



# 學校網絡安全漏洞的評估分享， 管理挑戰及趨勢

---





# Cyber Security and the Trend for Security Management in School Sector

## Agenda

1. Introduction
2. Assessment Result Sharing and Insight
3. Challenges in Security Management
4. Trends in Security Management
5. Q &A

## Introduction

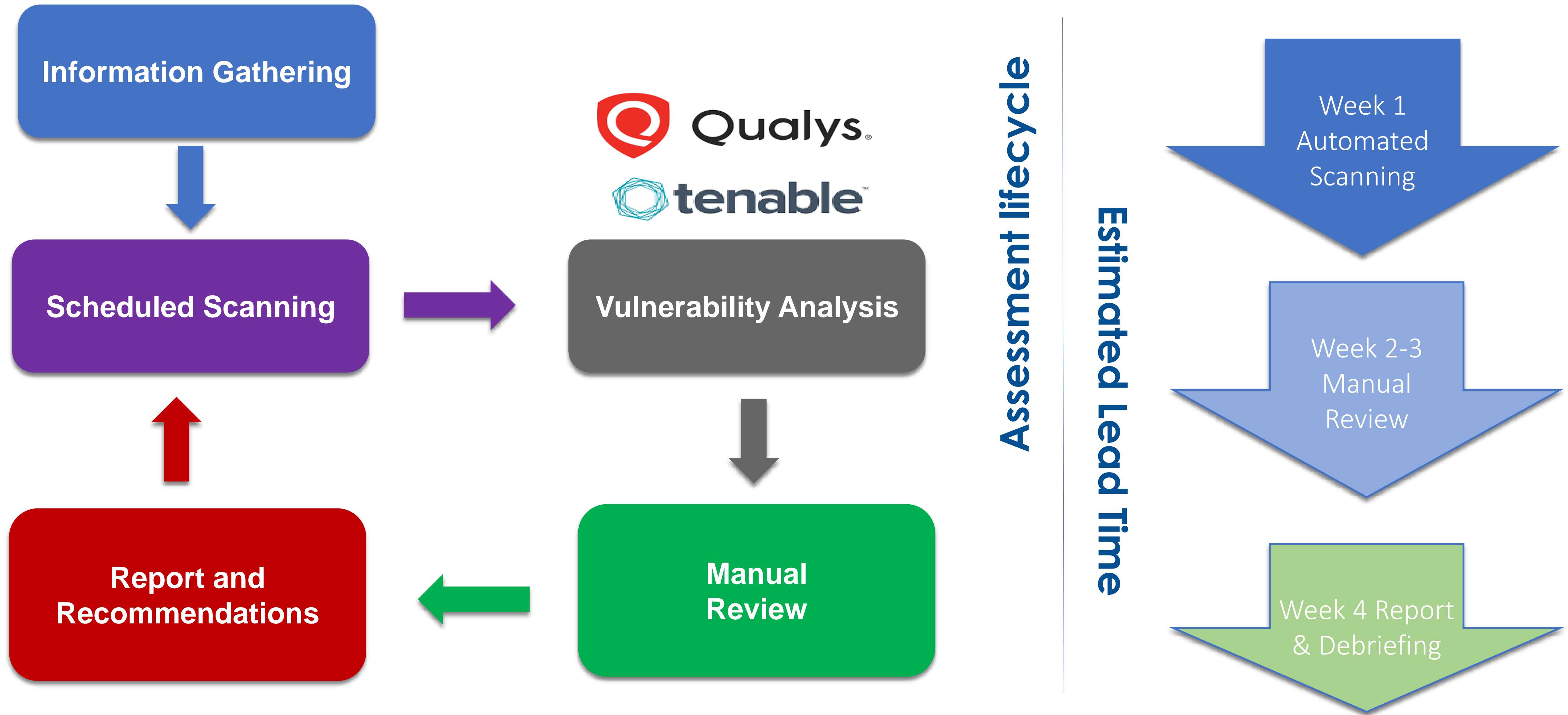
# School IT Security Risk Assessment

## Objectives

- ▶ Create awareness - Privacy issues
- ▶ Identify vulnerabilities in local primary & secondary schools
- ▶ Set the standard (baseline) for the industry
- ▶ Vendor to provide service - Qualified security experts should be appointed for security risk assessment



# HKT Web Vulnerability Assessment Service

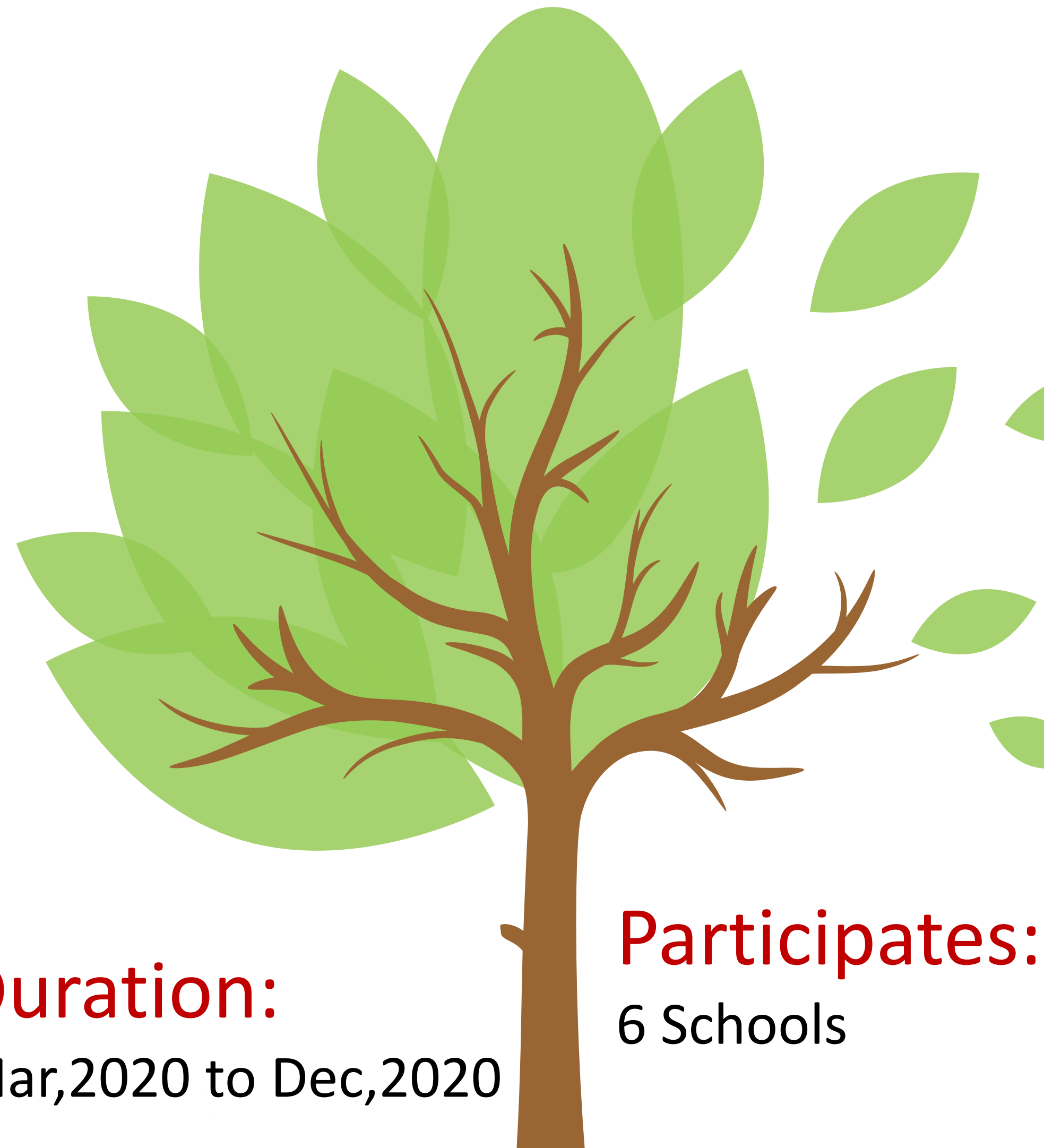


# HKT Web Vulnerability Assessment Service



Vulnerability Assessment Service is performed by a group of security certified engineers

# HKT's Web Vulnerability Assessment Summary



**Duration:**  
Mar,2020 to Dec,2020

**Participates:**  
6 Schools

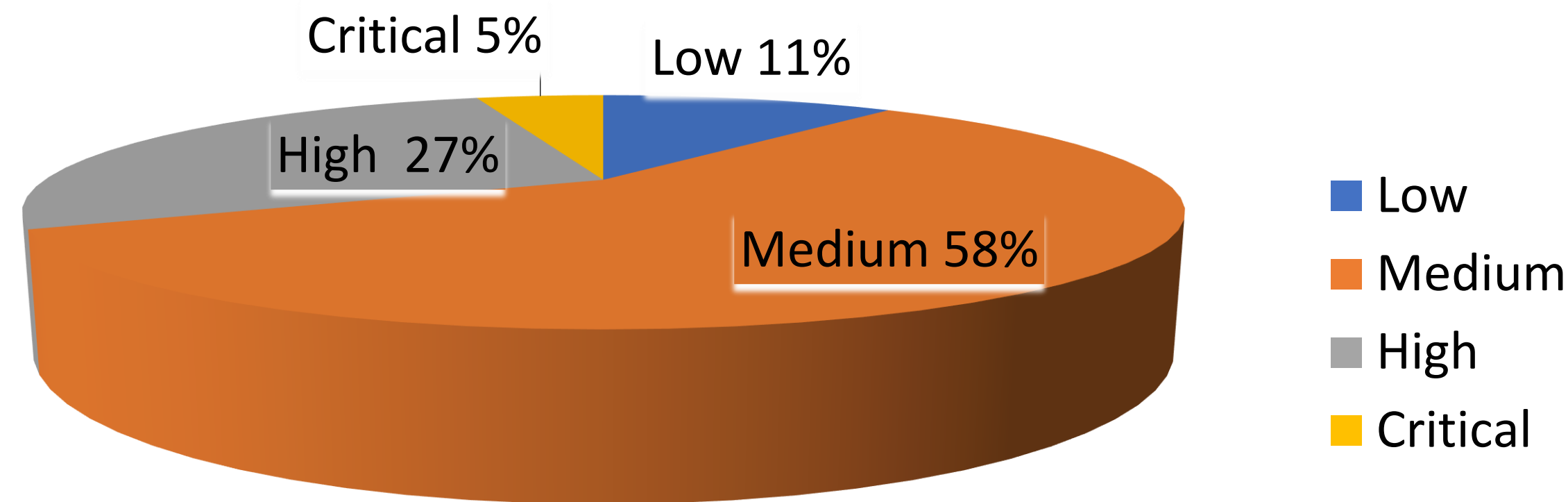
**25%** Web Services Scanning  
Host Discovery: 59 ; Web Services: 15  
(Around 25% has Web Page Services)

**66%** Average Risk Score is 54  
4 schools Risk Score over average value  
(around 66% School's Risk Score is above average)

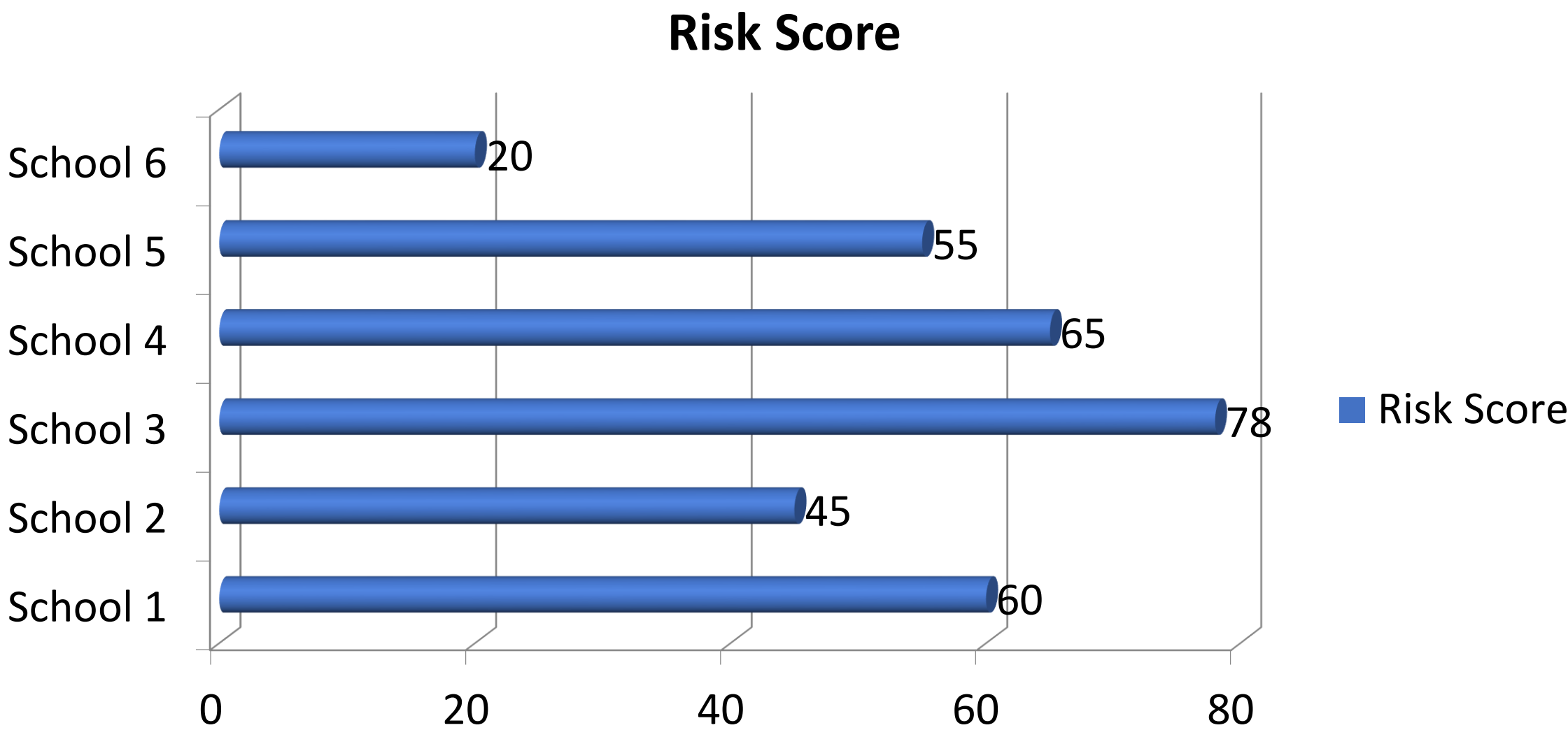
**32%** Application Vulnerability Scanning result  
Domain Vulnerability Result: 31% risk is in High Risk or above.  
Application Vulnerability Result: 33% risk is in High Risk Level. There are 283 high risk find in total 849 vulnerability records.



Domain Host Vulnerability Scanning Distribution



33% of Vulnerabilities are in Critical / High Categories



| Average Score | Highest Score | Lowest Score |
|---------------|---------------|--------------|
| 54            | 78            | 20           |

Among the ~15 systems scanned, we find Percentage get the below Vulnerability.....

26%

## Code (SQL) Injection

Allow an attacker to compromise the application, access or modify data, or exploit latent vulnerabilities in the underlying database.

6.9% of total attacks belongs to this category.

40%

## Cross-site Scripting (XSS)

The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.

32% of total attacks belongs to this category.

86%

## Using Outdated Components with Known Vulnerabilities

- SSL/TLS version
- OS version
- PHP version
- Apache version
- ...etc

4.7% of total attacks belongs to this category.



Code (SQL) Injection

Cross-site Scripting (XSS)

Using Outdated Components  
with Known Vulnerabilities



The vulnerability may impact your system, result in

- Data Leakage / Loss
- Content Defacement
- Malicious code injection
- Malware / Ransomware Infection



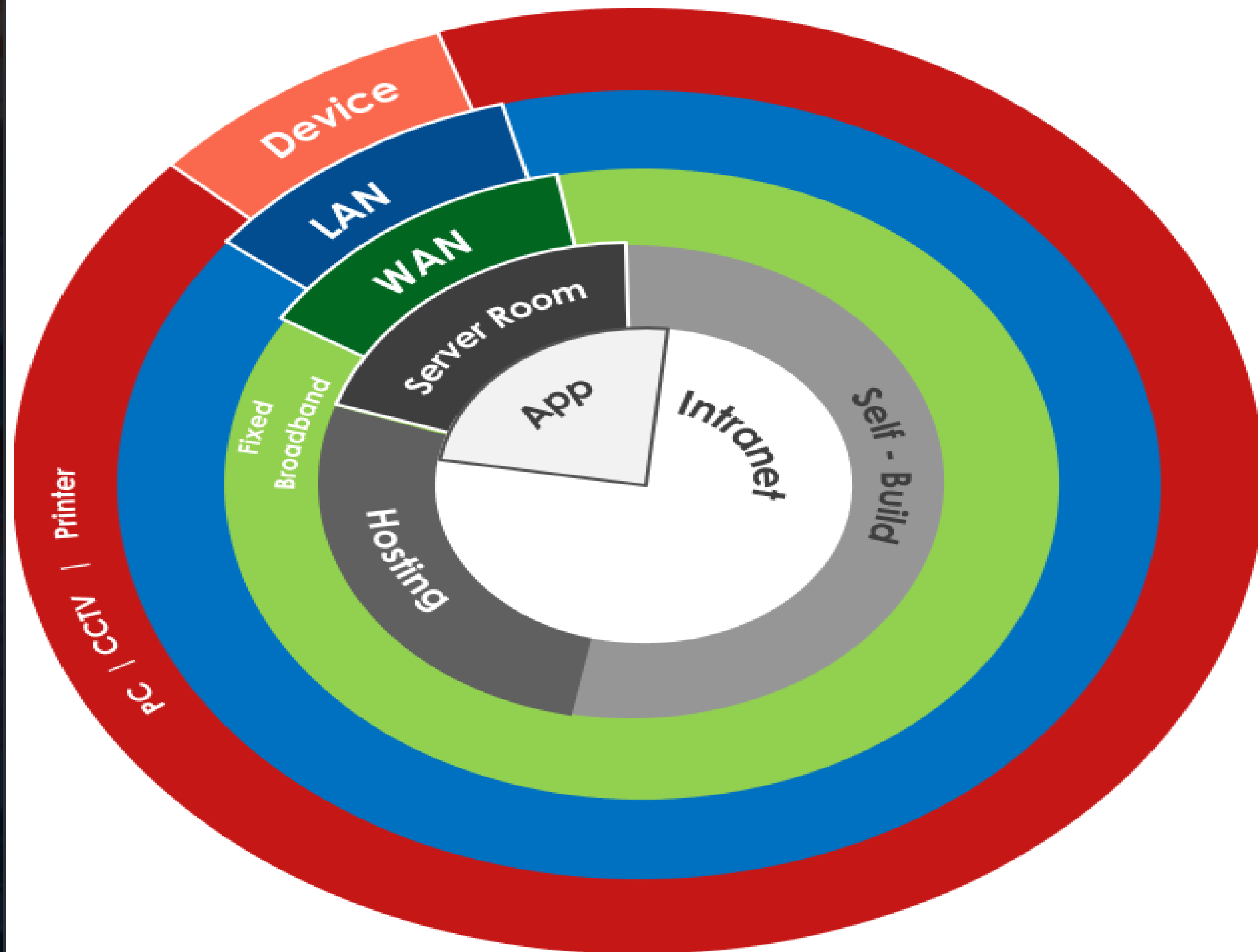
- Black Listing ↔ Affect SCHOOL OPERATON / REPUTATION

# Challenges in Security Management



IT Support

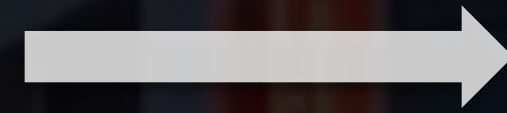
10+ years ago



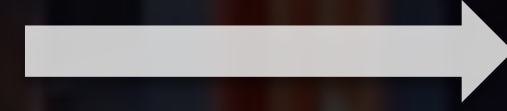


# Challenges in Security Management

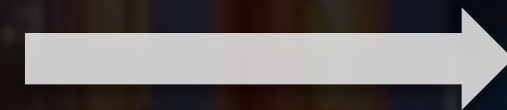
More User Touch Point



More System



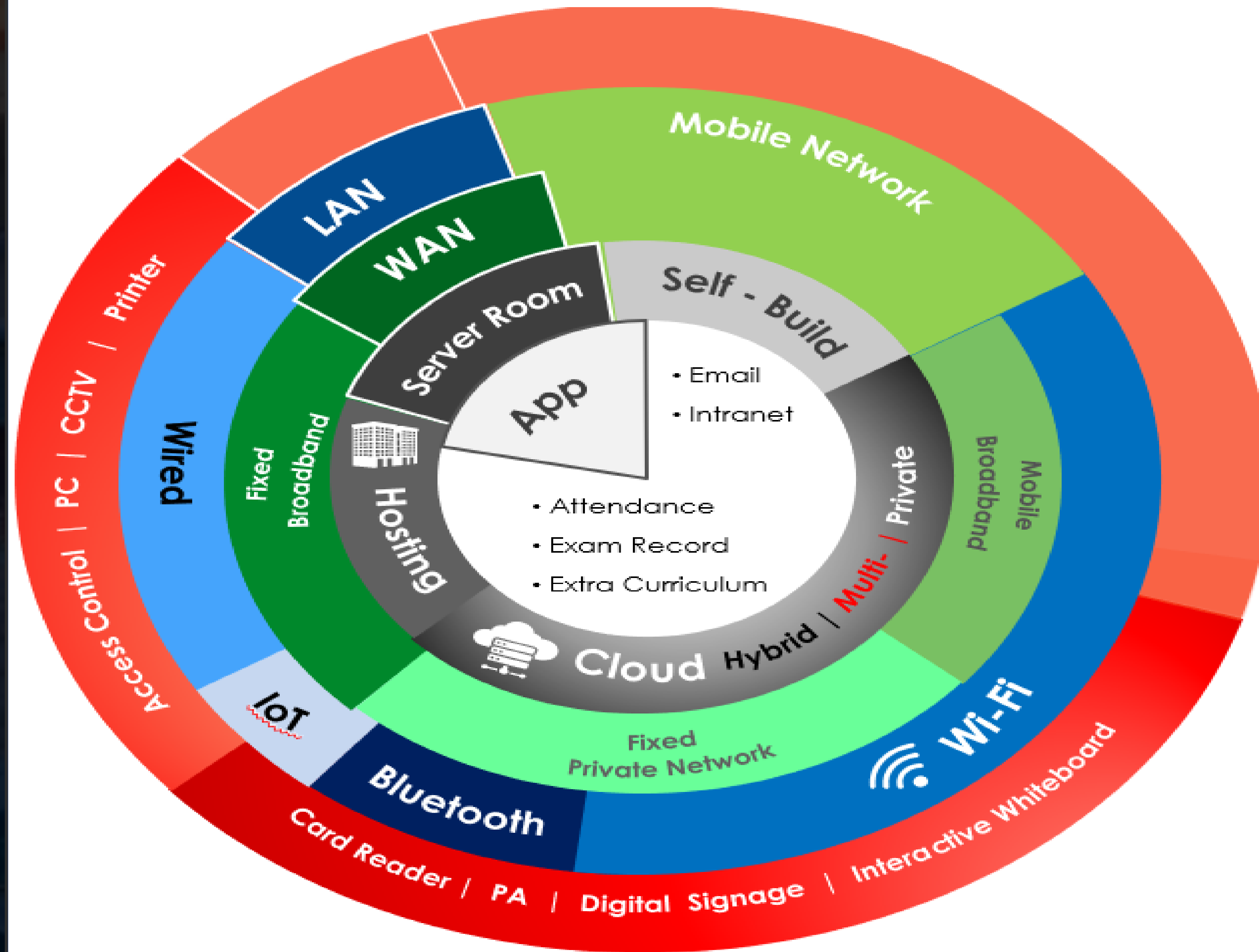
More Data  
(More Security Risk)



IT Support

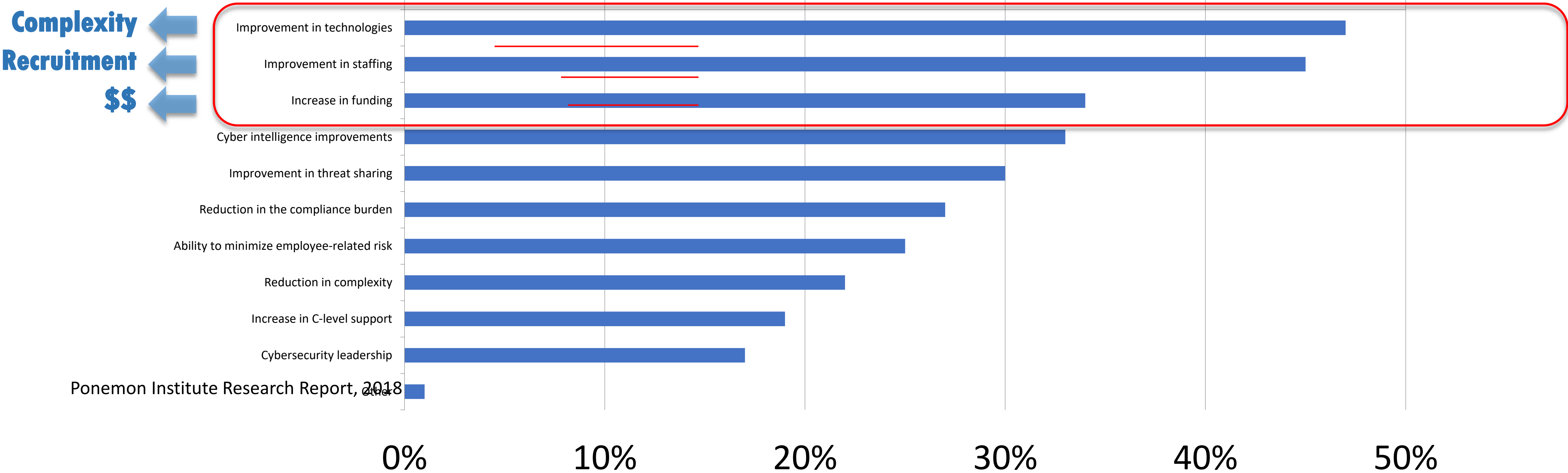
# N

owadays



# Investment spending in Cyber Security

Success factors that can strengthen your organization’s cybersecurity posture in the next three years







# Trends in Security Management

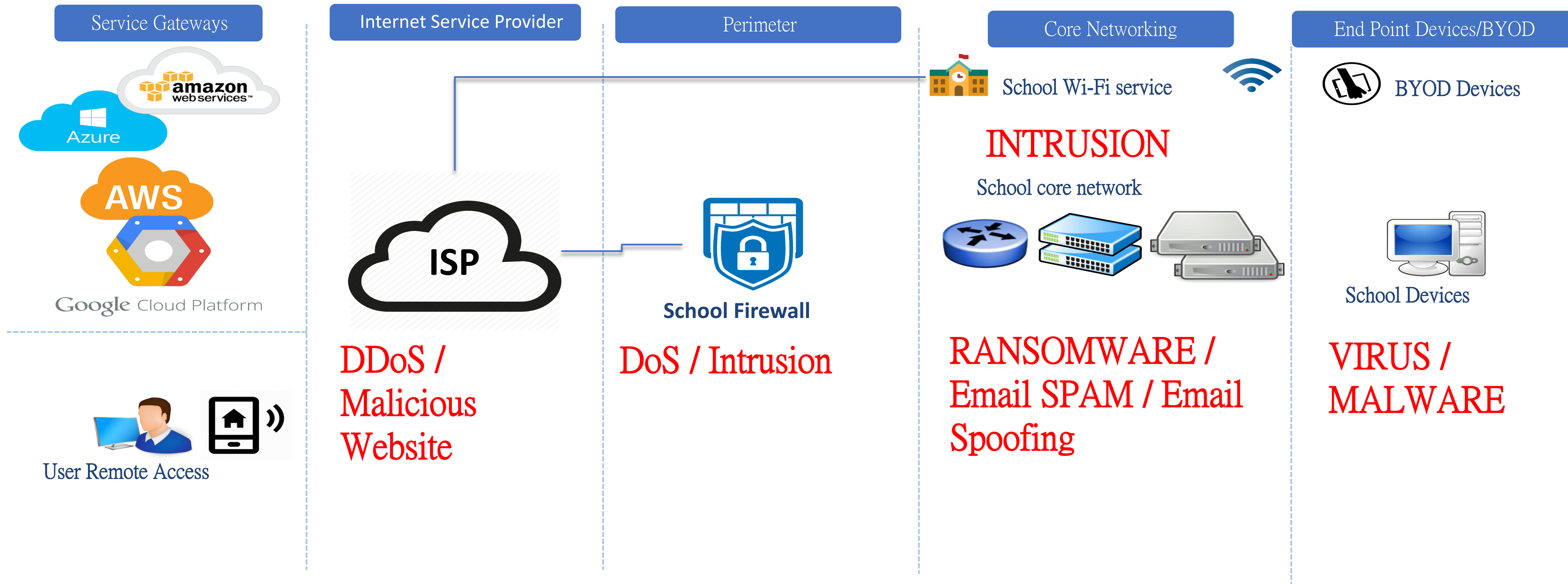
# How to Survive in the challenging Security Management?

**You CANNOT do it all by yourself, find  
a TRUSTED PARTNER for Security  
Management**



# "Security-Centric" - Security Management Everywhere

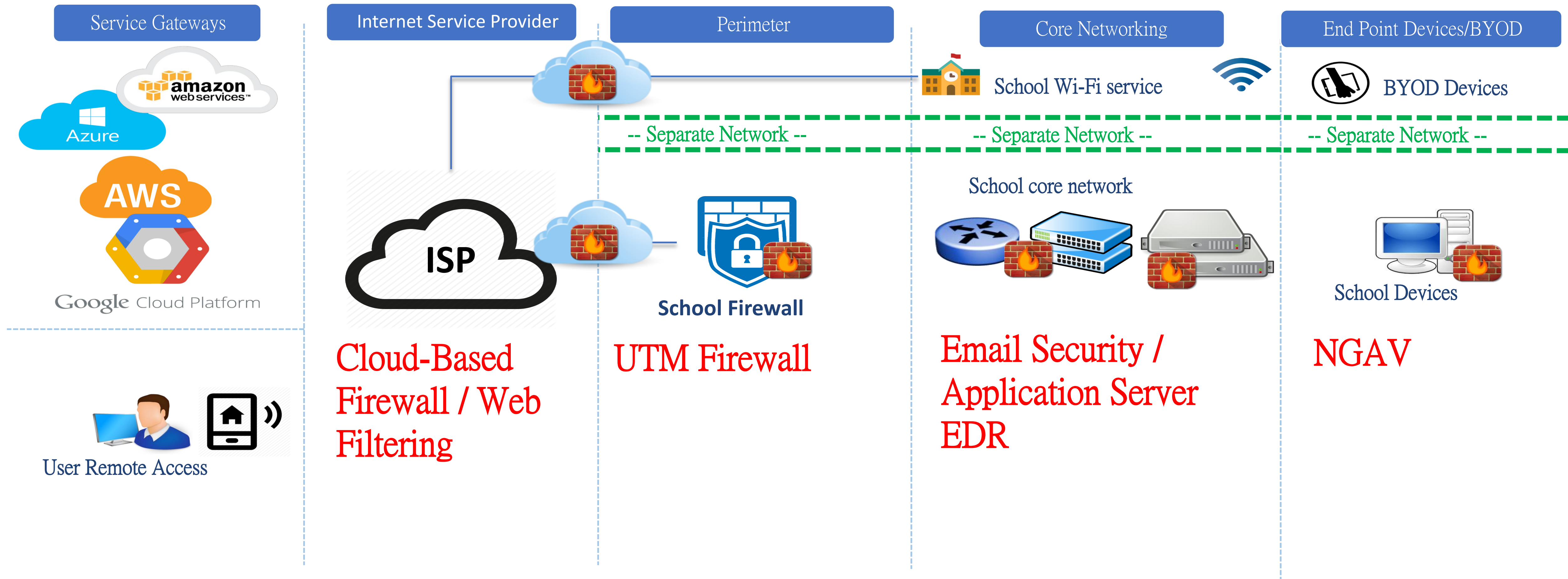
Potential Security Threat is everywhere!!



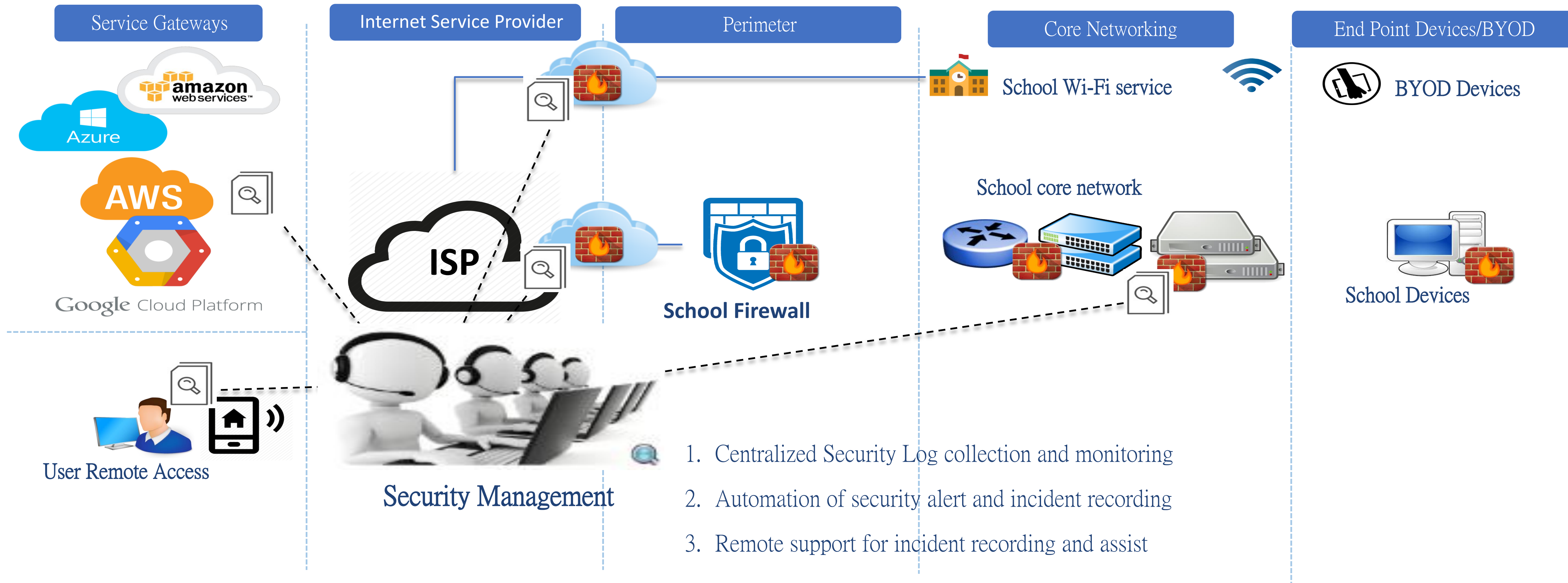


# "Security-Centric" - Security Management Everywhere

## Multi-Dimension Security Protection



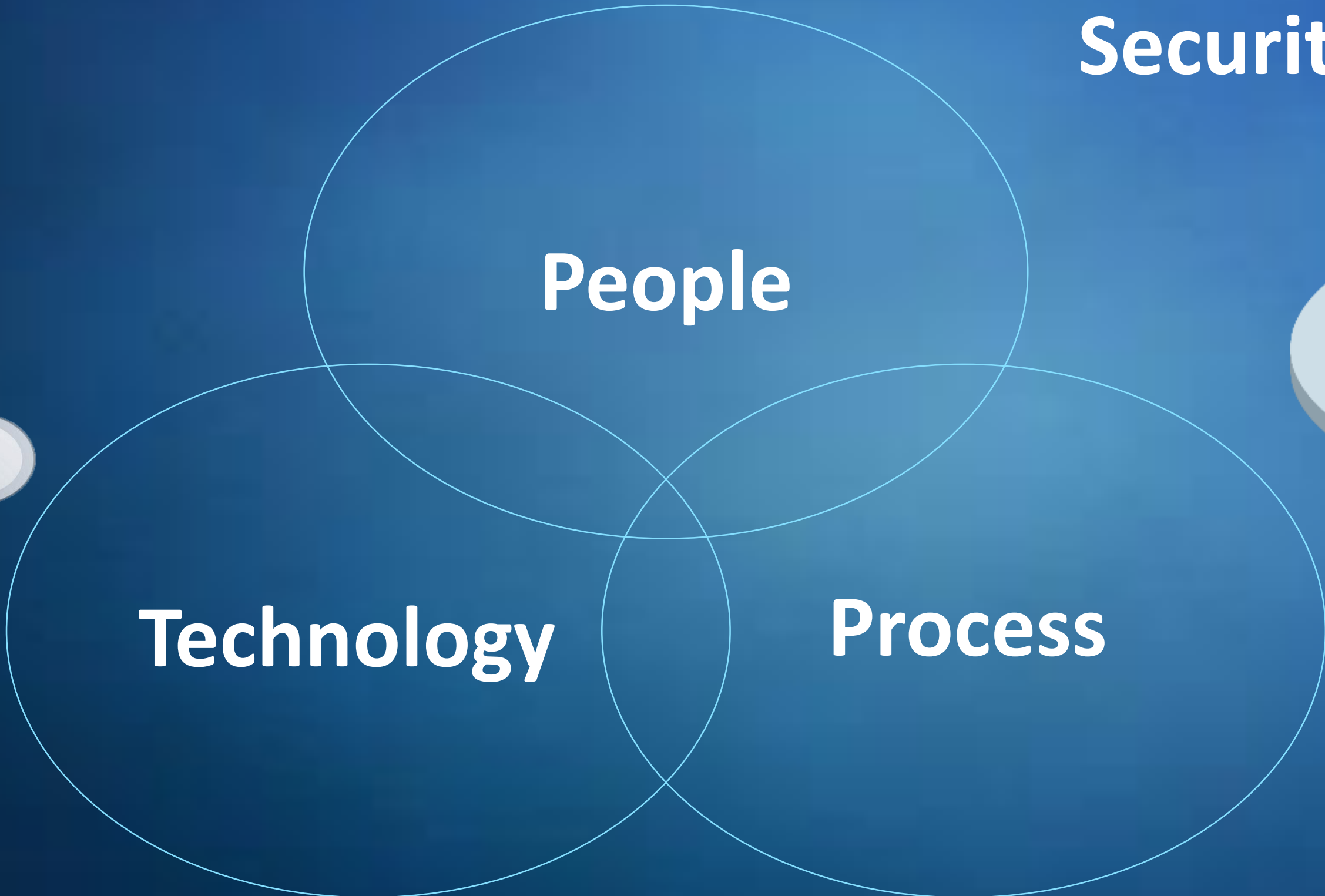
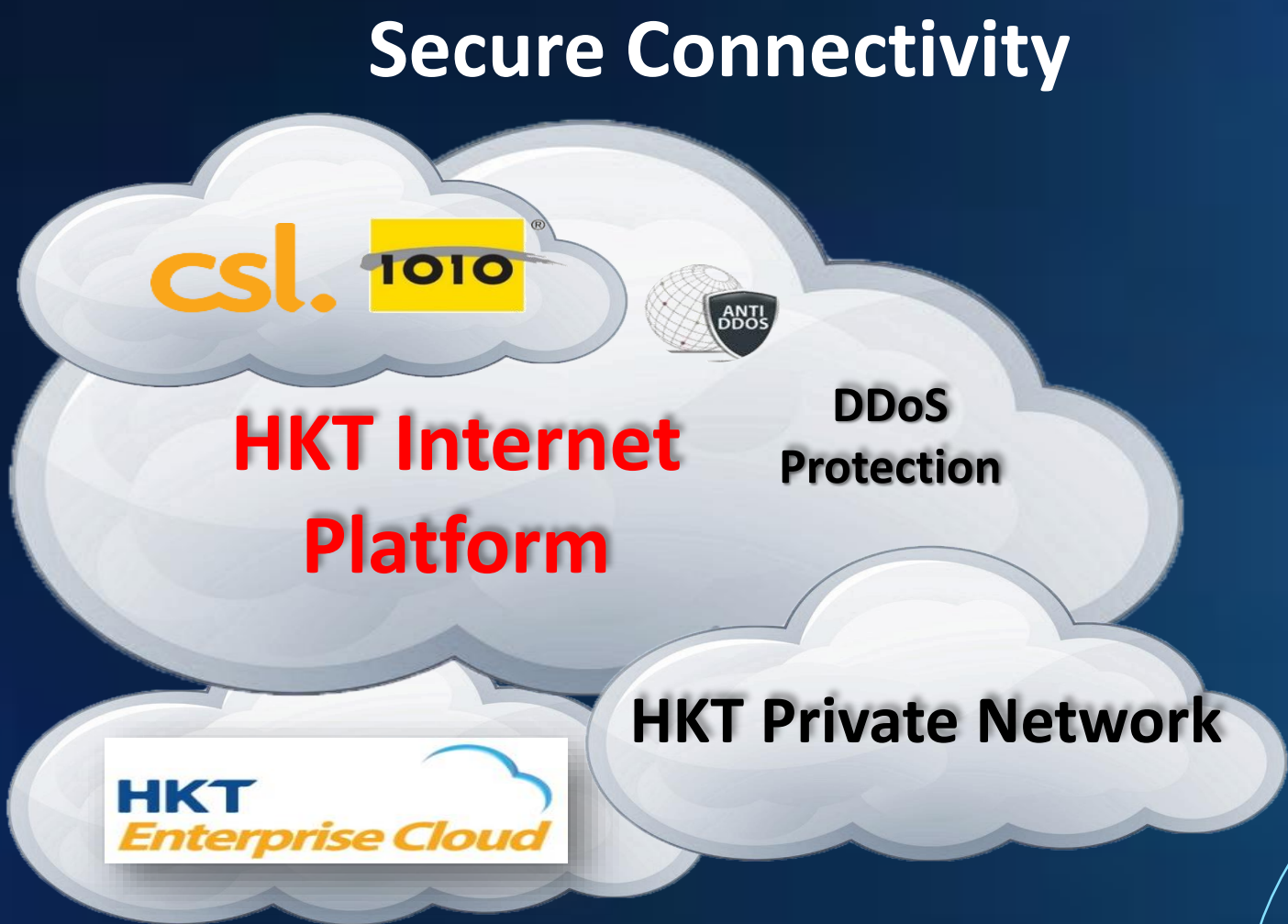
## Comprehensive Managed Security Service





# Key components on Security Management

## HKT School HelpDesk / Security Operation Center

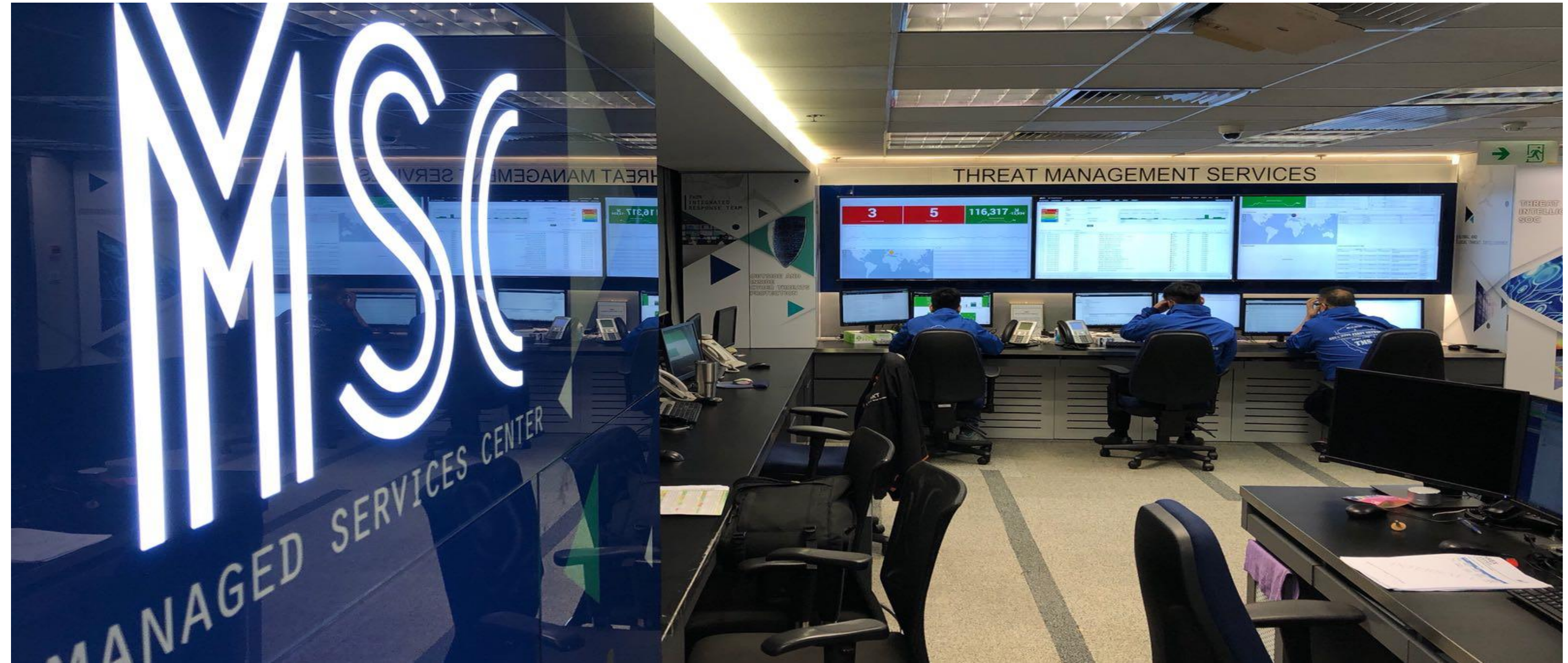




# Security Operation Center

- Security Expert
- Security Intelligence
- Security Management

Tools and Practice



SOC Manager

Tier 3

Tier 2

Tier 1








# School Helpdesk

## Background

於2017年5月12日晚起，全球各地的機構均受到一款名為**Wannacry**的勒索軟件所攻擊。近百國家在24小時內受到過10萬次的攻擊。牽涉範圍包括學校，銀行，公營機構，公用設施及政府機關等。因此導致大量公共受到影響而延後服務甚至癱瘓。更有英國醫院因系統停止服務導致手術臨時取消。

Wannacry一如其他勒索軟件，利用AES和RSA方式使用者電腦內的檔案迫使用戶提交贖金。**但當中的分別是**，駭客這一次利用了由美國國家安全局發的入侵工具EternalBlue針對性攻擊**Windows 10**系統的**SMB**服務執行遠端攻擊，因此駭客可透過進行短時間內的大規模攻擊且極難防備。

School Helpdesk Hotline: 187-2323



## Prevention (Con't)

- 7) 於Windows防火牆內可選擇性停用port 139及445，請注意這方法可能會對Windows影印機分享服務有所影響。  
  
控制台 -> 系統及安全 -> 防火牆 -> 進階設定 -> 輸入規則  
  
選取下列規則

## Prevention (Con't)

[illegible]

017 (Friday night)



related firewall TCP ports (139 & 445) in ALL school

- Occurred on 12-May-2017 (Friday night)



- 



- Completed all school wifi circuits (400+) on 15-May-2017 (Monday)



- Informed schools that HKT already take action to block the TCP ports via



- Dealing with the Data**

- Prepare user guide / preventive actions and sent to schools for them to take action on school's ITED network





# Key Takeaways

- Security Risk will keep **EVOLVING**
- **PERIODIC** Security Risk Assessment is important
- You **CANNOT** do it all by yourself
- Find a **TRUSTED PARTNER** for security management





Any Questions?

**Thank You**