



Security Operation Center (SOC) Service

KPMG Cybersecurity

KPMG China



kpmg.com/cn

Increasingly severe security situation

The threat landscape is continuously changing

Digital crime is estimated at \$450bn/yr globally and the impact of cyber incidents is growing. Today's digital organisation operates against an ever evolving cyber threat landscape and faces increasingly severe and complex cyber security attacks.

Robust Security Operations should help manage and reduce your cyber security risk. But it still face some challenges:

- Organizations turn to many industry-leading security technology, which leads to security monitoring that is performed using different tools and by different team. Piecing together the details of an attack in real time becomes incredibly difficult and even forensic analysis is slowed.
- How to build an effective intelligent SOC to improve the efficiency of global visualization and threat response, rather than just security device/ system stacking
- How SOC analysts deal with increasing volumes of alerts, many of which are false positives
- How to build the threat framework detection model related to the organization's security environment and security assets, which can be continuously and dynamically updated
- How to build an effective SOAR platform to automate based on whole process, rather than just blocking IP

Violation of compliance will bring serious economic losses

Since the implementation of the cyber security law of the people's Republic of China on June 1, 2017, all relevant ministries and industries have updated or issued relevant standards and

requirements, such as the information system security level protection 2.0, personal information security specification, etc.

At the same time, the "strength" and "granularity" of security inspection have been increased. In the national security inspection last year, most of the reasons for statistics of the organizations that have been attacked are still compliance control problems, such as weak password of VPN \ mailbox, no correction of website code execution loopholes, no sorting of Internet assets, security devices such as bastion machines unqualified the security control requirements. Therefore, even though each organization has established its own security management system in recent years, however, as the cornerstone of the whole security system, security compliance still faces the following challenges:

- Organizations lack a comprehensive understanding of their attack areas
- Passive inspection, not real-time and active monitoring, and the effectiveness of control measures cannot be quantified
- Safety compliance inspection stays at the level of baseline inspection and lacks the overall safety compliance situation display
- Various safety management requirements are too many to be effectively integrated and inspected
- There are many security assets and complex structure, which cannot guarantee the full coverage of inspection
- More reliance on personnel inspection can lead to fraud and inefficiency

Your Security Operations capability must also adapt

Security Operations needs to move beyond the traditional reactive routine and take a proactive stance that leverages disruptive technology such as artificial intelligence, machine learning and automation to address the challenges faced.

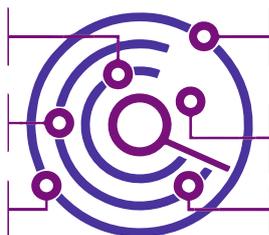
The future of Security Operations

"Given the increasing complexity and impact of cybersecurity attacks, and the increasing complexity of security tools generating alerts, organizations are looking to build or revitalize SOC's or outsource this function. By 2022, 50% of all SOC's will transform into modern SOC's with integrated incident response, threat intelligence and threat hunting capabilities, up from less than 10% in 2015"

Source: A view from Gartner's Top 7 Security and Risk Trends for 2019

Standardised

Define the SOC scope, measurement indicators, incident category, severity and process. Covering your entire organisation, following a consistent approach, to ensure you avoid blind spots.



Automated

Design playbook step by step based on use case. Leveraging SOAR (Security Orchestration, Automation and Response) tooling to accelerate response, increase productivity and allow your team to focus their attention where it really matters.

Agile

Being able to adapt and respond to the ongoing organisational changes and rapid shift in your attack surface.

Integrated

Enabling business and compliance integration, merging cyber detection and response capabilities and identifying synergies.

Risk-led

Threat model building and continuous follow-up, while enabling effective detection capability for threats applicable to your organisation, leveraging threat intelligence sources, asset level, vulnerability fixing status to determine your priorities and decide how you should respond.

Intelligent

Using an open architecture, flexible and adaptive analytical tools to allow you to make effective, fast decisions based on real-time insights.

You can't build a world-class SOC overnight no matter how much money you are willing to invest, the task is more of a marathon than a sprint. Creating a plan for incremental phases of implementation is critical to success.

Once you're identified what you need, it is important to realize that building a SOC requires collaboration and communication among multiple functions(people), disparate security products(technology), and varying processes and procedures(processes).

Source: building world class security operations center roadmap in 2015

Driving positive outcomes for your organisation



Reduced
Cyber risk



Effective
Security
Operations



Focused
Investment

How we can help:

Benefits for you:

<p>We can plan your security operation objectives and operation modes to help you build security operation capabilities consistent with the overall security objectives of the organization</p>	 <p>Planning</p>	<p>Risk-oriented, building a strong and secure operational capability can protect you from specific threats on an ongoing basis and meet compliance requirements Get the capacity building right the first time to maximize your investment in security operations</p>
<p>We can conduct gap analysis on the SOC of the organization based on the requirements of cyber security law, multilevel protection scheme, personal information protection, security management center, etc. We can assess the maturity of an organization's SOC based on international and domestic best practices.</p>	 <p>Assessment</p>	<p>Understand the gap with laws and regulations, identify improvement points Understand SOC security operations maturity to effectively improve your capabilities</p>
<p>We can design a security operation functional framework with SIEM as the security brain to effectively coordinate various security systems and devices. We can design scenarios such as threat framework model, Internet threat, Intranet threat, security compliance and information disclosure that match the customer's environment. We can design rule-based operation manuals and automation requirements, as well as automated risk assessment models</p>	 <p>Design/ Optimization</p>	<p>The autonomous and controllable threat monitoring model can keep the latest threats updated continuously User case analysis test method in detail Based on standardized risk rating model, security operation process and applicable user cases, effective security operation function is established</p>
<p>We can provide on site or non-on site security operation services such as vulnerability management, security threat monitoring and analysis, threat intelligence management, investigation and evidence collection, etc. We can provide intelligent security compliance subscription services to customers through deployment tools, and provide automatic or semi-automatic pre-compliance inspection, self-assessment posture display, reporting and real-time monitoring.</p>	 <p>Operation</p>	<p>Security operation service expected by customers Intelligent security compliance subscription service expected by customers Rapid delivery: familiar with international and domestic SIEM, security vulnerability, network traffic analysis, threat intelligence and other commercial or open source tools</p>

SOC Capability Model



Playbook and SOAR requirements

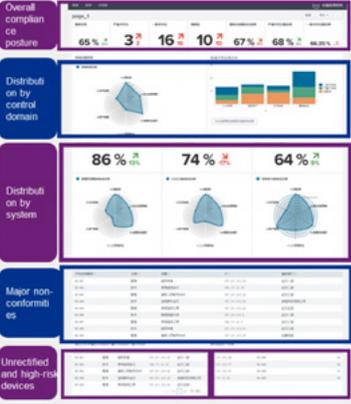
SOC maturity assessment



Based on ATT&CK & Kill chain threat framework and user case design

	Disgruntled Insider	Disgruntled Contractor	Contractor	Confidence Abuse	Caribbean Insider	Illegal Use of Corporate Assets	Organized Crime / Syndicates
Supplier violate use of personal data	X	X	X	X	X	X	X
Associate violate use of personal data	X	X	X	X	X	X	X
Non-Company Devices	X	X	X	X	X	X	X
Web Traffic	X	X	X	X	X	X	X
Webmail	X	X	X	X	X	X	X
Company Devices	X	X	X	X	X	X	X
Internal Email	X	X	X	X	X	X	X
Data Replication	X	X	X	X	X	X	X
User Download	X	X	X	X	X	X	X
Network Storage	X	X	X	X	X	X	X
Peer-to-Peer	X	X	X	X	X	X	X

SOC Compliance Dashboard



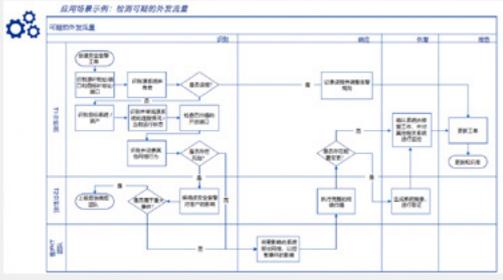
Overall compliance posture: 65% (3, 16, 10, 67%, 68%)

Distribution by control domain

Distribution by system: 86%, 74%, 64%

Major non-conformities

Unrectified and high-risk devices



Initial Recon	Initial Compromise	Establish Footprint	Escalate Privileges	Internal Recon	Move Laterally	Maintain Presence	Complete Mission
Host Scan	SMS Bomb	Remote Command Execution	High Risk Command	Host Scan	Remote service	Modify Scheduled Task	EDOS
Port Scan	Brute Force	Access Control Modification	Escalate Privilege Attack	Port Scan	SMB Attack	Extra Connection	DNS Tunnel
WEB Scan	Enumerating	SQL Inject	Security Bypass	Network Share Discovery	Pass USB	Command Abnormal	File/ Data Deletion
Remote Code	Port Redirect	Log Abnormal	Account Abnormal	Third-party Software	External Remote Service	Malicious Domain Name	
URL Redirect	Log Abnormal	Account Abnormal	Account Abnormal				
SOE Inject	Data Connection	Account Abnormal	Account Abnormal				
WEBSHELL							

Assist you to complete the digital transformation of security, active defence, continuous monitoring, rapid and effective response and disposal, escort for the business!

Contact us

Henry Shek

KPMG China
Cybersecurity
Partner
Tel: +852 2143 8799
henry.shek@kpmg.com

Richard Zhang

KPMG China
Cybersecurity
Partner
Tel: +86 (21) 2212 3637
richard.zhang@kpmg.com

Quin Huang

KPMG China
Cybersecurity
Director
Tel: +86 (21) 2212 2355
quin.huang@kpmg.com

Danny Hao

KPMG China
Cybersecurity
Director
Tel: +86 (10) 8508 5498
danny.hao@kpmg.com

Brian Cheung

KPMG China
Cybersecurity
Director
Tel: +852 2847 5062
brian.cheung@kpmg.com

Frank Wu

KPMG China
Cybersecurity
Associate Director
Tel: +86 (21) 2212 3180
fm.wu@kpmg.com

Jason Song

KPMG China
Cybersecurity
Associate Director
Tel: +86 (21) 2212 3306
jason.song@kpmg.com

Jason Li

KPMG China
Cybersecurity
Associate Director
Tel: +86 (10) 8508 5497
jz.li@kpmg.com

John Chiu

KPMG China
Cybersecurity
Associate Director
Tel: +852 2847 5096
john.chiu@kpmg.com

Kevin Zhou

KPMG China
Cybersecurity
Associate Director
Tel: +86 (21) 2212 3149
kevin.wt.zhou@kpmg.com

Kevin Fan

KPMG China
Cybersecurity
Associate Director
Tel: +86 (21) 2212 2200
kc.fan@kpmg.com

Olive Wang

KPMG China
Cybersecurity
Associate Director
Tel: +86 (10) 8553 3630
oh.wang@kpmg.com

Andy Yuen

KPMG China
Cybersecurity
Associate Director
Tel: +852 3927 4697
andy.yuen@kpmg.com

William Xu

KPMG China
Cybersecurity
Associate Director
Tel: +86 (21) 2212 4633
william.q.xu@kpmg.com

kpmg.com/cn/socialmedia



For a list of KPMG China offices, please scan the QR code or visit our website:
<https://home.kpmg.com/cn/en/home/about/offices.html>

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

© 2020 KPMG Huazhen LLP, a People's Republic of China partnership and KPMG Advisory (China) Limited, a limited liability company in China, are member firms of the KPMG global organisation of independent member firms affiliated with KPMG International Limited ("KPMG International"), a private English company limited by guarantee. All rights reserved. Printed in China.

The KPMG name and logo are registered trademarks or trademarks of KPMG International.