Development of Cyber Security Operations
網絡安全營運的發展

HKT
香港電訊

Introduction

It is no doubt that all the business activities are heavily relied on the Information Technology (IT) ranging from the mobile apps, web applications and online transactions in these days. While the IT development does bring a lot of benefit to business and convenience to general public, it is creating a greater risk in the IT security. We realized that a quantum jump in volume of cyber-attacks has been recorded in the recent years. The varieties of attacks including ransomware, loss of personal identifiable information, forgery in financial transactions and many mores, effectively put the personal and business activities under the risk of a huge financial loss. Cyber Security is emerging as a key element to protect the confidentiality, integrity and availability of IT infrastructure and data.

Corporations no matter big or small should adopt a prudent approach towards cyber security because increase of cyber-attacks and data breaches incidents become a major risk and challenge in Hong Kong as a financial centre in Asia. We have seen a number of well publicized data breach such as credit cards information being stolen. Cyber threats will continue to have an outsized impact on Hong Kong business operations, and it can erode public trust and reduces the ability to deliver effective and reliable financial transactions.

Staying on Top of the Cyber Attacks

The core function of cyber security in a corporation should focus on creating a security program that is anchored on PREVENT-DETECT-RESPOND. Prevention could be interpreted as the fortification of the cyber security infrastructure such as deploying two tiers firewalls, IPS (Intrusion Prevention system), DLP (Data Loss Protection) application etc. The aim is to protect the valuable assets of an organization, e.g. customer records and financial data. Another aspect of prevention is the cyber security policy, which must be clearly defined and executed accordingly. The common practice is to adopt well recognized standard, namely the Center for Internet Security (CIS) Critical Security Controls for Effective Cyber Defense as guidelines for computer security within an organization. It is usually referred to CIS Top20 guidelines, which have 20 most effective practices to avoid most of the cyber security breach.

Detection involves capability to detect any anomaly in IT environment of organization. In the latest approach of cyber defense, all organizations should assume they have been

前言

無可否認，由流動應用程式（APP）以至網頁應用程式（Web Application）及網上交易，現今所有業務營運都非常依賴資訊科技。雖然資訊科技確實為業務帶來很多好處，並為公眾提供便利，但卻在資訊科技安全方面帶來更大的風險。在近年，網絡攻擊次數急升，勒索軟件、個人驗證資料（PII）外泄、偽造交易紀錄等不同攻擊手法對個人及商業活動帶來極大的經濟損失風險。因此，網絡安全正在成為保護資訊科技基礎架構和數據的機密性、完整性和可用性的關鍵要素。

面對日益頻繁的網絡攻擊及數據外泄問題，香港作為亞洲金融中心，不論大小企業都應對網絡安全採取審慎的態度。例如信用卡資料失竊等數據泄露事件早已是眾所周知。網絡威脅不但持續為本地業務營運巨大影響，更會令公眾質疑企業能否參與有效和可靠的金融交易。

即時跟進網絡安全

就企業而言，網絡安全應該要建立一個以「預防-檢測-應對」（Prevent-Detect-Respond）為基礎的安全計劃。「預防」（Prevention）可以理解為強化網絡安全基礎設備，例如部署兩層防火牆（Two-tier Firewall）、入侵防禦系統（IPS）、資料外泄防護（DLP）等，目標是保護機構的客戶紀錄、財務資料等重要資產。另一方面，「預防」也可以通過執行清晰、確切的網絡安全政策（Security Policy）進行。最常見的做法是推行業界認可的「CIS關鍵安全控制措施」（CIS Critical Security Control），作為企業的電腦保安實務守則。該守則列舉防止應付攻擊的20個關鍵行動，協助企業抵禦網絡攻擊。

「檢測」包括在企業的資訊科技環境中偵測「異常」（Anomaly）情況的能力。在最新的網絡防禦方法中，所有組織都應該假設黑客已經以某些方法入侵其網絡。根據2018年的統計資料，亞太區企業到從系統受感染到檢測到的平均時間（即Dwell Time）為498日。可以想像，黑客在這段長時間中能對企業造成巨大的損失。因此，「檢測」能力在網絡防衛工作中顯得更為重要。

以往我們依賴特徵檢測（Signature-based detection）的設備及軟件作為主要檢測系統。然而，自2014開始，惡意軟件的數

compromised by hackers in some ways. Research results in 2018 indicated that the average duration to discover systems being compromised (commonly called Dwell Time) by organizations in Asia Pacific Region was 498 days. The hacker could certainly do a lot of damage within an organization in such a long time. Therefore, the detection capability becomes more critical in the cyber security defense chain.

In the past, we could rely on the signature base detection appliance or application as our main detection system. As the growth of malware was in exponential orders since 2014, there were around 350,000 new variants of malware being developed each day in 2018 according to the research of AV-Test Institute. It makes the signature-based detection becomes less effective because the determined hackers could produce a variant in short time to by-pass the anti-virus software and detection system.

Adopting the Best Practice on Cyber Security

In response to ever increasing hackers' activities and evolving technique, US Government advocates a new approach with four key innovative strategies to defend against and mitigate cyber-attacks. They are:

1. Proactive cyber threat hunting
2. Increased use and sharing of cyber intelligence data
3. Continuous security monitoring, with an emphasis on boundary protection and security event lifecycle management
4. Automation and orchestration of security operations

Proactive cyber threat hunting is usually riding on big data analytics. The advanced Security Operation Centres around the world currently devoted a lot of effort to produce detection scenario through the various data analytics and machine learning technique. This approach provides an in-depth analysis of any new attacker's tactic, technique and procedure, and is the most powerful way to detect any APT (Advance Persistent Threat) group or Zero Day attack in these days.

Sharing of the cyber intelligence does have the benefit to detect the new malware more effectively. One of the common practices to share cyber security information is through Information Sharing and Analysis Center (IT-ISAC), which is a nonprofit organization being set up worldwide that provides a central resource for gathering information on cyber threats to critical infrastructure and providing two-way sharing of information between the private and public sector. There are many close sharing groups for specific industry such as finance, utility and transportation.

HKT has established a Next Generation Security Operations Centre (NG SOC) based on an adaptive security model aiming to tackle the latest malicious attack in the form of APT and Zero Day Attack. HKT NG SOC rides on a large pool of cyber security expertise and makes use of big data analytics together with Cyber Threat Intelligence (CTI) platform to provide a brand of professional services namely, Threat Management Services (TMS).

量以幾何級數增加；根據外國組織AV-Test Institute的研究，在2018年，每天有多達35萬個新的惡意軟件出現。換言之，黑客可以利用惡意軟件變種來突破特徵檢測的防禦機制，使機制的效用變得十分有限。

採用「最佳實務守則」

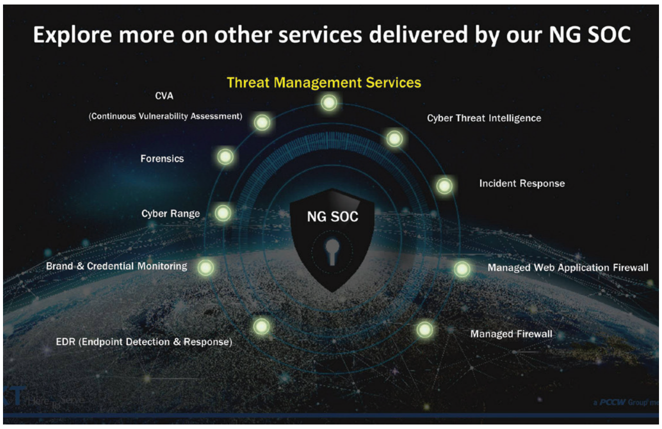
因應著黑客大量、多變的攻擊手法，美國政府提倡以4個重點創新策略方法用作抵禦網絡攻擊，包括：

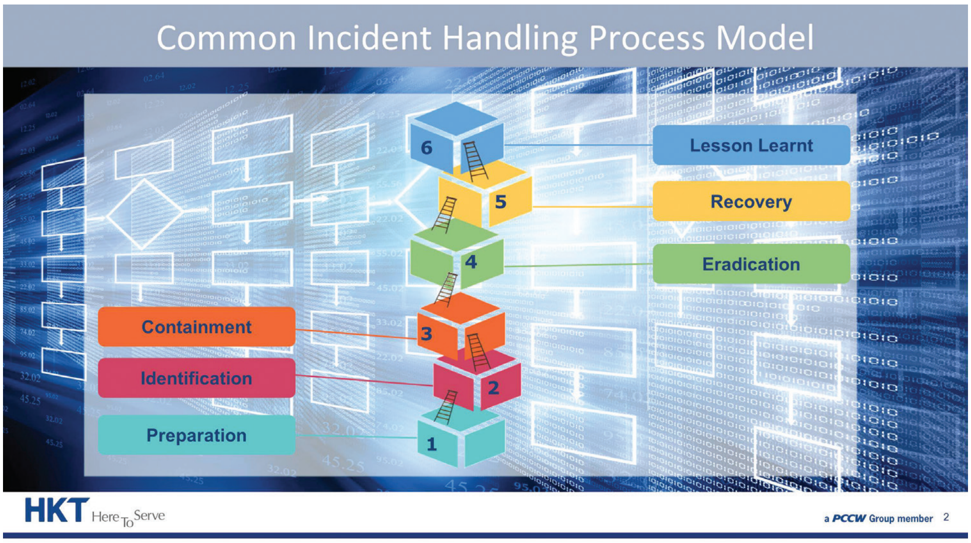
1. 主動追蹤威脅
2. 提升運用及分享網絡威脅的情報
3. 持續保安監察，著重邊界防衛及保安事件管理
4. 安全編排、自動化及應對

主動追蹤威脅通常依靠大數據分析。現在，世界各地的保安營運中心（Advanced Security Operation Center）利用數據分析及機器學習的方法來建構檢測方案。這種方法能夠深入分析黑客的策略、技巧及程序，亦是現今偵測「進階持續性滲透攻擊」（APT）及「零時差攻擊」（Zero Day Attack）的最有效方法。

此外，分享網絡威脅的情報能幫助我們更有效偵測新的惡意軟件。其中一個普遍分享情報的方法是IT-ISAC（Information Security Analysis Center）。IT-ISAC是一個世界性非牟利組織，統一收集及提供關於威脅私營、公營關鍵基建的情報。此外，亦有專門為不同行業而設的威脅情報，例如金融、公共基建、交通運輸等。

香港電訊採用適應性安全模式為基礎，建立了新世代網絡安全監控中心（NG SOC），應對最新的「進階持續性滲透攻擊」或「零時差攻擊」手法惡意攻擊。香港電訊的新世代網絡安全監控中心運用本地工程綜合團隊和大數據分析，配合新世代網絡威脅情報資訊平台 Cyber Threat Intelligence（CTI），為企業提供專業的資訊安全威脅管理服務Threat Management Services（TMS）。TMS服務包括24小時的監察、檢測、應對網絡安全事故以及其他專業服務。


Explore more on other services delivered by our NG SOC
Threat Management Services
CVA
(Continuous Vulnerability Assessment)
Cyber Threat Intelligence
Forensics
Incident Response
Cyber Range
NG SOC
Brand & Credential Monitoring
Managed Web Application Firewall
EDR (Endpoint Detection & Response)
Managed Firewall
a PCCW Group member



TMS includes 24 x 7 surveillance, detection, incident response and related professional services.

Responding to Cyber Security Incidents Effectively

Both Security Event Lifecycle Management and Automation and Orchestration of security operations are mostly related to security incident handling. Organizations should have the incident response plan, which consists of communications and practice of incident response process, in place. Otherwise, they are running into a big risk that their IT would easily turn into a chaos under a cyber-attack.

The current best practice of Incident Response divides the handling process into six different phases. Each phase is extremely important to follow in sequence, as each one builds upon the other. The following phases are mostly adopted by the cyber security practitioners. They include preparation, identification, containment, eradication, recovery and lesson learnt. The lesson learnt phase is very important in terms of knowledge and experience build-up as well as the information sharing through ISAC group.

HKT NG SOC adopts the latest incident response methodology which is based on intelligence driven incident response. When we come to identify the hacker's tactic, technique and procedure, it becomes more effective to discover the full extent of new malware attack comparing to the traditional incident response process which is malware centric. HKT NG SOC has deployed the SOAR platform to facilitate the alert analysis and automate the triage process as much as possible. It brings the benefit of being able to respond to large amount of cyber security alerts within a short time and filter out the false positive effectively.

HKT also invests a lot of resources to groom a pool of cyber security specialists to operate the NG SOC. These efforts have been recognized by HKT NG SOC winning the open competition Top of SOC (BOTS) a Capture-the-Flag style event in November 2017, and the Best Managed Detection and Response Partner Award of North Asia 2018 by a renowned cyber security Big Data

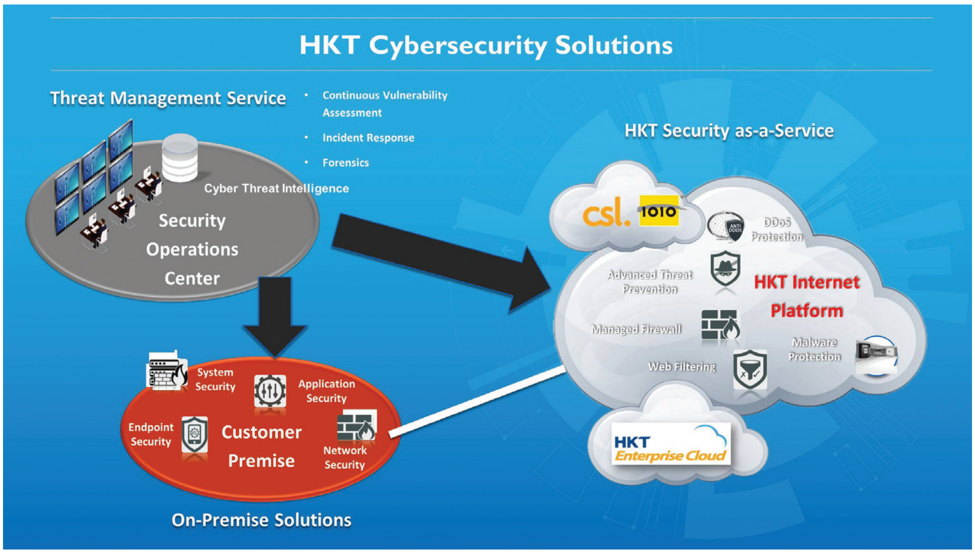
有效率地應對網絡保安事故

「保安事件管理」及保安營運的「安全編排、自動化、應對」與處理網絡保安事故有莫大關連。企業必須制定好保安事件的應變方案，例如通報、應對流程等，否則，當遇到網絡攻擊時就得容易因未能及時處理，為企業的資訊科技設施帶來混亂的風險。

目前，應對網絡事故的最佳實務守則分六個階段。順序執行每個階段的步驟是非常重要，因為每個階段的行動都是建基於前一個階段的結果。這六個階段包括準備（Preparation）、辨識（Identification）、遏制（Containment）、根除（Eradication）、恢復（Recovery）以及經驗傳承（Lesson Learnt）。其中，「經驗傳承」階段對於建構團隊的知識庫、經驗，以及對威脅情報分享是尤其重要。

香港電訊旗下新世代網絡安全監控中心應對網絡事件的最新方法是以「智能推動」（Intelligence-driven）為本。對於偵測及應對前面所提到的黑客策略、技巧及程序，用這種方法來偵查整個攻擊的流程，遠比過往「特徵檢測」的方式更為有效。香港電訊的資訊安全管理中心利用「安全編排、自動化、應對」管理平台，盡可能將警報分析和分流自動化，從而可以在短時間內處理大量的資訊安全警報，並有效過濾假陽性個案。

香港電訊亦投入大量資源培訓資訊安全科技人才，以配合新世代網絡安全監控中心運作。香港電訊在這方面的努力深受業界認同，於2017年11月的 BOTS （BOSS of SOC）奪旗賽中載譽歸來，並於2018年5月榮獲一間著名的資訊安全大數據供應商頒發「The Best Managed Detection and Response Partner Award of North Asia 2018 」獎項。新世代網絡安全監控中心的專家亦於本年「網絡安全精英嘉許計劃」中獲香港警務處和政府資訊科技總監辦公室頒發獎項，彰顯香港電訊在網絡保安方面的整體能力和質量。



Vendor in May 2018. The members of HKT NG SOC also won CSPA (Cyber Security Professional Awards) awarded by HK Police Force and OGCIO this year. These awards demonstrate the global capability and quality of HKT's cybersecurity strength.

HKT's Response to Cyber Security Needs

In view of the demand of highly technical expertise to run a cyber-security program for each organization, HKT offers an all-round cyber security solutions suite providing end to end cyber security solutions covering WAN, LAN, Wireless and Wireline environment. There are three core components that support HKT to deliver superb cyber security solutions to corporates and the community. They are NG SOC (Next Generation Security Operations Centre), Fixed and Mobile Network Operations and Security Control, CTI (Cyber Threat Intelligence). Based on these three cores functions, HKT leverages the capabilities to support all aspects of our solutions suite including Security-as-a- Service, which provides a network based protection such as DDoS and DNS attack. Other types of services include Professional Services (such as Vulnerability Assessment and Management), On-Premise System supports (such as security infrastructure setup) and Managed Security Services (such as managed Web-Application firewall service). HKT continues to build cyber securities capabilities through NG SOC and develop more services to meet the needs of business community.

Conclusion

As the cyber security landscape is in ever evolving state, corporations have to gear up the cyber security capability to mitigate the cyber threat through adopting the best practice and automation platform. The practice of PREVENT–DETECT–RESPOND should be implanted into the IT security operations of each organization.

香港電訊應對資訊安全的需要

因應市場對資訊安全人才短缺和技術的需求殷切，香港電訊提供全面的資訊安全服務方案，涵蓋廣域網（WAN）、局域網（LAN）、無線網絡（Wireless）以至固網（Wireline）。這套資訊安全服務方案是由三個核心元素組成，讓香港電訊能為商業機構及社會提供超卓的網絡安全服務，包括新世代網絡安全監控中心（NG SOC）、固網及流動通訊網絡的營運和安全管理，以及網絡威脅情報資訊平台（CTI）。香港電訊藉著運用這三個核心元素的能力，支援服務方案的各個層面，包括安全即服務（Security-as-a-Service），提供以網絡為本的保障，以抵禦拒絕服務攻擊（Anti-DDoS）或網域名稱系統攻擊（DNS）。其他的資訊安全專業服務包含多項專業服務（例如漏洞評估及管理）、上門系統支援（例如網絡安全基礎建設）以及管理式網絡安全服務（例如託管Web應用程式防火牆）。香港電訊會繼續提升資訊安全技術和能力，開發更多服務以滿足商界的需要。

結論

網絡保安服務的市場發展一日千里，各業機構需要做好準備，採用最佳實務守則及自動化平台，同時應在其資訊科技營運中應用「預防-偵測-應對」（Prevent-Detect-Respond）的策略，以提升抵禦網絡威脅的能力。