Solutions for Cyber Security Challenges of the Tokyo 2020 Games

TAMAI Kuniharu　NOJIRI Yasuhiro　HOSODA Naofumi
IBAYASHI Hiroaki

Abstract

The Olympic and Paralympic Games Tokyo 2020 have been managed by a large number of systems. In order to protect the Olympic and Paralympic Games Tokyo 2020, it was necessary to strengthen security by hardening each system and implementing defense in depth solutions for detecting, preventing, and responding to attacks as a security solution. This article describes how system hardening and security solutions have been implemented.

Keywords：Tokyo 2020 Games, Cyber attack, Security solution

1. Introduction

The Olympic and Paralympic Games Tokyo 2020 (hereinafter referred to as "Tokyo 2020 Games") utilized a large number of systems to manage the Games, and these systems were located in various domains depending on their purposes. The specific domains included the Back Office Network (BON) used by Tokyo 2020 Organising Committee members for their work, the Competition Network (CPN) that connects the venues, the Olympic Technology Network (OTN) which was a network to accommodate various services, such as dedicated VLANs for games stakeholders, and the website domain in the Cloud. By implementing security solutions for the characteristics of each of these domains, we aimed to comprehensively enhance security before the Games. This article introduces the details.

2. Common Security for All Domains

In Section 2, we introduce the common issues for all domains and examples of countermeasures implemented to solve them.

First, a typical issue was the prevention of leakage of credential information such as authentication IDs and passwords, as well as confidential information. Ideally, systems should be implemented and operated in compliance with predefined rules, but unfortunately in some cases the rules could not be fully complied with, because many organizations and companies were involved in the implementation and operation of each system in Tokyo 2020 Organising Committee. For this reason, it was important to implement strict security functions and to organize systems to operate security from the viewpoint of zero trust. Zero trust refers to the concept of taking security measures in advance without trusting all communications, assuming that not all attacks can be protected by the conventional approach of dividing the network into trusted and untrusted areas and restricting communications between the two areas. Specifically, authentication methods were strengthened to increase the durability against leakage of credential

TAMAI Kuniharu
Technology Services Bureau, The Tokyo Organising Committee of the Olympic and Paralympic Games
NOJIRI Yasuhiro
Technology Services Bureau, The Tokyo Organising Committee of the Olympic and Paralympic Games
HOSODA Naofumi
Technology Services Bureau, The Tokyo Organising Committee of the Olympic and Paralympic Games
IBAYASHI Hiroaki
Technology Services Bureau, The Tokyo Organising Committee of the Olympic and Paralympic Games

The Journal of The Institute of Electronics, Information and Communication Engineers, Vol.105, No.8, Supplement, pp.264-271, August 2022

information, and the possessed data was encrypted using mechanisms such as IRM (Information Rights Management) so that files could not be viewed even if they are leaked to the outside.

Other examples included configuration management to quickly grasp the impact on the system when new risks such as vulnerabilities were discovered, and countermeasures against DDoS (Distributed Denial of Service) attacks.

These are described in detail below.

2.1 Thorough Protection of Credential Information

In many cases, security incidents are caused by attackers exploiting the credentials they have obtained illegally, pretending legitimate users and infiltrating devices or systems. In order to make it impossible to break in easily even if some of the credential information were leaked, Tokyo 2020 Organising Committee had thoroughly strengthened authentication method by using of Multi-Factor Authentication (MFA) in principle. Even when MFA could not be used due to device restrictions, security had been reinforced by restricting the source IP address.

In addition, the use of shared accounts was prohibited, and it was made to be thorough to use individual accounts with the minimum privileges granted as necessary. This enabled the logging of privileged operations, ensured traceability, and enabled prompt detection of any credential abuse.

In addition to these measures, we also prevented credential leaks. Tokyo 2020 Organising Committee set a password policy that was stronger than the general standard, specifically, passwords must have been at least 10 characters long and contain at least three different types of characters. This was intended to increase the strength of passwords and prevent their reuse by making them stricter than the requirements for general services. In addition, we issued the warning that the passwords were not to include words related to the Tokyo 2020 Games, which were easily recalled by attackers, and password cracking tests were conducted monthly to confirm the actual passwords. Furthermore, just prior to the Games, all staff members' passwords were reset. We believe that this has completely invalided any credential information that might have been passed to an attacker.

However, these measures cannot be applied directly to future Games. Password policy standards are becoming more complex every year, and there have been reports of MFA being breached in some implementations. It is necessary to select credential protection methods in accordance with changes in attack methods and corresponding countermeasure technologies.

2.2 Configuration Management and Vulnerability Management

Managing configurations and vulnerabilities are very significant challenges because each system consists of wide variety of devices and software. If newly discovered vulnerabilities are not addressed in a timely manner, or if some of them remain unaddressed, the vulnerabilities will be used as footholds for intrusion into the system, resulting in major damage.

In order to take appropriate measures against vulnerabilities, configuration management and vulnerability information gathering are essential. Configuration management is to comprehensively keep track of all the devices, software and their versions. Vulnerability information gathering is to promptly understand details of newly discovered vulnerabilities. Furthermore, it is important to visualize the impact of vulnerabilities and the progress of countermeasures of all systems. Tokyo 2020 Organising Committee introduced several types of configuration management systems according to the types of devices and software, and always kept that all devices and software were registered without omission through security checks. For vulnerability information gathering, in addition to dedicated platform for collecting vulnerability and threat information, we also took advantage of Threat Intelligence from outside agencies, such as the JPCERT/CC, information sharing platforms provided by the government and the International Olympic Committee, etc. By making maximum use of them, we established a system that enabled us to collect a wide range of vulnerability information quickly and in detail.

In addition, a centralized configuration deployment system is essential to promptly complete actions such as updates and workarounds after the discovery of vulnerabilities. In principle, Tokyo 2020 Organising Committee used centrally managed PCs to enable batch configuration changes. For devices that are not subject to centralized management, we clearly identified administrator for each devices and direct them to take appropriate action promptly for each vulnerabilities.

2.3 DDoS Protections

Any environment connected to the Internet must be prepared for DDoS attacks that aim to disrupt the use of the environment. Although DDoS is known to target websites, any environment connected to the Internet can be a target.

Since DDoS protection requires large-scale environment in the network infrastructure, the Organising Committee implemented a common implementation rather than individual protections. For BON, CPN, and OTN, we adopted a scrubbing center type of the service which pulls in communications and separates offensive communications from legitimate ones. On the other hand, for Web sites, we adopted CDN (Content Delivery Network). By utilizing these services, we protected our services from DDoS attacks.

3. BON and CPN Security

For both BON and CPN, a number of security solutions were implemented for the network and endpoints such as PC terminals and servers based on the concept of defense in depth (Figure 1). Basically we have prevented the intrusion of attackers by defense-in-depth through perimeter defense by network security, hardening to minimize attackable points by stopping unnecessary functions and appropriately enabling security functions, and endpoint defense by anti-malware software. And based on the concept of zero-trust, we have managed privileges strictly and have introduced mechanisms to detect suspicious behavior. The details of these measures are described below.

3.1 Network Security

The network was divided into zones such as Secure, Trusted, Edge, DMZ, etc., and communication between these zones were restricted by using the whitelist to block malicious communication on Proxy, UTM (Unified Threat Management), IPS/IDS (Intrusion Protection/Detection System), and firewalls according to the IT security architecture. The traffic flow was monitored by NDR (Network Detection and Response) for early detection of attacks and anomalous communications. Even within the same zone, communication between terminals was restricted to prevent lateral movement, which was the expansion of the range of attacks and infection in the case of internal intrusion. 802.1x authentication was also used to prevent unauthorized terminals from connecting to the network.

For the use of Internet services, the possibility of

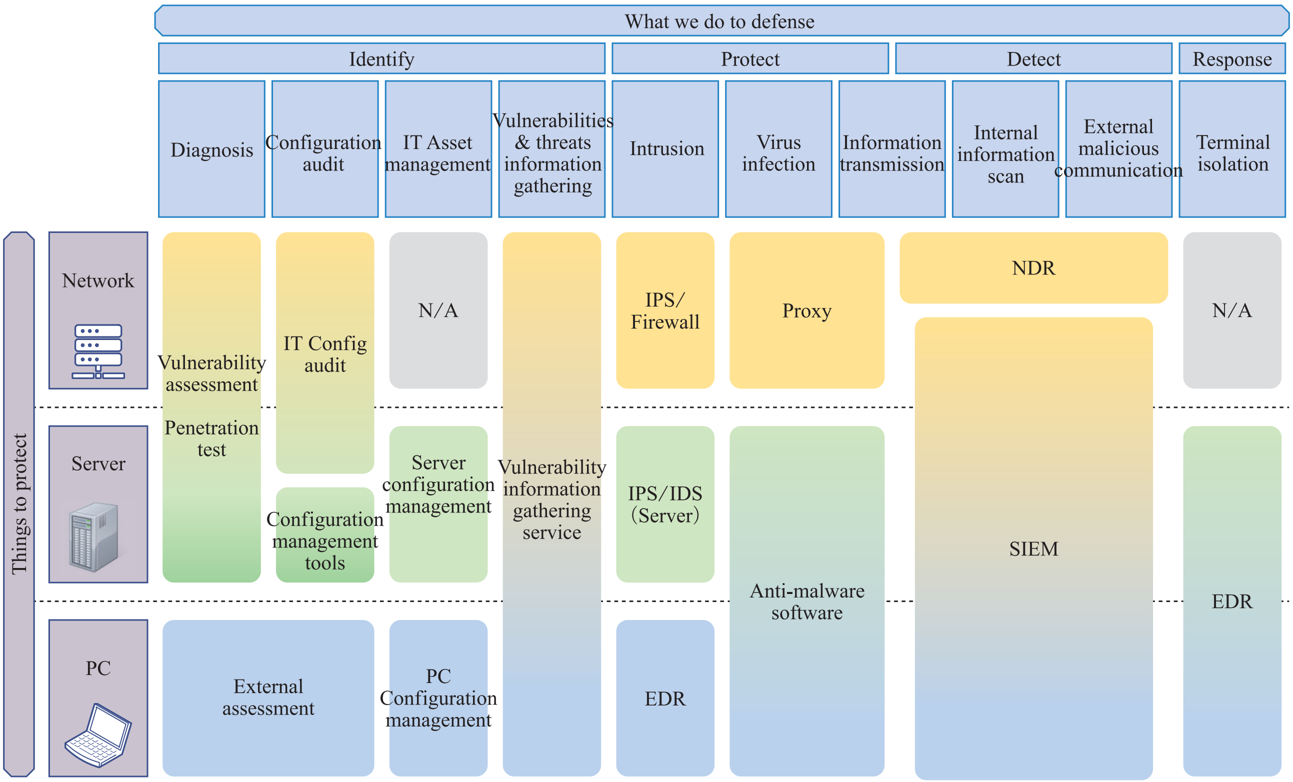


Figure 1 Defense in Depth Solutions

access to malicious sites and the introduction of malware into the BON/CPN was reduced by DNS filtering, URL filtering functions of proxy, anti-virus functions, sandbox functions, and other functions. Furthermore, the use of free Internet storage services and Internet e-mail services, which had been the target of attacks in the past Games, was prohibited, and other services were restricted appropriately to reduce the risk of information leaks.

As security measures for network devices themselves, they were configured in accordance with Tokyo 2020 Organising Committee's configuration standard (Configuration Standard) to ensure uniform hardening. Security logs of devices such as UTMs and proxies were captured by SIEM (Security Information and Event Management) and UEBA (User and Entity Behavior Analytics).

3.2 PC Security

Tokyo 2020 Organising Committee also had a Configuration Standard to fortify PC terminals. The Standard defined Windows OS security features such as credential protection, execution control by application whitelisting, vulnerability mitigation and disk encryption and Windows Group Policies such as restrictions on macro execution, restrictions on account synchronization and extension usage of browser, randomization of privileged administrator passwords, etc. Security was enhanced through the use of the Standard.

In addition to the above, security was further enhanced by deploying multiple perspectives by installing multiple security solutions, specifically anti-malware software, EDR (Endpoint Detection and Response), SIEM, and UEBA.

Although some of the functions of anti-malware software overlapped with those of EDR, the anti-malware software was mainly used for restrictions on script execution such as PowerShell and on external device connection and flexible policy application according to the connected network, while EDR was mainly used for incident response such as PC terminal investigation, specimen acquisition and quarantine. There was a difference in the scope of deployment between anti-malware software and EDRs, which will be discussed in detail in Section 4.

SIEM was used not only to collect logs of network devices, but also to obtain PC security logs and output logs of anti-malware software for analysis and visualization. SIEM could detect the use of privileges and the execution of scripts whose use was prohibited in the BON/CPN. But it was not possible to determine whether the detection result was an attack action or an operational task by the system administrator, so we implemented a process to check each time a detection was made to see if the user had performed the detected operation. In addition to SIEM, logs were also incorporated into UEBA, which could detect not explicitly suspicious behavior but unusual behavior.

The above was the basic policy, but since CPN PC terminals handled competition data in real time, the design policy was adjusted to give priority to avoiding functional impact. Specifically, we decided to implement periodic scans instead of real-time scans for malware countermeasures.

3.3 Server Security

In the server environment, security was reinforced at a higher level not only by the same hardening and security solutions as for PC terminals, but also by implementing auditing mechanism to check the validity of settings and patch application status and installing IDS/IPS software.

In particular, AD (Active Directory), which was the core of operation and management, was more carefully secured than general servers. Specifically, AD security was strengthened by introducing a tier model that classify administrators based on the resources they manage, by access control of requiring connections via a dedicated stepping stone server for AD operation and by a dedicated mechanism to detect suspicious activity from the contents of AD-related communications. AD logs were also imported into SIEM and monitored with special attention by implementing logic to detect suspicious behavior related to AD authentication.

Based on the same approach as for PC security, we did not implement IDS/IPS for CPNs, which would have placed a heavy load on the system.

4. OTN Security

4.1 Network Security

The OTN network was divided into separate networks for each service. Moreover, as in the case of the BON and CPN, UTM was installed at the connection points to the Internet, traffic flows were monitored by NDR, DNS filtering was performed, and hardening was performed according to the Configuration Standard. However, because of the wide range of applications, it was difficult to use the whitelist, which registered in advance the communications to be allowed, so the blacklist was adopted, where communications determined to be malicious by security operations were added sequentially.

In addition, since a large number of devices brought in by guests were connected to the OTN, there was a high risk that malicious devices might be connected by slipping into them. Based on this premise, multiple countermeasures against malicious device connections were implemented. For example, when connecting to services such as broadcasting and press, MAC address authentication was performed and communication between terminals was restricted to mitigate the risk of lateral movement attacks. Captive portal authentication using accreditation IDs (IDs used to control the admission of Games stakeholders to the venue, etc.) was introduced in the guest network to connect to the terminals brought in by guests.

4.2 PC Security

Each user had various requirements for PC terminals brought into the OTN, and it was very difficult to implement uniform security measures. Considering these conditions, to prevent infection of PC terminals and the spread of infection between terminals, a security review was conducted for each system to determine the minimum requirements for PCs used in the system, and each system was strongly requested to comply with these requirements.

In addition to the terminals brought into the OTN, there were also loaner PC terminals managed by Tokyo 2020 Organising Committee for the use of Games stakeholders. The loaner PC terminals were used by the athletes staying in the athletes' village and by critical infrastructure providers, and like the terminals brought in, they must be able to use for a variety of purposes. On the other hand, because of the wide range of users, it was difficult to disseminate the policies of Tokyo 2020 Organising Committee to all users, which could have resulted in numerous security incidents. Considering these conditions, we decided to avoid using strict security settings with anti-malware software in order to maintain the usability of PC terminals, and instead, we have adopted a policy of implementing EDR of the same level as BON/CPN to detect and respond to incidents as soon as they occurred. Furthermore, since the cooperation of PC terminal users was indispensable for incident response, we have obtained an agreement with the users in advance by stipulating in the OTN terms of use that they must cooperate with response in the event of an incident.

As a result, several incidents actually occurred during the Games Time, but we were able to respond promptly as expected and deal with them without causing any damage.

In addition, there were some issues to be considered for future Games regarding the selection of anti-malware and EDR solutions for loaner PC terminals. This is explained in Section 4.3.

4.3 Consideration of Solution Configuration and Scalability

In deciding on a security solution for OTN PC terminals managed by Tokyo 2020 Organising Committee, we considered the possibility of expanding the BON/CPN solution, but we had to give up due to limitations imposed by the solution architecture.

Many security solutions require not only an agent installed in each PC terminal, but also a manager that manages the group of agents. The manager can be deployed on-premises (hereinafter referred to as "on-premise solution") or in the cloud (hereinafter referred to as "cloud-based solution").

Based on the technological trends at the time, we adopted the on-premise solution of anti-malware software for BON/CPN that could be configured in detail. In this configuration, the connection between the BON/CPN and OTN was limited, so OTN PC terminals and the manager could not be connected, and the BON/CPN solution could not be deployed on the OTN.

On the other hand, many EDRs were originally designed as cloud-based solutions, and EDR adopted for BON/CPN was also cloud-based solution. In the case of cloud-based solutions, a common solution could be used in any environment as long as there was connectivity between the manager in the cloud and the PC terminal, so the same level of security measures could be deployed by extending the BON/CPN solution to OTN. The cost of the solution was also low because it required only a small increase in the number of licenses.

Although it was assumed that the requirements for security measures for OTN PC terminals managed by Tokyo 2020 Organising Committee would be different from those for BON/CPN PC terminals, in consideration of the above-mentioned restrictions on deployment, it was finally decided to expand the EDR solution for BON/CPN, to apply it to the OTN and to select the minimum necessary security measures to meet the requirements of OTN in addition to the EDR.

The difference between on-premise solution and cloud-based solution was also evident during the software upgrade process. The anti-malware software was operated for a long period of time from the early stages, including the preparation period of the Games, resulting in two version upgrades during the period of use. The on-premise environment required a large scale and long term project. In addition, it was necessary to re-distribute the agent software for the version upgrades, but the anti-malware software itself did not have an agent distribution function, resulting in a large workload. On the other hand, the EDR of cloud-based solution had a mechanism for easy distribution, so the workload for version upgrades was small.

In consideration of long-term use, it is inevitable that OS versions of PC terminals and servers must get upgraded, and the security solution itself will need to be upgraded to cover the new versions. The workload to upgrade such a solution should be one of the indicators to select a solution.

At that time, on-premise solution was adopted for anti-malware software, but since then technology has advanced and cloud-based solution has become a realistic option of solution. Considering cost advantages and the convenience of long-term use, including version upgrades, future Games will change to focus on cloud-based operational design.

5. Website Domain Security

Websites operated by the Organising Committee include not only official sites and ticket sales sites that are open to the public, but also many systems that are open only to specific users, such as games information distribution systems for the media. The composition of these systems varies widely, and security measures need to be implemented for each site individually. However, there are solutions that can be applied centrally to many of them, which can be very effective. This section introduces CDN as a typical example.

5.1 Content Delivery Network (CDN)

Web systems are very attractive targets for attackers and are frequently subjected to DDoS attacks intrusion attempts for data falsification and exploitation, and reconnaissance attacks as a preliminary step. Although each website is hardened in accordance with its security policy, it is necessary to have additional dedicated protection for large-scale attacks. The Organising Committee has decided to procure CDN to cover all public web systems of the Organising Committee.

CDN is a service that delivers content from a web server (origin) located in a data centre or cloud to end users from delivery servers (edges) distributed around the world. By delivering content from edges, which is closer to the end user, CDN improves the access speed to the website and reduces the load of the origin by aggregating a large number of accesses at the edge and accessing the origin only when necessary. It is also very useful for cyber attacks protection, as it reduces direct attacks by cloaking the origin, and attacks via edges can be handled in a decentralized manner at each edge.

We minimized damage of DDoS attack by CDN edge structure, while at the same time utilizing three filtering functions to block other attacks. The first is rule-based filtering which examines the contents of traffic and blocks them if unique characteristics, such as the inclusion of attack code, are contained. The second is rate-based filtering which blocks continuous access to generate heavy load on the origin such as intensive access to search pages. The third is reputation-based filtering which blocks access from blacklisted sources. The blacklist is created and maintained by the CDN provider with their own knowledge such as attacks for other websites. All of these filters were used in a block mode which immediately blocked malicious communications as soon as they were detected. In addition, since the origin cannot be fully concealed and can be directly targeted, all origin set their firewalls to deny all connections except the edges. In addition to the firewalls, scrubbing center-type services and DDoS mitigation options provided by cloud services are also used DDoS attacks that target the gateway network of the origins. By combining these measures, we constructed a defense infrastructure that can respond to a wide variety of attack methods.

However, these security measures were only a baseline. Each website adopted defense-in-depth design and implemented various of countermeasures depending on its configuration and characteristics. Although CDN is a very useful security measure, we should not be overconfident that they alone are sufficient.

5.2 DoS Simulation

Security measures are implemented in a defense-in-depth design, but it is also important to check whether they work together as expected and whether the expected protection effect is achieved.

Although the Organising Committee system undergoes sufficient functional and load tests prior to release, cyber attacks are very different from normal access in terms of both quality and quantity, so dedicated tests are needed to measure attack resistance. Penetration tests measure resistance to malicious communications such as injection attacks, in addition, other tests were conducted to measure resistance to the load of large accesses caused by DDoS attacks.

Specifically, we prepared an environment which generated the simulation of DDoS traffic, and checked whether each DDoS protections worked as expected for the generated traffic. Because this is only a simulation and the scale is limited to some extent, we call the test "DoS simulation" rather than a DDoS. However the test was well arranged so that it could cause a sufficient load by appropriately adjusting the system configuration during the test according. Because this test involved not only the security operation centre but also the data centre and cloud service provider where the CDN and origin servers were located, the target systems were limited to critical systems only. For example, there were cases in which security measures activated simultaneously interfered with each other and unexpectedly blocked legitimate connections, and cases in which the activation of protective functions was delayed beyond expectations. By optimizing the settings based on the knowledge obtained here, we were able to set up a state in which the expected defense effect could be achieved.

5.3 Notes on Shared Infrastructure

While 4.3 describes the advantages of cloud based solutions in terms of scalability, there are some points to note when many systems use a shared infrastructure, as in the case of cloud based solutions. These are described below.

The first issue is the authorization design. In a multi-tenant configuration where the infrastructure is shared by multiple systems, it is essential to separate the authorization so that the resources for each system can be freely accessed by its owner, while the others cannot be accessed. In the case of CDN, the management functions for filtering falls into this category. Fortunately, this was not a problem because the security function originally needed to be managed by the Cyber Security Team centrally and we could hide the management function for each system operators. The use of a shared infrastructure requires careful research on the specifications of authorization settings and elaborate authorization design tailored to the intended use.

The second issue is the impact of service failures. If the common infrastructure fails, many services will be affected simultaneously, resulting in extensive damage. Since the infrastructure itself will be large-scale, it will be difficult to prepare a secondary system equivalent to the current system and switch to them when primary system gets in trouble. It is necessary to select a service with sufficient stability, carefully prepare countermeasures in the event of failure, and build a system that can promptly coordinate information with infrastructure operators so that appropriate measures can be selected in a timely manner.

6. Conclusion

In the BON, CPN, OTN, and website domains, system hardening has been achieved through the implementation of MFA, the elimination of vulnerable configurations, configuration management, and vulnerability management. In addition, with the implementation of defense in depth and visualization solutions for each system, as well as continuous activities to prevent the obsolescence of solutions by version upgrades of them, we could have increased defenses and resulted in the completion of the Games without any major security incidents.

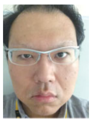
(Received February 28, 2022 ; Revised April 5, 2022)

TAMAI Kuniharu

TAMAI Kuniharu has engaged in providing solutions for corporations at NTT Communications Corporation and has been seconded to the Tokyo 2020 Organising Committee as the Project Director of Cyber Security Department, Technology Services Bureau since 2018. During the Games, he oversaw the operation of security solutions at the SOC.

NOJIRI Yasuhiro

NOJIRI Yasuhiro has been working for CSIRT start-up support and education at NEC Solution Innovators. He has been seconded to the Tokyo 2020 Organising Committee as security solutions manager since 2019 in the Cyber Security Department of the Technology Services Bureau. During the Games, he oversaw the operation of security solutions at the SOC.



HOSODA Naofumi

HOSODA Naofumi has been working for ISP backbone operation and analysis of cyber threats at NTT Communications Corporation. He was seconded to the Tokyo 2020 Organising Committee as Security Operations Manager of the Cyber Security Department, Technology Services Bureau since 2014. During the Games, he was in charge of web security operations at the SOC.

IBAYASHI Hiroaki

IBAYASHI Hiroaki has been working in the service development of cloud and security businesses at NTT Communications Corporation since 2014, and has been seconded to the Tokyo 2020 Organising Committee as the Director of Cyber Security Department, Technology Services Bureau. During the Games, he was responsible for the overall security operations in the SOC.