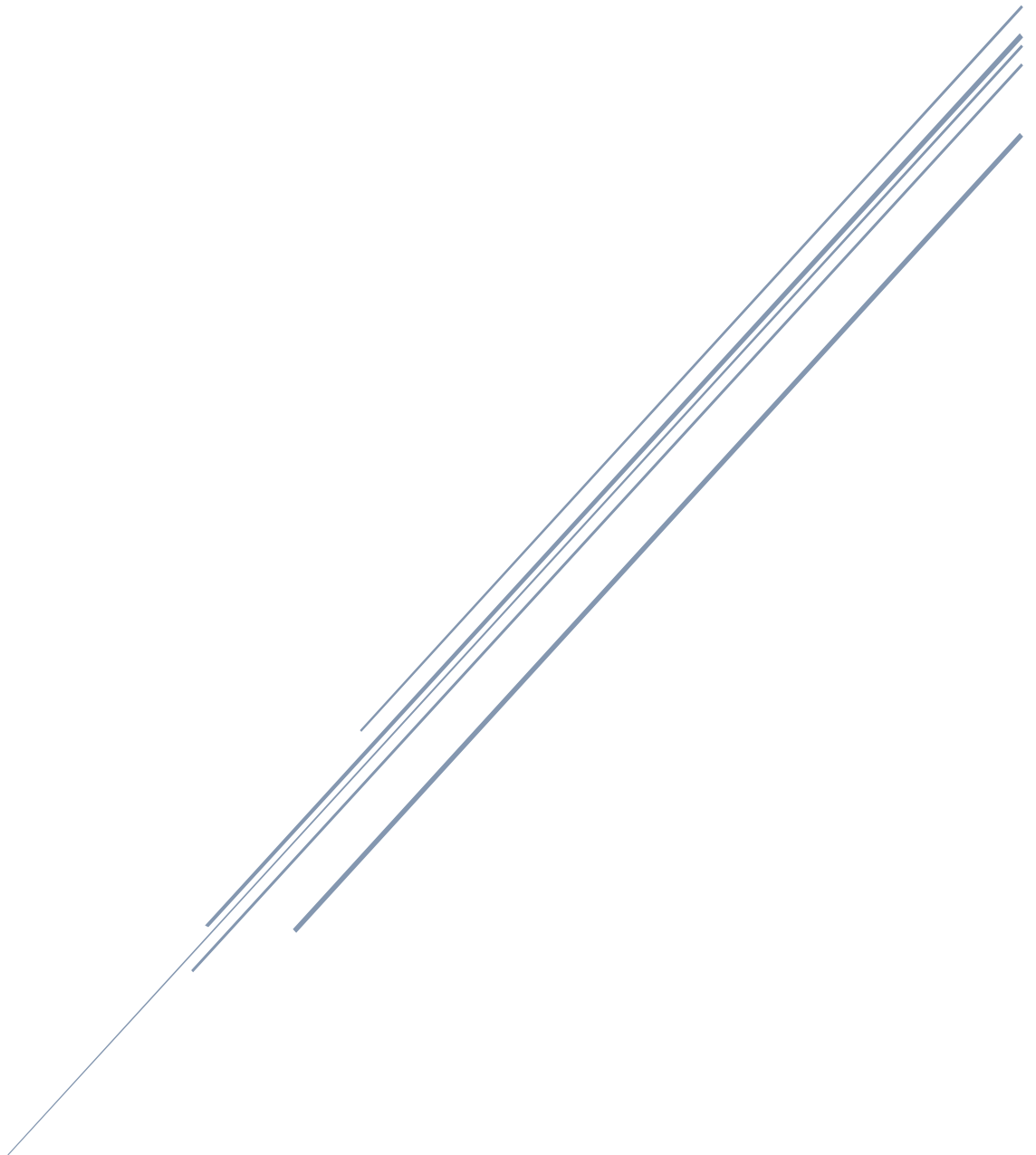


BLUE TEAM – CYBER SECURITY

ACCB6000 - Computer Networks & Cyber Security



Che Morris - 2203458
Networks & Cyber Security

Table of Contents

<i>Introduction</i>	2
<i>Challenges</i>	2
<i>Advancements</i>	3
<i>How have these methods worked in the past?</i>	4
<i>Conclusion</i>	4

Introduction

Within modern cybersecurity, blue team operations play a crucial part in helping to defend organisations against evolving cyber threats. They are the main way threats are detected, mitigated and responded to which helps ensure that data within organisations remains confidential and secure. Blue team is quite a wide term, they have many different areas where they focus such as threat detection and response, threat hunting, cloud security and information and event management.

This report will discuss the challenges and advancements within two focus areas, these being threat hunting and threat detection and response, focusing on how things are currently being done and the tools and strategies used. The aim will also be to evaluate the effectiveness and limitations within these areas.

Challenges

Cybersecurity is a rapidly changing and growing atmosphere, with this the challenges faced are always changing. One of the main challenges that has been ever present is that there is just overwhelming demand to keep up with security alerts and notifications that need to be investigated. A study in 2017 that completed a survey with 150 cybersecurity professionals found that keeping up to date with security alerts was the biggest challenges they faced with 43% of them saying they ignore more than 25% of them just to keep up [1]. This may be a huge factor in why we see so many data breaches and such these days, whether it's down to lack of staff or lack of time, it's a huge risk. Another contributing factor to this is that in the same study, 29% of respondents thought that the security tools they use are not well integrated or outdated [1]. As threats in the modern day are always evolving, so the tools should be alongside them otherwise that race will be consistently lost.

Focusing more on threat hunting, as it's a relatively new field, the skill gap is hard to work with. A study on the threat hunting team associated with the US Department of Homeland Security found that they all had the same common problem, judging a potential threat hunters' expertise [2]. This wouldn't usually be an issue but it's apparently also common for people in this field to change job "every two years" [2]. This gives threat hunters the upper hand as it will take time for them to get used to the new job & it seems to take a while for them to find people in the first place. Threat hunting suffers from mostly everything being done by humans; there's little automation in threat hunting [2], which becomes a challenge due to things being slower, yes more accurate, but with how rapid cybersecurity changes, it doesn't really fit.

Advancements

The use of artificial intelligence and machine learning has become prevalent within threat detection & response as one of the most important tools that they use now. AI is now used within cyber security for various things and tends to be heavily relied upon. One of the main things it's used for is threat and anomaly detection where it's used for "enabling real-time identification of potential risks and deviations from normal behaviour" [3]. This addition allows for employees within organisations to quickly jump on threats and handle them accordingly, where sometimes without the AI this could have been missed and could have had devastating consequences. AI has also "significantly enhanced security monitoring and incident response capabilities" [3], these can come in significantly handy for threat detection and response as AI can help in modifying and creating ways of dealing with threats without humans even being involved in the process at all.

Focusing more on advancements with machine learning, advancements have been made there about real time threat detection also. Machine learning has now become integrated with general threat intelligence, by this it is now "leveraging external threat intelligence feeds and integrating them with internal ML systems allows organizations to enhance their situational awareness and improve detection accuracy" [4]. The integration of machine learning with threat intelligence will have significantly enhanced how threats are detected and allow for the significant increase in general threat detection and can also allow for the identification of future emerging threats & patterns.

Advancements in threat hunting are few and far between due to it being quite a newer thing, these mostly come in new methodologies by people within the cyber security space but are still quite interesting to review. A methodology created by cybersecurity leaders CrowdStrike is based on that threat actors may already be within the system [5] which I guess you could say is like how a traditional antivirus would work, but it has proven to be effective within the space and is quite efficient with detecting and eliminating anomalies.

How have these methods worked in the past?

If you focus on the WannaCry ransomware attacks from back in 2017, taking everything into account you can now see where things did go wrong and how things could have been prevented if they had been properly thought through. The attack worked by utilising a known vulnerability at the time with Windows machines that had already been patched by Microsoft.

A combination of organisations failing to keep their machines up to date & the fact that there was a severe lack of effective intrusion detection at the time lead to organisations like the NHS falling victim to the attack. Whether this was because of the sheer scale of the attacks or due to incompetence, this weighs in with both things that were mentioned above, there's so many security alerts that show up that some do tend to get skipped, so maybe that was the case here & some people within the industry believe that the tools are not adequate enough which clearly they weren't for this attack that things really needed to evolve. They have evolved since but WannaCry did come out of nowhere so it shows that innovation is key and needs to continue as something could do the same as WannaCry did.

Conclusion

Blue team operations, especially within threat detection and response, play such a crucial part within protecting organisations and protecting our personal data. Whilst it will never be a perfect industry, as discussed it will always have its challenges, innovations like machine learning and AI have shown to be extremely promising advancements and allow for threat detection to be perhaps the best it's ever been. As we've seen from previous incidents though, like the WannaCry ransomware, the evolution of cybersecurity will always be in that race with the evolution of newer threats and trends, and it will always have to do its best to keep up. The advancements like AI and machine learning will be integral for the future and will be crucial to closing those gaps and ensuring blue teams are equipped with everything they need to protect organisations in the modern world.

References

- [1] Jon Oltsik, "2017: Security Operations Challenges, Priorities, and Strategies," Mar 2017. Available: <http://pages.siemplify.co/rs/182-SXA-457/images/ESG-Research-Report.pdf>
- [2] William P. Maxam III and James C. Davis, "An Interview Study on Third-Party Cyber Threat Hunting Processes in the U.S. Department of Homeland Security," Feb 19 2024. Available: <https://arxiv.org/abs/2402.12252>
- [3] N. T. M. Huyen and T. Q. Bao, "Advancements in AI-Driven Cybersecurity and Comprehensive Threat Detection and Response," *Journal of Intelligent Connectivity and Emerging Technologies*, vol. 9, no. 1, pp.1–12, 2024.
- [4] Siva Subrahmanyam Balantrapu, "Current Trends and Future Directions Exploring Machine Learning Techniques for Cyber Threat Detection," Oct 23 2024. Available: <https://ijsdai.com/index.php/IJSDAI/article/view/72>
- [5] A. Mahboubi, et al., "Evolving techniques in cyber threat hunting: A systematic review," *Journal of Network and Computer Applications*, vol. 232, pp.104004, 2024. doi: 10.1016/j.jnca.2024.104004. Available: <https://www.sciencedirect.com/science/article/pii/S1084804524001814>