OPERATIONALISING MINDEF BUG BOUNTY PROGRAMME

CHIAM Tze Wei Raymond, SOH Yiyong

ABSTRACT

In January 2018, the Ministry of Defence (MINDEF) organised a Bug Bounty Programme (BBP) to harness collective intelligence and capabilities of top hackers to uncover underlying security vulnerabilities within MINDEF's systems. Because of the criticality of the systems and the calibre of the hackers invited, the BBP represented considerable risk as it attracted attention and increased hacking attempts from top hackers, both ethical and malicious, all over the world on MINDEF's operational systems and infrastructure.

This article outlines the motivation behind running a BBP, the challenges in ensuring swift validation, impact assessment, mitigation and remediation of the vulnerabilities found and how a cross-departmental Technical Operations Centre was set up to overcome these challenges.

Keywords: MINDEF bug bounty programme, hacker, cyber defence, cybersecurity

INTRODUCTION

The Ministry of Defence (MINDEF) and the Singapore Armed Forces (SAF) engage National Service (NS) men and the public for administration, recruitment and outreach through the NS Portal, MINDEF/SAF Internet website and supplementary portals. MINDEF and SAF personnel also rely on these systems and the Defence Mail for administration and communication. To protect these systems from cyber threats, robust vulnerability[1] assessments are conducted before every system deployment and thereafter regularly. Systems traffic and performance are monitored and contingency measures to respond to cybersecurity incidents have been established.

Despite these best practices, absolute security is not possible because of the constant trade-offs between cost, usability and the continuous evolution of technology. In order to enhance the security of these systems, in particular Internet-facing ones, DSTA formed a working group to explore several options including conducting a Bug Bounty Programme (BBP). After considering various options, the working group recommended conducting a BBP.

MOTIVATIONS BEHIND THE BBP

The BBP allowed MINDEF to supplement its existing robust vulnerability assessments with the industry best practice of crowd-sourcing and harnessing the collective capabilities of top white-hat[2] hackers. The three-week programme, which was facilitated by HackerOne (one of the world's leading white-hat hackers security platforms), invited 300 white-hats from around the world to test MINDEF's internet-facing systems. Two hundred of these invited white-hats were among the highest ranking professional bug bounty hackers world-wide, possessing sophisticated network, hardware and application hacking skills. The remaining 100 were hackers from Singapore, who were more familiar with the systems and had accounts to access more functions within the systems. The programme aimed to harness the collective intelligence and capabilities of these top white-hats to uncover deep-lying security vulnerabilities within MINDEF's systems.

CHALLENGES OF THE BBP AND OVERCOMING THEM

Preparing Critical Systems within a Short Period of Time

In order to show commitment to the BBP, MINDEF opened up not only its static websites but also its transactional and operational systems. Eight major systems, including a total of 36 e-services and applications, were tested during the programme. These systems included the medical system, communication (web mail) system and systems that support MINDEF's NS men in performing administrative tasks such as the booking of physical fitness tests, leave application and online self-learning. Refer to Figure 1 for a breakdown of the applications involved in the BBP.

Due to the criticality of the systems and the calibre of the hackers invited, the BBP represented considerable risk as it attracted attention and increased hacking attempts from top hackers, both ethical and malicious, all over the world on MINDEF's operational systems and infrastructure. The increase in network traffic could potentially affect these systems' availability. There was also risk of the participating hackers attempting to exploit the discovered vulnerabilities or publishing them online. Any exploitation of vulnerabilities found could result in data exfiltration and data corruption, which would affect business continuity and lead to loss of public confidence in MINDEF.

There was only about three months between the conceptualisation and start date of the programme to take measures for mitigating the risks and minimising the potential impact. A cross-departmental working group comprising Subject Matter Experts (SME) from various disciplines – software application development, cybersecurity, network infrastructure and database administration was formed to plan and coordinate pre-BBP activities across the different departments. The working group reviewed the security posture of the systems and servers, developed the processes and set up the necessary infrastructure to support the programme.

The 36 applications were scanned for vulnerabilities on top of the security checks performed regularly. Servers hosting the applications were checked for conformance to prescribed hardening and patching processes. Web application firewalls and intrusion prevention systems were checked for proper configurations and system administrator accounts were taken stock of. Systems traffic and performance were also monitored and contingency measures to respond to cybersecurity incidents were reviewed for adequacy.

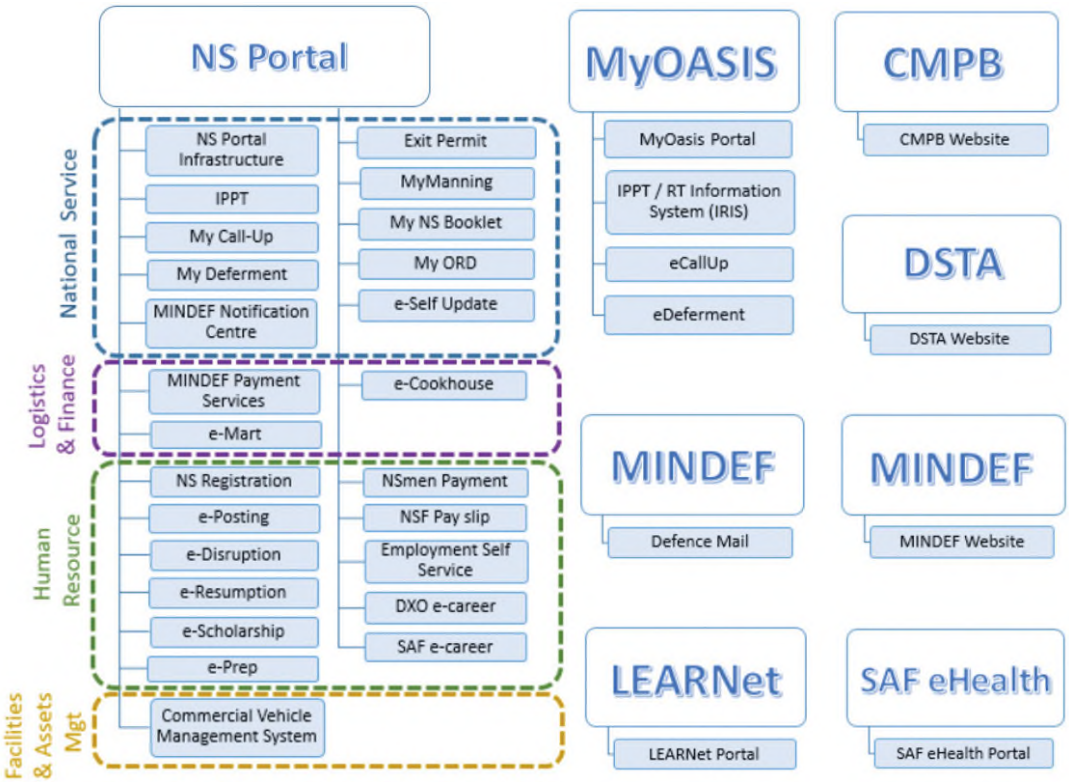

Figure 1. Breakdown of the systems involved in the BBP

Operationalising the BBP

During the BBP, the working group then transformed into a Technical Operations Centre (TOC) to run the BBP smoothly as well as to manage communication to the public, MINDEF principals and other stakeholders. The TOC ensured any detection, validation, assessment and remediation of vulnerabilities was well coordinated and performed swiftly. During and after the programme, the TOC also conducted extensive checks to ensure the data integrity of the systems was not compromised. Figure 2 shows the structure of the TOC. The TOC comprised three teams – triage, remediation and reporting.

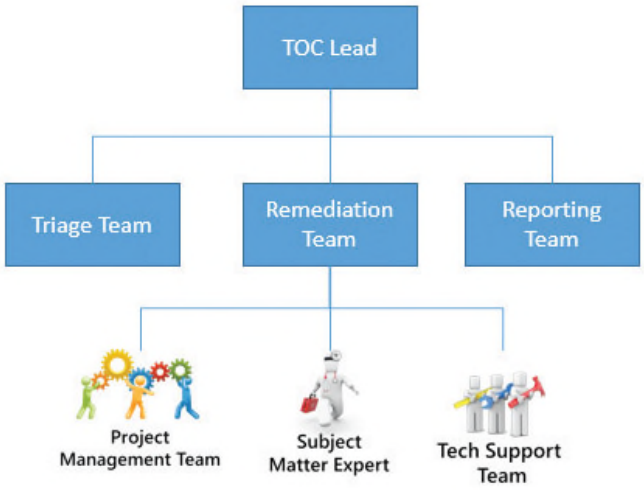

Figure 2. Structure of the TOC

TOC Lead

The TOC was led by Director (Technology), Enterprise IT.

Triage

The triage team was made up of the cybersecurity SMEs. This team was responsible for validating the bug submissions, assessing their severity and determining the root causes of the bugs. Details of the triage team would be elaborated in later sections.

Remediation

The remediation team was made up of software development and cybersecurity SMEs. The software development SMEs were responsible for looking into the details of the bugs and recommending potential solutions to project management teams (PMT) and system vendors to contain, mitigate and/or remediate the bugs. After the solutions have been deployed in the staging environment, the cybersecurity SMEs were responsible for verifying that they were adequate and provide residual risk assessments based on the solutions performed. The bug remediation details and residual risk assessments would then be submitted to the TOC Lead for approval before deployment to the production environment. The cybersecurity SMEs were also responsible for verifying that the bugs were successfully mitigated or remediated after production deployment.

Reporting

The reporting team was made up of software development and cybersecurity SMEs. This team was responsible for tracking, consolidating and reporting the classification of bugs by severity levels, validation statuses and their remediation statuses on a daily basis to MINDEF principals and DSTA management. This team was also responsible for informing MINDEF of scheduled system maintenance downtime.

See Figure 3 for an overview of the TOC process.

Managing Business Operations and Controlling Changes

Many of the system applications were undergoing planned upgrades, architectural changes and migration to new data centres. This posed challenges in balancing between the scheduled upgrades and maintaining the stability and security posture of the systems that would be opened up for the BBP because changes to the applications risk introducing new vulnerabilities inadvertently.

In order to prevent uncontrolled changes to the systems, the TOC defined a change control process, where a Change Control Management Board (CCMB) maintained oversight over all change requests during the BBP to balance BBP risks and business operational requirements optimally. Every change request being put up by the business users had to be assessed for its urgency and its impact to the security posture of the respective system. Details of the software code change had to be scrutinised and potential vulnerabilities needed to be mitigated. Any residual risk of each change would be assessed and either approved at the CCMB level, or for bugs of higher severity, escalated to the appropriate forum for deliberation before further action was taken.

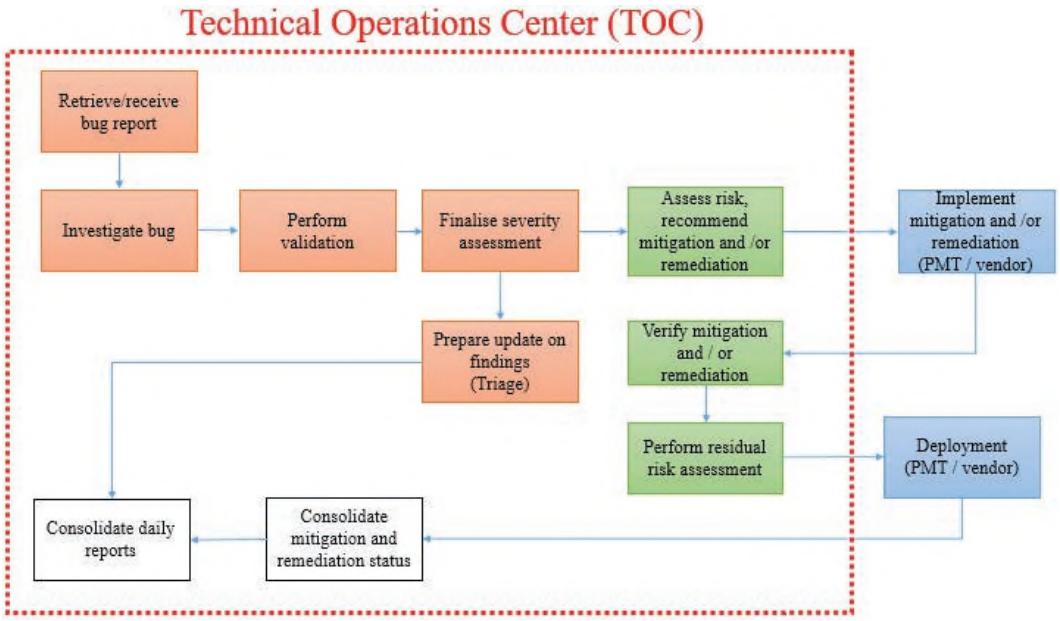

Figure 3. Overview of the TOC process

The baselined versions of the system software codes used in the BBP needed to be stored and backed up for safe-keeping before and during the BBP. To facilitate this, the TOC set up the infrastructure to host a central code repository. The change control process was also set up to ensure that software changes resulting from change requests or remediation of vulnerabilities found during the BBP were required to be scrutinised by the remediation team and checked into the code repository. The code repository also served a secondary purpose of facilitating faster access to the software code of all the BBP systems, which enabled the SMEs within the TOC to expedite vulnerability and risk assessments.

To facilitate the deployment of software code changes, the BBP systems had to be shut down for up to several hours at a time. To determine the optimal downtime, the TOC had to manage several contending factors and stakeholders including the duration for systems patching, the accessibility of the systems by NSmen, and expectations of business users and the white-hats participating in the programme.

Managing High Volume of Bug Submission

Given the large number of systems and applications participating in the BBP and the calibre of the white-hats invited, the TOC had to prepare for a high volume of bug reports that may be submitted. Should such a scenario take place, it would severely stretch triage and rectification engineering resources simply to assess and verify the reports, and then to a greater extent when remediation is required. The same resource would also be involved in the maintaining of operational readiness of the systems, thereby exacerbating the situation even further. SMEs with a variety of skill sets ranging from network to cybersecurity to database and software architecture were pulled in to assess the bugs found and to develop mitigation and remediation measures.

An operations centre was set up at DSTA Integrated Complex to accommodate the triage, remediation and reporting teams in close proximity to facilitate faster coordination, execution, resource utilisation and discussion. MINDEF's network is segregated into various segments due to operational and security constraints. In order for the TOC to function swiftly during the BBP, a network infrastructure was set up so that the triage and remediation teams had access to the central code repository and the different networks hosting the Quality Assurance and production environments of each system as well as communicate with MINDEF counterparts.

To be prepared for a high volume of bug submissions, there was a need to track all the information about the bugs – such as their assessment, rectification status, methods of rectification, and expected resolution date. The tracking of information was necessary for its timely dissemination internally within the TOC between the triage and remediation teams. The information was also necessary for the reporting team to communicate externally with the MINDEF principals, HackerOne, PMT and systems vendors.

The lifecycle stages of each bug took place in three different networks – Internet, DSTA internal network and the MINDEF network – due to operational and security reasons. The TOC improvised a bug management workflow using existing intranet tools to manage and share updated information of each bug among the different teams and stakeholders. See Figure 4 for the lifecycle of a typical bug.

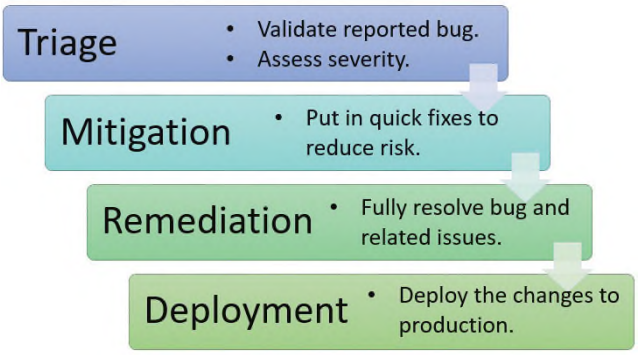

Figure 4. Lifecycle of a typical bug

Triaging the Bug Submissions

To ensure swift response to the expected high volume of bug submissions, the TOC incorporated a triage team. This team was led by experienced vulnerability analysis SMEs, with support from software/network architects and system developers in the TOC. This triage team focused on achieving four objectives:

1. **Validation of Bug Submissions** – Validation of bugs was required to ensure that submissions were credible. From experience, not all bug submissions were valid, even if the white-hats have given them high severity ratings. This key step helped the TOC to triage and prioritise the team's effort in remediation.

   The approach to validate bug submissions varied. It was a common misconception that all bug submissions could be validated by simply replaying the steps provided by the white-hats. However, this was not always possible due to many factors such as different privileges and accounts used. In these cases, the triage team would employ other techniques such as testing on staging, debugging and source code reviews to establish the validity of the submission. A total of 97 bug submissions were triaged and 62 of those were found to be invalid.

2. **Assessment of Bug Severity** – Accurate severity assessment of the validated bug was key to the overall TOC response. This helped to prioritise engineering resources for higher risk areas. To ensure consistency, the team established a common understanding of reporting and measuring severity based on factors including attack vector, attack complexity, privileges required, user interaction, scope, confidentiality, integrity and availability with service provider and white-hats. These factors contributed to the assessment on the likelihood and impact of the reported bugs. This approach provided an effective means to provide feedback especially in cases where the white-hats had over-rated their own severity assessment.

3. **Determination of Root Cause of Vulnerability** – The team anticipated scenarios where reported bugs could pose an immediate threat to their Internet-facing systems. One of the key goals of the triage team was also to establish the root cause of the reported vulnerabilities (e.g. insecure coding practices, commercial off-the-shelf or previously unknown vulnerabilities, etc.) by performing sufficient vulnerability analysis of the validated bug. This additional step proved to be very effective in terms of managing risk as it provided detailed information that was required by the mitigation and remediation teams for swift follow-up. When necessary, the triage team would also explore alternatives on how a reported vulnerability could be further exploited in real world conditions. This was required as it provided a more thorough understanding of the reported vulnerability beyond the scenarios provided by the white-hats. With deeper insights into the vulnerability and conditions that could trigger it, the remediation team had more technical options that could be considered for mitigation.

4. **Support Service Provider** – HackerOne, the service provider, performed initial assessments based on the bug reports submitted. These gave the team initial insights when the bugs were first submitted. However, there were many cases in which the service provider was not able to perform these initial assessments. This could be due to lack of account privileges, etc. for the service providers. In these cases, the service provider would alert the triage team to take over the assessment promptly.

OUTCOME AND LEARNING POINTS OF THE BBP

Costs and Benefits of the BBP

The BBP brought about a review that helped to further strengthen the security posture of the systems by identifying areas for improvement in their delivery. From an operations perspective, the BBP allowed vulnerabilities to be uncovered, which could otherwise not have been detected with conventional penetration testing in the development and Quality Assurance environments.

In addition, these benefits came only at a small fraction of the cost of engaging a cybersecurity consultancy firm to perform a cybersecurity assessment, which would have amounted to a million dollars. Furthermore, the TOC team managed to operationalise the ops centre with existing tools and infrastructure without incurring much cost.

Tight Integration of a Multi-disciplinary TOC

The organisation of the TOC and having SMEs from various teams located in close proximity stood out as important parts in managing the BBP. The result of that arrangement was close discussion, quick assessment and remediation of the bugs, especially the high risk ones which were remediated within 24 hours, providing testament to the benefits of a tightly integrated TOC. Equally important was the close working relationship between the triage and remediation teams prior to the BBP. The teams had experience working with one another and trusted their co-workers' professionalism and level of competency.

Forming a multi-disciplinary TOC comprising SMEs from the domains of cybersecurity, network infrastructure, application development, software architecture and database administration provided the crucial engineering knowledge necessary for the quick resolution of the bugs.

Inflation of Vulnerability Severity

One learning point from the BBP was the tendency of white-hats to "inflate" the severity of the bugs in their submissions. This could be attributed to their desire to receive a higher bounty as well as having their submitted reports given higher priority when being processed. About 60% of the submissions from the white-hats were eventually invalidated by the triage team and majority of them also reassessed to lower severity.

The inflation of bugs' severity, however, did pose some problems for the TOC as bugs with higher severity naturally generated more concerns and expectations from system owners. The TOC had to manage these concerns and expectations in order for the due triage and assessment processes to take place.

The TOC's approach proved to be effective in handling bug submissions and ultimately ensured that the overall security posture of the systems was not elevated during the conduct of the bug bounty exercise.

Compounding Relationship of Bugs

Another learning point from the BBP was how two low severity bugs affected and compounded with each other to form a bug of high severity. This incident epitomised the unpredictability of cybersecurity domains, where real life situations can sometimes go against conventional paradigms and beliefs.

Programme of Conflicting Goals

The BBP was an interesting programme in that there were conflicting goals. On one hand, providing less obstructions for the white-hats to access the systems would have yielded many more vulnerability submissions, constituting a successful programme for MINDEF. However on the other hand, such a scenario would have posed challenges to DSTA's resources, which, besides supporting BBP, would still be needed to support the ongoing operation of the systems. In addition, this would also not be an accurate measure of the true cyber defence capabilities of the systems as every level of obstruction placed between the hackers and the systems had its place in the collective defence of the system.

Such conflicts were also evident in the scheduling of system downtime for patching purposes. On one hand, business users would prefer to shut down the systems as soon as possible and during non-peak usage hours. On the other hand, white-hats would prefer systems to remain operational especially during non-peak hours, as white-hats generally performed their testing after office hours.

CONCLUSION

The MINDEF BBP symbolised MINDEF's shift towards embracing a new cybersecurity paradigm, with MINDEF collaborating with the white-hat hacker community to uncover security vulnerabilities quickly and more efficiently before malicious hackers do. The BBP received a total of 97 vulnerability reports, of which 35 were assessed to be valid security vulnerabilities. Finding and rectifying these vulnerabilities improved the security posture of MINDEF's internet-facing applications within a short span of three weeks.

The programme has provided benefits in finding vulnerabilities in an unconventional manner but also presented many challenges. To support the programme, DSTA operationalised the BBP in the form of a TOC to ensure all related systems were ready for the programme, formulated new processes and formed cross-departmental teams to ensure any detection, validation, assessment and remediation of vulnerabilities was well coordinated and performed swiftly. The manner in which the cross-department, multi-disciplinary engineering teams worked together proved crucial to the success of the BBP and provided a roadmap to hosting similar programmes in future.

Following the successful MINDEF BBP, the Government Technology Agency of Singapore and Cyber Security Agency of Singapore also held a government bug bounty programme from 27 December 2018 to 16 January 2019 to improve the security posture of five government systems.

ACKNOWLEDGEMENTS

The authors would like to thank Mr Gabriel Tang, Mr Lim Swee Kay and Mr Henry Wong for their help in reviewing and editing the article.

REFERENCES

Kuehn, A. (2014, August). *New paradigms in securing software vulnerabilities – an institutional analysis of emerging bug bounty programs and their implications for cybersecurity*. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2809862

MINDEF Singapore. (2018, February). *Fact sheet: Ministry of Defence (MINDEF) bug bounty programme 2018 results*. Retrieved from https://www.mindef.gov.sg/web/portal/mindef/news-and-events/latest-releases/article-detail/2018/february/21feb18_fs

Perlroth, N. (2015, June 7). HackerOne connects hackers with companies, and hopes for a win-win. *The New York Times.* Retrieved from https://www.nytimes.com/2015/06/08/technology/hackerone-connects-hackers-with-companies-and-hopes-for-a-win-win.html?_r=0

ENDNOTES

[1] A software vulnerability is a security flaw or weakness found in software or in an operating system that can be exploited to cause unintended behaviour.

[2] A White-hat or White-hat hacker is an individual who uses hacking skills to identify security vulnerabilities in hardware, software or networks while respecting the rules or laws that apply to hacking.

BIOGRAPHY

CHIAM Tze Wei Raymond is a Principal Engineer (Enterprise IT). He is a key member of a team responsible for improving the security posture of the enterprise IT applications through process improvements in the software development lifecycle. He is also a certified Project Management Professional from Project Management Institute, a Certified Software Quality Analyst from Quality Assurance Institute and a Certified Tester Advanced Level – Technical Test Analyst from International Software Testing Qualifications Board. Raymond graduated with a Bachelor of Computer Science degree from the University of Western Australia in 2002.

SOH Yiyong is a Development Programme Manager (Cybersecurity). He leads in the analysis of vulnerabilities that impact MINDEF and the SAF's systems, builds mitigations against them and transits Research and Technology prototypes to a cyber-solution. Yiyong graduated with a Bachelor of Engineering (Computer Engineering) degree with Honours from the National University of Singapore in 2011.