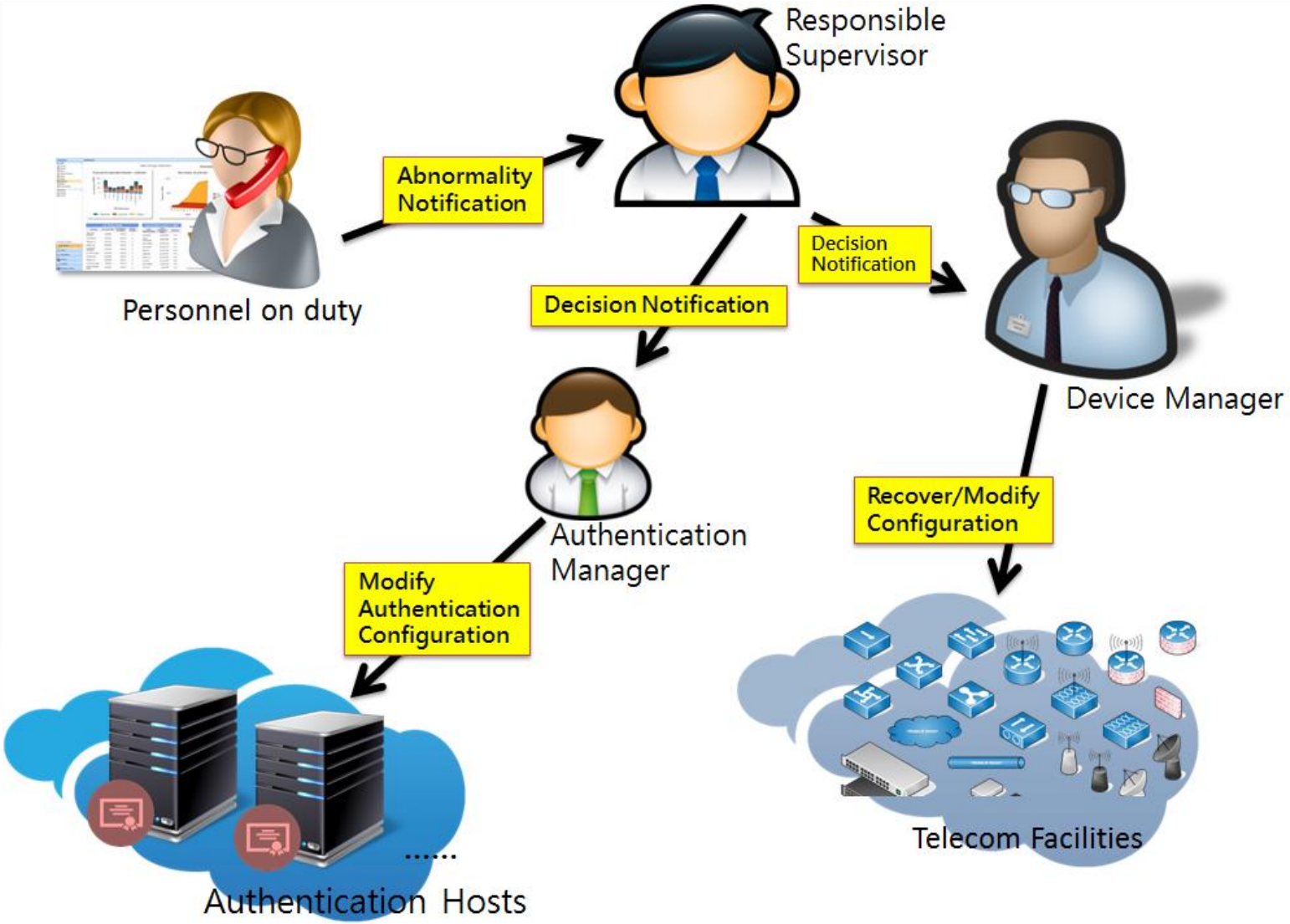
Methodology(2/3)

Network device log collection architecture



Methodology(3/3)

Security event notification process



System Implementation(1/3)

Log Server Modules

Different Log format between different devices

Log Raw Data

<27>Apr 22 15:18:10 TON Security-Auditing: 4625: AUDIT_FAILURE 帳戶無法登入。 主旨: 安全性識別碼: S-1-5-18 帳戶名稱: TON$ 帳戶網域: WORKGROUP 登入識別碼: 0x3e7 登入類型: 2 登入失敗的帳戶: 安全性識別碼: S-1-0-0 帳戶名稱: user 帳戶網域: TON 失敗資訊: 失敗原因: 不明的使用者名稱或錯誤密碼。 狀態: 0xc000006d 子狀態: 0xc000006a 處理程序資訊: 呼叫者處理程序識別碼: 0x3e24 呼叫者處理程序名稱: C:\Windows\System32\winlogon.exe 網路資訊: 工作站名稱: TON 來源網路位址: 127.0.0.1 來源連接埠.....

Filtering

```
filter {
  grok {
    match => { "message" =>
"<%{POSINT:syslog_pri}>%{SYSLOGTI
MESTAMP:syslog_timestamp}
%{SYSLOGHOST:syslog_hostname}
%{DATA:syslog_program}:
%{NUMBER:syslog_pid}:
%{GREEDYDATA:syslog_message}" }
    add_field => [ "received_at",
"%{@timestamp}" ]
    add_field => [ "received_from",
"%{host}" ]
  }.....
```

Normalized Data

received_at	2016-04-22T07:18:11.756Z
received_from	127.0.0.1
syslog_facility	daemon
syslog_facility_code	3
syslog_hostname	TON
syslog_message	AUDIT_FAILURE 帳戶無法登入。 主旨: 安全性識別資訊: 失敗原因: 不明的使用者名稱或錯誤密碼。 狀態: TON 來源網路位址: 127.0.0.1 來源連接埠: 0 詳細試存取的電腦上產生。 主旨欄位顯示要求登入的類型是 2 (互動式) 與 3 (網路)。 處理程序資訊欄位次特定登入要求的詳細資訊。 轉送的服務欄位顯示工作階段金鑰剩為 0。

Search

q=syslog_message:*AUDIT_FAILURE* OR *:*&wt=json&fq=@timestamp:[NOW/MINUTE-15MINUTE%20TO%20NOW/MINUTE%2B1MINUTE]&..... (15分內登入失敗次數)

Analysis

Analysis result

Alarm

Analysis result To Alarm

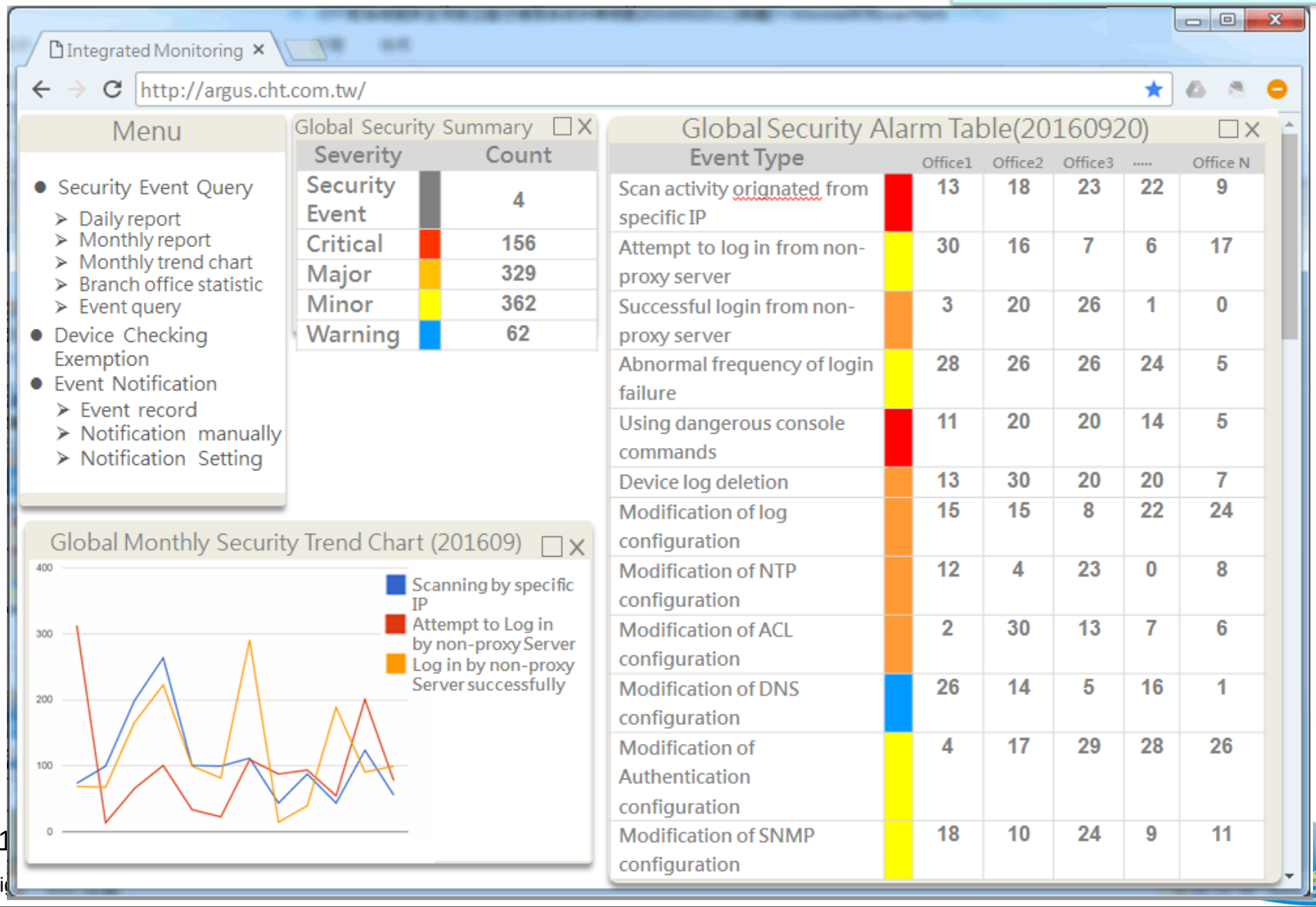
System Implementation(2/3)

Important Monitor items

Classification	Potential Attack Type	Monitor item	Severity	Detection technic
Device Access & Log in	Port Scanning	1.Scan activity orignated from specific IP	Critical	Analysis of firewall & device connection log
	Unauthorized Login Attempt	2.Attempt to log in from non-proxy server	Minor	Analysis of firewall, authentication server, and device connection log
	Unauthorized Login Activity	3.Successful login from non-proxy server	Major	Analysis of firewall, authentication server, and device connection log
	Bruteforce Login Attempt or Activity	4.Abnormal frequency of login failure	Minor	Analysis of firewall, authentication server, and device connection log
Console Command Operation	To track user data or paralyze device service with console commands	5.Using dangerous console commands	Critical	Analysis of authentication server & device connection log
	To destroy logging & tracking ability	6.Device log deletion	Major	Analysis of authentication server & device connection log
Configuration Modification	To destroy logging & tracking ability	7.Modification of logging configuration	Major	Analysis of device setting modification or authentication server log
	To confuse invading logging by time modification	8.Modification of NTP configuration	Major	Analysis of device setting modification or authentication server log
	Device intrusion by modifying access rules	9.Modification of ACL configuration	Major	Analysis of device setting modification or authentication server log
	To paralyze service by DNS modification	10.Modification of DNS configuration	Warning	Analysis of device setting modification or authentication server log
	Device intrusion by modifying Authentication setting	11.Modification of Authentication configuration	Minor	Analysis of device setting modification or authentication server log
	Device intrusion by modifying SNMP Setting	12.Modification of SNMP configuration	Minor	Analysis of device setting modification or authentication server log

System Implementation(3/3)

Integrated Monitoring panel



Conclusion

- **Building an Integrated Security Monitoring System for Digital Service Network Devices**
- **To help telecom operators to establish centralized device security mechanism for network devices.**

中華電信研究院
Chunghwa Telecom Laboratories

Thank You