Comparison of cybersecurity protections for a small business

To what extent is outsourcing a Security Operation Centre more effective than social engineering training for small businesses in Queensland, Australia?

Digital Society Extended Essay

Word count: 3468

Introduction

As technology improves, the cybersecurity space becomes more complicated and chaotic, and each year more businesses are victims of cyberattacks (Australian Signals Directorate, 2023). Cyberattacks often have a large impact across many contexts such as physical, economic, psychological, and reputational (Agrafiotis et al., 2018). Economic effects include reduced profits, loss of jobs, and costs of investigations. Needless to say, it is often detrimental to any business to experience a cyberattack. Whilst large businesses are a bigger target for attackers, small businesses are also at risk because they have less funds, connections, and experience. Approximately one half of small businesses in Australia allocate less than $500 for cybersecurity, which compared to large businesses is miniscule (Tam et al., 2021). Recently my father hired a consultant to improve the cybersecurity profile of his business for approximately $4000. The consultant implemented Sophos MDR, a type of a Managed Detection and Response system (MDR), among other protections but did not do any training with the employees of the business. I initially thought that this was the wrong decision as it would help prevent social engineering, which is one of the methods most commonly used for cyberattacks. It involves manipulating people into trusting and helping an attacker, and even in large companies, employees still fall for it which is why I thought the consultant should have done atleast some training against it. Sophos MDR also seemed overpriced and unnecessary, but I realised that implementing it might be much easier and effective than training the employees.

This brings me to my research question: “To what extent is outsourcing a Security Operation Centre more effective than social engineering training for a small business?”. A Security Operation Centre (SOC) is a similar term to an MDR system but is more commonly used so I chose it instead. In this essay I hope to analyse the benefits and challenges of both protections in the context of small businesses and outsourcing as a form of investigation into how the consultant improved my father’s business. I will assume that the small business can only implement one of these options as it is too expensive or time consuming to implement both, but they have implemented other protections such as email filters.

Methodology

Firstly, some preliminary secondary research was conducted in order to prepare some questions for the cybersecurity consultant. A variety of sources such as academic articles, statistical reports, and blog posts from reputable companies were used to gather both quantitative data and qualitative real life examples. Then, some questions were written for the consultant about the consultation itself but also some about cybersecurity in general. This helped narrow down the scope and aim of the inquiry from evaluating the use of a SOC to comparing it to the implementation of social engineering training, since he said in his responses that he had not done any training (see Appendix C).

This primary research was beneficial because the consultation is a real world example of using a SOC and the impacts on stakeholders are clear. The goal of it was to better understand the consultant’s reasoning and perspective behind not conducting any training. Afterwards, some more secondary research was done and was followed by an interview with an IT employee from a large security company. This interview was done because the company is very experienced with both a SOC and social engineering training (see Appendix A). It also specialises in security and the employee would likely have seen instances where these protections have failed as he works closely with people that manage them. The aim of the interview was to investigate how a company would use both protections in the long term, and also to see how this might be different for a large company to a small one. Finally, I also sent some questions to an IT employee at my high school with the hope that it would either corroborate or contradict these other sources in relation to both a SOC and cybersecurity in general (see Appendix B).

Background information

SIEM and SOC

A SOC is similar to several other security products such as a Security Information and Event Management system (SIEM). A SIEM is a tool that analyses all events in an organisation’s technology infrastructure for malicious activity (Pinson-Roxburgh, 2023). Events can come from a wide variety of sources including applications, network devices, and databases, such as a firewall allowing data into the network, or Command Prompt running a command (see Appendix C). One use of a SIEM is to comply with regulations that require businesses to store logs of operations for a prolonged period of time, so that in the case of a breach authorities could conduct a proper investigation. A SIEM can also detect unusual behaviour such as if an account were logged into from a vastly different location to the usual one (Teodor, 2022). It would then notify the business so that they can then decide if it is malicious and prepare for the impending cyberattack. Finally, a SIEM can also recognise when an attack has been successful, such as an attacker reading an enormous amount of data from a database.

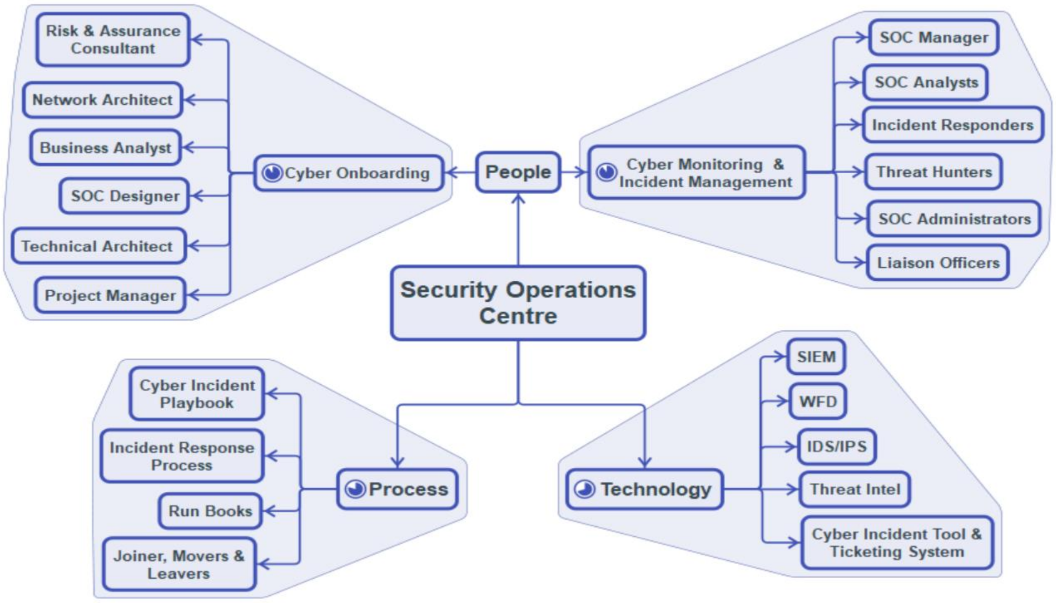


Figure 1. The components of a SOC (Onwubiko & Ouazzane, 2019)

A SOC is the combination of People, Processes, and Technology as shown in Figure 1, and is much more sophisticated than a SIEM. A SIEM is simply a tool, whereas a SOC is a team of experts that use several technologies including a SIEM to detect malicious activity and notify the relevant people (Orange Cyberdefense, 2023). These people could include the owners of the business, legal authorities, or victims of the attack. However, they would only focus on the detection of attacks and not the response or protection from attacks. A SOC is often outsourced to a company such as Sophos (Sophos, 2024), which was done in my father’s case.

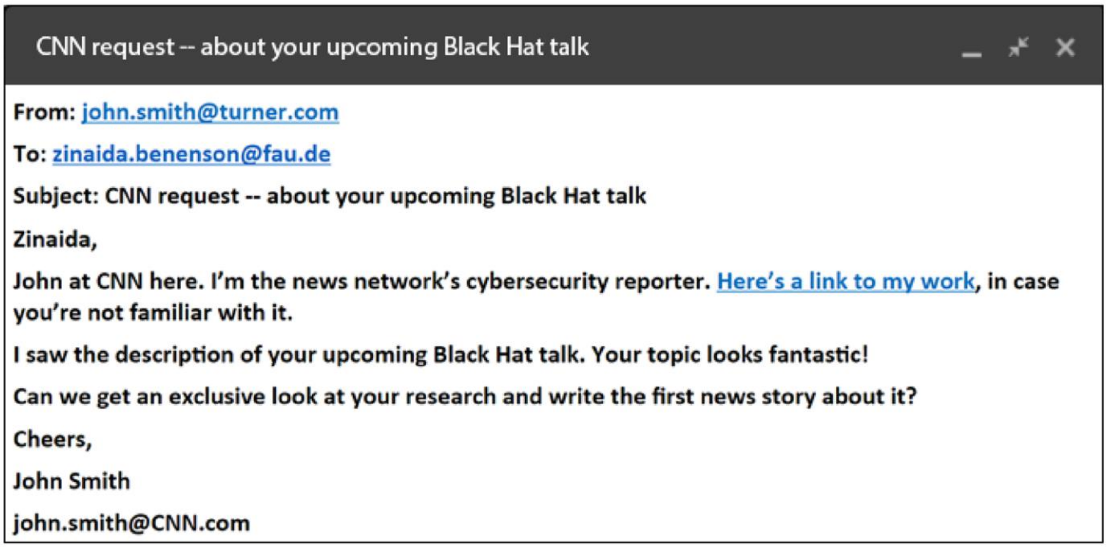
MDR system

Whereas an MDR system is an extension of a SOC that does deal with the response to attacks (Pinson-Roxburgh, 2023). This would involve attempting to contain the attack, and directly investigating it after it has happened.

Social engineering

Social engineering refers to manipulating victims with digital tools into divulging information or doing inappropriate actions (Graphus, n.d.). These digital tools can be email, websites, or many other forms of digital media. Phishing is a form of social engineering where an attacker contacts a large number of victims simultaneously, usually through email (*Phishing, Technique T1566 - Enterprise | MITRE ATT&CK®*, n.d.). Attacks are usually performed by encouraging victims to open a malicious link which executes malicious code on the victim's device or impersonates a legitimate website and stores their account's details when they try to login. However, attackers also sometimes attempt to start a conversation with the victim to manipulate them into giving money or other acts. Phishing was by far the most used initial access method in cyberattacks during 2022 and 2023 (Iacono et al., 2023). This is because the victim often does not realise that they did anything wrong until long after the attacker has exploited them, and people are often the weakest link in a business' security profile.

Spear-phishing is a form of phishing where the attacker targets a single victim and does research on them in order to launch a specialised attack (Graphus, n.d.). It can require significantly more effort than a regular phishing attack but is also more likely to be successful as the attack can seem more believable and urgent to the victim. Figure 2 is an example of a spear-phishing attack where the attacker has done some research on the target and disguised a link to a malicious website as a link to their work. Spear-phishing could be used by attackers to build a relationship with an employee of a business and then coerce them into divulging information or providing control over some of the business.


CNN request -- about your upcoming Black Hat talk

From: john.smith@turner.com

To: zinaida.benenson@fau.de

Subject: CNN request -- about your upcoming Black Hat talk

Zinaida,

John at CNN here. I'm the news network's cybersecurity reporter. Here's a link to my work, in case you're not familiar with it.

I saw the description of your upcoming Black Hat talk. Your topic looks fantastic!

Can we get an exclusive look at your research and write the first news story about it?

Cheers,

John Smith

john.smith@CNN.com

Figure 2. Example of a spear-phishing attack (Jampen et al., 2020)

Social engineering training

In the context of this inquiry, social engineering training refers to both teaching employees of a business about social engineering and simulated campaigns that involves social engineering. For example, the company IT employee stated that the company ran a simulated social engineering campaign where real employees were sent phishing emails which lead to a website that recorded that they clicked the link (see Appendix A). A small business would likely outsource this training to a professional third party, similarly to how they would outsource a SOC. The aim of the training would be to not only to reduce the chance of an employee being fooled by a social engineering attack but also to teach them what to do if a cyberattack has occurred.

Discussion of findings

Change

One advantage of a SOC is that it is immediately applied to the entire company (see Appendix A), whereas the training would only apply to the people that the business has trained. However, this would not be very impactful for a small business as there are fewer people to train. Although, the business would need to repeat the training after a while as employees would become complacent or less aware of social engineering techniques (Juroeayvant, 2023). Attackers are also constantly creating new techniques so employees might not know how to deal with them (Iacono et al., 2023). For example, an emerging phishing technique is AI generated voice calls, which is more sophisticated than current techniques since the AI would be able to hold a lengthy conversation with the victim. The AI would then manipulate them into helping the attacker such as by printing a large amount of customer data. A well-made SIEM would be able to flag this as an odd behaviour and could alert the victim’s superior because whilst the attacker is using a new phishing technique, the method of data exfiltration is not new and that is what the SIEM is analysing (Teodor, 2022). Whereas if the business had only done the social engineering training, the attack would be more likely to succeed since it has not trained the victim to deal with the new technique. Therefore, a SOC would be more effective in this way than the training because it is less affected by the changing landscape of techniques used in cyberattacks.

When a SIEM flags a non-suspicious action as suspicious, it is called a false positive and this is very common both when the SIEM has been initially implemented and even after it has been fine-tuned to the business (Onwubiko & Ouazzane, 2019). One such false positive could be an employee updating an app through Command Prompt, which would be suspicious even though it is not malicious because Command Prompt is often used by malware (see Appendix A). Furthermore, a SIEM can also produce false negatives, which occur when the SIEM flags a suspicious action as not suspicious. These occur much less frequently than false positives but are arguably more significant because they represent a real cyberattack that went unnoticed. An employee would have to manually report one for it to be entered in the SIEM. Whilst tuning the SIEM would reduce the number of false positives and negatives, it requires ongoing maintenance as it will never be perfect.

Consequently, implementing a SOC would be quite expensive due to the costs of ongoing maintenance and contacting the team behind the SOC. Additionally, the business would also need to put a considerable amount of effort into helping the SOC integrate with its systems, as well as responding to false positives since this can take up to a few hours for one false positive (Vielberth et al., 2020). The team behind the SOC could confirm that a false positive is not malicious without talking to the business, however most of the time they will need to do this so that the SIEM can be specialised to the business' needs. Whereas the social engineering training would very gradually improve the business' security profile and would likely take less time as there are not many people to train.

As well as making employees more aware of social engineering, the training would likely also cause them to better understand the need for other protections such as multi-factor authentication. This is because the training could demonstrate to employees how easily attackers can obtain their account details, and that without multi-factor authentication the attackers would be able to log in to their account (Zain, 2021). Whereas if the SOC was implemented then the employees may not see the need for the protections as well, and as a result be more complacent and increase the chances of a cyberattack. Additionally, employees could become frustrated with how much the SOC has to confirm that false positives are truly not malicious.

Power

A SOC can make attackers less powerful by reducing the costs of cyberattacks, which greatly vary but are steadily increasing each year and are significant (Michail, 2015). Logs recorded by a SIEM decrease uncertainty about the causes and impacts of a cyberattack which could subsequently decrease regulatory and compliance fines, the time it takes to undergo legal action, and the cost of remediation activities. Furthermore, the cyber-reputation of a business significantly worsens if they cannot quickly and effectively communicate the causes and impacts of a cyberattack, which a SOC would help with (Perera et al., 2022). A SOC would also aid in the prevention of cyberattacks by suggesting improvements to the company’s cybersecurity profile even if they do not implement them. Thus, a SOC would reduce the costs of a cyberattack by ensuring that the business understands its causes and ramifications.

On the other hand, the training would reduce the chance of a cyberattack in addition to the impacts of cyberattacks that do happen. Social engineering attacks are often powerful through information since phishing emails that are more specific to the target are more likely to succeed (Jampen et al., 2020). The training would probably make employees more conscious of what they share online so it could make it harder for attackers to find information that they can leverage in an attack. Furthermore, the training would make it harder for the attacker to manipulate the target as they would be more likely to recognise a phishing email as suspicious and report it.

Moreover, the team behind the SOC would need to know a lot about the business, which would much more difficult if it is outsourced (Glynn, 2023). This is less needed to teach the employees about social engineering in the training as it could be generalised for all businesses. Furthermore, if the team that is testing the employees with simulated phishing attacks knows less about the business, then it would be more similar to a real attacker, so this would in fact be beneficial for the training.

Space

A SIEM is only implemented in the space of the company's network, so if an employee is outside of it then they are not monitored. Attackers can exploit this by encouraging employees to move off of the network, such as through a new phishing technique where a link to a malicious website is included in an email in the form of a QR code (Young, 2024). This encourages the employee to use their phone to scan it and then visit the malicious website, which would likely not use the office network that is monitored by the SIEM. Furthermore, it is difficult and computationally expensive to detect this attack through email filters because a machine learning algorithm would have to be used to recognise that an image is a QR code and then visit the site that it leads to. Whereas if this was done on the network then the SIEM could flag it as suspicious, and the SOC would be notified.

Systems

Another advantage of a SOC over social engineering training is that it is automated so there is less pressure placed on employees and they also do not need to record logs of operations (see Appendix C). This would ensure that the business collects the data required by law in case of an investigation, and without it this would be very tedious to do. Furthermore, a SOC would eliminate a lot of the area for human error in the system as there is a fallback in case someone makes a mistake or is malicious. For example, a SIEM could recognise that someone tried to log in to an employee’s enterprise account for an app from an odd location and subsequently flag it as suspicious. Then, someone on the team for the SOC could confirm with the business that it is not malicious, but if it is then they could lock or delete the account.

The company IT employee stated that in the company’s simulated social engineering campaign about 60% of the company clicked on a malicious link, and that an attack would likely succeed if they did not have a SOC implemented (see Appendix A). Most cyberattacks exploit human qualities, such as by offering free gift cards which exploits the human weakness of greed (Alkhalil et al., 2021). Phishing attacks also often attempt to induce impulsive decisions by making the situation seem urgent, so even with training it does take quite a bit of effort to decide whether an email is malicious (Davies, 2023). With enough

time, this will eventually take a toll on employee wellbeing, but a SOC would dampen the effects of an employee faltering.
Although, SOCs rely on manual reporting so if employees have not been trained to identify cyber-incidents it can substantially reduce the quality of them (see Appendix B). This is because it increases the likelihood of false positives and when they happen staff need to manually report them to both stop the impending cyberattack and improve the SIEM. Additionally, employees might hesitate in reporting attacks due to the fear of repercussions or being seen as incompetent (Davies, 2023). Whereas if the training was done effectively then they would likely be more comfortable with reporting a mistake or cyberattack.

If a business outsources their SOC, then the time to detect and understand a cyberattack is shorter because the SOC is run by experts and there is a set process for detecting cyberattacks (Ostra Cybersecurity, 2023). It would also be operational round-the-clock, whereas it would be unreasonable for a small business with few employees to be constantly monitoring the SIEM. Consequently, if the SOC is outsourced then the business would be able to divert their attention to other things rather than trying to detect cyberattacks. Although, a third party could sometimes be busy investigating can guarantee a consistent turnaround time if they put enough effort in, whereas a third party might be busy dealing with other businesses. Overall, outsourcing the SOC would be the safer option as the business is inexperienced and has limited resources.

Values and ethics

Both a SIEM and social engineering training would provide customers and employees of the business with more privacy as their data is better protected. However, with an outsourced SIEM that is well integrated with the business' systems, the third party would be able to view and record its processes. Whilst the third party would be trusted, they would also be yet another target for a data breach so people's data would be more vulnerable. On the other hand, simulated phishing campaigns can be quite invasive because the third party would perform extensive research and manipulation on targets. Consequently, these campaigns could induce paranoia in the employees and backfire by lowering morale and productivity (Davies, 2023).

Outsourcing either protection would also shift some of the ethical responsibility of the business' cybersecurity profile onto the third party, so if there is a cyberattack it would be less at fault (Rowe, 2008). Although, outsourcing a SOC would also grant it less control over its cybersecurity profile and its day-to-day operations (Glynn, 2023). Whilst the third party would be required to provide a confidentiality agreements to ensure that the business' data is secure, the business would not be able to know or change the inner workings of how its data is handled. To summarise, the SOC would probably be more ethical primarily because it would affect the wellbeing and productivity of the employees less than the social engineering training.

Evaluation

Overall, there are many benefits and challenges to both training employees to have awareness of social engineering and implementing a SOC. A SOC would immediately make the entire business noticeably more secure, but this matters less for a small business and training would likely require less effort, time, and money as a SIEM needs to be tuned. Both protections would reduce the impact of cyberattacks, however the training would also help prevent them. Moreover, if an attacker lures an employee off of the business' network, the SIEM would not be able to monitor them. On the other hand, an outsourced SIEM automates a lot of processes so there is a fallback in case an employee falters to an attack and employees need to log processes less. The team behind the SOC are also a group of experts so the time to detect an attack would be shorter and the business would have some guidance for responding to it. Both protections would be invasive towards but also guarantee that the employees' privacy would be kept safe from attacks. Therefore, a SOC would be slightly more effective than the training.

Conclusion

Whilst implementing the SOC would be slightly more effective, it would still be significantly beneficial to also conduct social engineering training but with a lower priority. The training would likely enhance the SOC as employees would be better and faster at reporting incidents. However, this inquiry was limited by the fact that I only considered the SIEM and the team behind the SOC. In fact, there are many other tools and components in the SOC, which could affect the result of this inquiry (Vielberth et al., 2020).

References

Agrafiotis, I., Nurse, J. R. C., Goldsmith, M., Creese, S., & Upton, D. (2018). A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. *Journal of Cybersecurity*, *4*(1), tyy006. https://doi.org/10.1093/cybsec/tyy006

Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing Attacks: A Recent Comprehensive Study and a New Anatomy. *Frontiers in Computer Science*, *3*. https://www.frontiersin.org/articles/10.3389/fcomp.2021.563060

Australian Signals Directorate. (2023). *ASD Cyber Threat Report 2022-2023*. https://www.cyber.gov.au/about-us/reports-and-statistics/asd-cyber-threat-report-july-2022-june-2023

Davies, V. (2023, April 28). *The psychological impact of phishing attacks on employees*. https://cybermagazine.com/articles/the-psychological-impact-of-phishing-attacks-on-your-employe

Glynn, P. (2023, May 30). What Are Pros and Cons of Outsourcing Cybersecurity? *Insight Global*. https://insightglobal.com/blog/outsourcing-cybersecurity-pros-cons/

Graphus. (n.d.). *Spear Phishing & Social Engineering | Graphus eBook*. Graphus. Retrieved 5 May 2024, from https://www.graphus.ai/resources/spear-phishing-social-engineering/

Iacono, L., Glass, G., & Wojcieszek, K. (2023). *Q4 2023 Cyber Threat Landscape Report: Threat Actors Breach the Outer Limits*. Kroll. https://www.kroll.com/en/insights/publications/cyber/threat-intelligence-reports/q4-2023-threat-landscape-report-threat-actors-breach-outer-limits

Jampen, D., Gür, G., Sutter, T., & Tellenbach, B. (2020). Don’t click: Towards an effective anti-phishing training. A comparative literature review. *Human-Centric Computing and Information Sciences*, *10*(1), 33. https://doi.org/10.1186/s13673-020-00237-7

Juroeayvant, A. (2023, May 1). How Often Do You Need to Train Employees on Cybersecurity Awareness? *ayvanT IT Services - Irvine, California*. https://ayvant.com/blog/how-often-do-you-need-to-train-employees-on-cybersecurity-awareness/

Michail, A. (2015, July 21). *Security Operations Centers: A Business Perspective*. https://www.semanticscholar.org/paper/Security-Operations-Centers%3A-A-Business-Perspective-Michail/a72d5cf608761c2df7154f2a8373db3aa60e26f6

Onwubiko, C., & Ouazzane, K. (2019). Challenges towards Building an effective Cyber Security Operations Centre. *International Journal on Cyber Situational Awareness*, *4*(1), 11–39. https://doi.org/10.22619/IJCSA.2019.100124

Orange Cyberdefense. (2023, April 5). *SOC, SIEM, MDR, EDR... What are the differences?* https://www.orangecyberdefense.com/global/blog/managed-detection-response/soc-siem-mdr-edr-what-are-the-differences

Ostra Cybersecurity. (2023, August 15). *Insourcing Vs. Outsourcing Cybersecurity:How To Find The Best Approach For Your Practice | Ostra*. https://www.ostra.net/insourcing-vs-outsourcing-cybersecurity/

Perera, S., Jin, X., Maurushat, A., & Opoku, D.-G. J. (2022). Factors Affecting Reputational Damage to Organisations Due to Cyberattacks. *Informatics*, *9*(1), Article 1. https://doi.org/10.3390/informatics9010028

Phishing, Technique T1566—Enterprise | MITRE ATT&CK®. (n.d.). Retrieved 5 May 2024, from https://attack.mitre.org/techniques/T1566/

Pinson-Roxburgh, O. (2023, March 28). *Difference between MDR, SOC & SIEM*. Defense.Com™. https://www.defense.com/blog/mdr-soc-and-siem

Rowe, B. R. (2008). *Will Outsourcing IT Security Lead to a Higher Social Level of Security?* http://www.lib.ncsu.edu/resolver/1840.16/441

Sophos. (2024, April 30). *Managed Detection and Response | Sophos MDR*. https://www.sophos.com/en-us/products/managed-detection-and-response

Tam, T., Rao, A., & Hall, J. (2021). The Good, The Bad and The Missing: A Narrative Review of Cyber-security Implications for Australian Small Businesses. *Computers & Security*, *109*, 102385. https://doi.org/10.1016/j.cose.2021.102385

Teodor, B. (2022, July 13). *Top Five SIEM Use Cases For Active Threat Detection*. Arcanna.Ai. https://blog.arcanna.ai/top-five-siem-use-cases-for-active-threat-detection

Vielberth, M., Böhm, F., Fichtinger, I., & Pernul, G. (2020). Security Operations Center: A Systematic Study and Open Challenges. *IEEE Access*, *8*, 227756–227779. IEEE Access. https://doi.org/10.1109/ACCESS.2020.3045514

Young, P. (2024, April 17). *How Cloudflare Cloud Email Security protects against the evolving threat of QR phishing*. The Cloudflare Blog. https://blog.cloudflare.com/how-cloudflare-cloud-email-security-protects-against-the-evolving-threat-of-qr-phishing

Zain, M. (2021, October 18). *8 Benefits of Multi-Factor Authentication (MFA)*. https://www.pingidentity.com/en/resources/blog/post/eight-benefits-mfa.html

Appendix

A. Company IT employee

Notes from my interview with an employee at a company's IT department

SIEMs produce a lot of false positives

- updating an app sometimes runs commands in command prompt
- browser extensions are often suspicious

False sense of security - huge majority of false positives

The company ran a simulated phishing campagin through email

- over 60% of employees clicked the link which could easily lead to them downloading malware or inputting credentials into a fake site
- phishing emails should be filtered by an email filter or a SOC should be used to quickly notice that an employee clicked on an unknown link

SOC atleast initially is still better than other protections and training (better as size of company gets bigger) because it immediately applies to the whole company, whereas other protections take more time

Hacker impersonated another company (spearfishing), ordered stock to a random location, was very successful

B. High school IT employee

My questions to and the answers from an IT employee at a high school

1. How does the risk and impact of social engineering threats in cybersecurity compare to other cyber threats?

Social engineering threats are relatively common and usually come from one compromised account being used to spread a phishing or scam email. Socially engineered threats like this can also cause distrust of the system and users may be less inclined to use our systems. These threats can become especially dangerous if a high level account such as the principle or IT manager were compromised as it could result in exposing confidential data about students and staff.

2. How effective are Managed Detection and Response systems (or specifically Sophos) in mitigating social engineering threats (e.g. phishing and scam emails)?

The system used for web monitoring is “Symantec WebFilter”. This will usually classify and automatically block dangerous websites, including those from known phishing sites. For emails we use a combination of manual reporting and automated detection from Microsoft. In the event of a detected phishing threat any user who has interacted with it will have their account locked until the threat is managed.

3. Does a lack of social engineering training reduce the effectiveness of MDR systems?

Manage Detection and Response systems often rely on manual reporting and if staff are not able to detect and identify these threats it can substantially reduce the MDR systems ability to detect these kinds of threats.

C. Consultant

My questions to and the answers from the consultant that implemented Sophos for my father

When I say “Sophos”, I’m referring to any Sophos product but the focus is on the Managed Detection and Response component

1. How much did you educate the employees of this business about social engineering threats (e.g., scam emails, spear phishing), and could you do more of this?

No formal training has been proposed; however, this would be highly recommended.

From conversing with the employees, they all have basic understanding and common-sense awareness in comprehending a received e-mail by checking first the senders address to see if the addressee and domain name is relatable to the content in the body of the e-mail. If unsure, not clicking on URL links within the body. Brining the e-mail to attention of the IT department and their line manager.

To answer the second part of your question, yes, we could do more about educating the end user by using handouts, pdf documents, in person training sessions remotely by MS Teams or Zoom sessions, education as part of employee onboarding/induction training, using company acceptable e-mail and Internet use policies. The employee acknowledging, they have completed the training and understand.

Proposing and implementing a ‘Phishing Campaign’ function within Sohpos Central (at additional licensing cost per year), to simulate a phishing email, that is sent on random intervals, and if an employee clicks on a link within the e-mail body, the administrator and their line manager is notified, and they have to complete a mandatory online course.

Sophos, like other cybersecurity companies, often employs a multi-faceted approach to educate end users about phishing threats. Here are some common methods:

Phishing Simulation Training:

Sophos and other security companies may conduct phishing simulation exercises. These simulations involve sending mock phishing emails to employees to test their ability to recognize and resist phishing attempts. These exercises aim to raise awareness and improve users' ability to identify suspicious emails.

Interactive Training Modules:

Sophos may offer interactive training modules that cover various aspects of cybersecurity, including phishing awareness. These modules often include educational content, quizzes, and real-life examples to help users understand the tactics used by attackers.

Security Awareness Programs:

Sophos may provide comprehensive security awareness programs that cover not only phishing but also other security best practices. These programs can include videos, articles, and other resources to help users stay informed about evolving cybersecurity threats.

Regular Security Updates and Tips:

Security companies often share regular updates and tips with their users to keep them informed about the latest threats and best practices. This may include information about new phishing techniques, common tactics used by attackers, and steps users can take to protect themselves.

Email Alerts and Warnings:

If Sophos detects a phishing campaign or a new threat, they may issue email alerts or warnings to their users. These notifications can provide details about the threat, red flags to look out for, and guidance on how to avoid falling victim to the specific attack.

Currently Security Alerts are sent to the Managed Service Provider (myself) and to the Office Manager.

Integration with Security Software:

Sophos may integrate educational elements directly into their security software. For example, if a user receives an email that the system flags as potentially malicious, the software may provide real-time guidance on why the email is suspicious and what precautions the user should take.

Preventative measures using a managed security technology was the first priority to implement within the organisation to provide the capability of Network scanning, and protection and detection of malicious code via the network gateway (The Sophos Firewall Appliance), and the installation of a managed Security software agent for all computing end points which include Windows desktops and laptops within the company. These are monitored via the Sophos Central Cloud based service. More about Sophos Central Below.

Sophos Central is a cloud-based security platform developed by Sophos, a leading cybersecurity company. Sophos Central provides a unified interface for managing various cybersecurity solutions and services offered by Sophos. It is designed to simplify the deployment, management, and monitoring of security measures across an organisation's IT infrastructure.

Key features of Sophos Central include:

Unified Security Management:

Sophos Central serves as a centralised management console that allows administrators to oversee and control multiple security products from Sophos. This includes antivirus, endpoint protection, firewall, mobile security, email security, and more.

Cloud-Based Architecture:

Being cloud-based, Sophos Central enables organisations to manage their security infrastructure from anywhere with an internet connection. This is especially valuable for businesses with remote or distributed workforces.

Real-time Security Insights:

The platform provides real-time insights into the security posture of the organisation. Administrators can view threat data, security events, and other critical information to make informed decisions.

Endpoint Protection:

Sophos Central includes endpoint protection capabilities, helping organisations secure their devices (computers, servers, and mobile devices) against malware, ransomware, and other threats.

Server Protection:

Sophos Central offers server protection features to secure critical servers within an organisation. This includes antivirus, web protection, and other server-specific security measures.

Email Security:

Sophos Central provides tools for managing email security, protecting against phishing, spam, and other email-borne threats. It integrates with various email platforms to provide a comprehensive defence against email-based attacks.

Network Security:

Sophos Central includes features for managing network security, such as firewalls and intrusion prevention. This allows administrators to define and enforce security policies across their network infrastructure.

Mobile Security:

Mobile device management (MDM) and mobile security features are included in Sophos Central, helping organisations secure and manage mobile devices used by employees.

Currently no company issued mobile devices are managed via Sophos Central. Employees have BYOD personal phones.

Synchronised Security:

Sophos emphasises a concept called “Synchronised Security,” where different security components within Sophos Central work together to provide a more coordinated and effective defence against cyber threats.

Sophos Central is designed to streamline security management, enhance visibility, and improve the overall security posture of organisations. The platform is suitable for businesses of varying sizes and provides a scalable solution to address the evolving challenges in the cybersecurity landscape.

2. How does the risk and impact of social engineering threats in cybersecurity compare to other cyber threats

Social engineering threats in cybersecurity pose a significant risk and can have a substantial impact, often comparable to or even more damaging than other types of cyber threats. Social engineering involves manipulating individuals to divulge confidential information, perform actions, or make decisions that compromise the security of an organisation's systems or data.

Here's how social engineering threats compare to other cyber threats in terms of risk and impact:

Human Factor Vulnerability:

Social engineering exploits the human factor, relying on psychological manipulation to deceive individuals. People can be more unpredictable and susceptible to manipulation than technological defences.

Other cyber threats may exploit technical vulnerabilities, but social engineering specifically targets human weaknesses, making it a potent avenue for attackers.

Breadth of Targets:

Social engineering attacks can target anyone within an organisation, from low-level employees to top executives. This broad reach makes it a versatile method for attackers.

Other cyber threats may focus on specific vulnerabilities in software, networks, or systems, but they might not have the same widespread reach as social engineering attacks.

Adaptability and Creativity:

Social engineering attacks are often adaptive and can evolve based on the current social and technological landscape. Attackers continually develop new tactics to exploit human psychology.

Other cyber threats may rely on known vulnerabilities or attack vectors, and their effectiveness might diminish as security measures are improved.

Impact on Reputation and Trust:

Social engineering attacks can have a severe impact on an organisation's reputation and erode trust. If employees or customers feel deceived or if sensitive information is exposed, the damage can be long-lasting.

While other cyber threats can also harm reputation, social engineering has a unique ability to exploit trust relationships, making the impact more personal and damaging.

Detection Challenges:

Social engineering attacks can be challenging to detect because they often involve manipulation rather than technical exploits. Traditional security measures like firewalls and antivirus software may not be as effective in preventing social engineering attacks.

Other cyber threats may leave more detectable traces, making it easier for security systems to identify and respond to them.

In summary, social engineering threats in cybersecurity are a major concern due to their ability to exploit human vulnerabilities, their adaptability, and their potential for widespread impact on individuals and organisations.

While other cyber threats also pose significant risks, social engineering attacks stand out for their focus on manipulating people rather than exploiting technical weaknesses alone.

Combining technical defences with robust cybersecurity awareness training is crucial for mitigating the risks associated with social engineering.

3. With respect to businesses you've previously consulted, how much effort and thought did you have to put into maintaining and changing the Sophos programming in due course?

With medium size companies we use the SIEM (Security Information and Event Management) alert and reporting capablilties within Sophos Central to monitor and take action on events that need attention, for example out of date definitions and engine software for the computing endpoints, alerts and clean up actions taken by Sophos agents that detect a treat and report back to Sophos Central and if manual invention is required to remove a threat.

We have deployed Sophos Central as the management software for the computing end points for Windows devices.

Firewall security appliances are adopted into the Sophos Central so they can be remotely managed from the dashboard.

Sophos MDM (mobile device management) for iPhone and Android devices.

As for the management of Firewall appliances within Sophos Central, this is a consolidation of firewall appliances where some of our clients have multiple branch offices, and to securely access the firewall to manage and make changes.

Changes to a firewalls configuration (to it’s rules and security polices and services) are determined from ongoing regular security audits.

Outside of the Sophos Central dashboard, the firewall can be configured to report separately to Sophos Central and requires the administrator to login into the firewall to manage the configuration. The firewall can be setup to generate reports and emailed automatically using a schedule.

Other Security companies use Similar Cloud based management to manage multiple firewall appliances. They may include advanced holistic reporting and capture analysis.

SIEM stands for Security Information and Event Management. It is a comprehensive approach to managing an organisation's information security by providing real-time analysis of security alerts generated throughout the organization's IT infrastructure. SIEM combines Security Information Management (SIM) and Security Event Management (SEM) into a single solution to provide a holistic view of an organisation's information security.

For our small to medium size clients: Using Sophos Central (Could based).

Sophos Security Products are managed within Sophos Central including the licensing. Security Agents for the computing endpoints. Sophos firewall security appliances for the Internet Gateway. Sophos mobile device management MDM for mobile phones IOS and Android devices.

It is worth noting a Firewall is not a router, however they can do static routing and network address translation, which are functions of a router.

Other examples of SIEM’s are:

For our enterprise clients we use: (They all have different requirements).

Microsoft Defender XDR SIEM for our Azure Cloud Clients.
https://www.microsoft.com/en-au/security/business/microsoft-defender

Mircosoft InTune for endpoint management of computing and mobile devices for Windows updates, applications, conditional access etc.
https://www.microsoft.com/en-us/security/business/endpoint-management/microsoft-intune

Custom integration of the open source SIEM Wazuh https://wazuh.com

Here are the key components and functions of a SIEM system:

Data Collection:

SIEM systems collect, and aggregate log data generated throughout the organisation's technology infrastructure, including host systems and applications, network and security devices, databases, and more.

Normalisation:

Raw log data from various sources often come in different formats. SIEM systems normalise this data, converting it into a consistent format. This process makes it easier to correlate events from different sources and facilitates analysis.

Correlation:

SIEM tools correlate and analyse the normalised data to identify patterns, trends, and anomalies. Correlation helps to connect seemingly unrelated events and detect potential security incidents or threats.

Alerting and Notification:

When the SIEM system identifies a potential security incident based on its correlation rules, it generates alerts and notifications. These alerts are then sent to security administrators or analysts in real-time, enabling quick response to potential threats.

Dashboards and Reporting:

SIEM solutions provide dashboards and reporting tools that offer a visual representation of security-related data. Administrators can use these dashboards to monitor the security status of the organisation, identify trends, and gain insights into potential risks.

Incident Response:

SIEM systems support incident response efforts by providing information about the nature of security incidents, their scope, and the affected systems. This information helps security teams investigate and mitigate incidents more effectively.

Compliance Management:

Many organisations use SIEM tools to help meet compliance requirements by collecting and analysing data related to security events. SIEM solutions often include predefined reports and features that aid in compliance reporting.

Log Retention and Forensics:

SIEM systems store log data for a specified retention period, allowing organisations to conduct forensic analysis after a security incident. This historical data is valuable for understanding the timeline of events and identifying the root causes of incidents.
User and Entity Behaviour Analytics (UEBA):

Some SIEM solutions incorporate UEBA capabilities, which analyse the behaviour of users and entities to detect abnormal patterns that may indicate insider threats or compromised accounts.

4. With respect to businesses you’ve previously consulted, how effective is Sophos in mitigating social engineering threats (e.g. phishing and scam emails)?

Sophos has been quite effective as a front-line defence to preventing phishing and scam emails for clients, we deployed Sophos Intercept X.

Sophos Intercept X, which is primarily known for its advanced endpoint protection capabilities, includes features designed to detect and prevent various types of threats, including phishing and social engineering attacks. However, the specific details of the features and their effectiveness may be subject to updates and improvements, so it's recommended to refer to the latest Sophos documentation or contact Sophos directly for the most current information.

Here are some general aspects related to Sophos Intercept X and its ability to handle phishing and social engineering threats:

Email Security Integration:

Sophos Intercept X may integrate with Sophos' email security solutions to provide a layered defence against phishing attacks delivered via email. This integration allows for a more comprehensive protection strategy, combining endpoint security with email security measures.

Advanced Threat Prevention:

Intercept X often includes advanced threat prevention features such as behaviour-based analysis, machine learning, and real-time threat intelligence. These capabilities help in identifying and blocking sophisticated phishing attempts that may employ social engineering tactics.

Web Filtering:

Intercept X may include web filtering capabilities to block access to known phishing websites and malicious domains. This can prevent users from inadvertently interacting with malicious content.

Security Awareness and Training:

While Intercept X focuses on endpoint protection, Sophos recognises the importance of user education in preventing social engineering attacks. Sophos may offer additional tools and resources for security awareness training to help users recognize and avoid phishing attempts.

Phishing Simulation:

Sophos, as part of its security awareness training, offer phishing simulation tools for example phishing campaign. These tools allow organisations to simulate phishing attacks on their employees, helping assess their susceptibility and providing targeted training based on the results.

Sophos employs a multi-layered approach to mitigate social engineering and phishing threats. Here are some common strategies and features:

Email Security:

Sophos offers email security solutions that include advanced threat detection and filtering capabilities. This helps in blocking phishing emails before they reach the users' inboxes. These solutions often leverage machine learning and threat intelligence to identify and block malicious content.

Anti-Phishing Education:

Sophos, like many cybersecurity providers, recognizes the importance of user education. Sophos provides resources and tools for organizations to educate their employees about the dangers of phishing and how to recognize and avoid phishing attempts.

Phishing Simulation:

Sophos may offer phishing simulation tools as part of their security awareness training. These tools allow organisations to conduct simulated phishing attacks on their employees to assess their susceptibility to phishing and provide targeted training based on the results.

Endpoint Protection:

Sophos provides endpoint protection solutions that include features like advanced threat prevention, web filtering, and behaviour-based analysis. These measures help protect endpoints (computers, servers, and other devices) from malware and phishing attempts.

Web Filtering:

Sophos may incorporate web filtering capabilities to block access to known phishing websites and malicious domains. This helps prevent users from inadvertently visiting websites that may host phishing content.

Synchronised Security:

Sophos emphasizes a concept known as "Synchronised Security," where different security components within their ecosystem work together to provide a more coordinated and effective defence. This integration helps improve the overall security posture and response to threats, including those related to social engineering.

Threat Intelligence:

Sophos utilises threat intelligence feeds to stay updated on the latest phishing campaigns, tactics, and techniques. This information is used to enhance the detection capabilities of their security solutions.

Effectiveness can vary based on various factors, including the specific Sophos products deployed, the organisation's security policies, and the level of user awareness and training.

No security solution can provide 100% protection, and a comprehensive cybersecurity strategy often involves a combination of technical measures, user education, and proactive monitoring.

5. To what extent does a lack of social engineering training reduce the effectiveness of Sophos?

Social engineering training plays a crucial role in enhancing the overall security posture of an organisation, and its absence can impact the effectiveness of security solutions, including Sophos.

While Sophos provides advanced endpoint protection and other security features to defend against various threats, including those involving social engineering, **the human element remains a significant factor in cybersecurity.**

6. What would you recommend to the business to improve their awareness of social engineering threats, or their cybersecurity profile as a whole?

Cybersecurity is an ongoing process, and a combination of proactive measures, user education, and technology solutions is essential for creating a robust defence against social engineering and other cyber threats.

Regularly reassess and update security strategies to address emerging risks.

Improving awareness of social engineering threats and enhancing overall cybersecurity posture is crucial for any business.

Here are some recommendations:

Implement Security Awareness Training:

Provide regular security awareness training for all employees to educate them about common social engineering tactics, such as phishing, pretexting, and baiting. Include real-world examples and scenarios to make the training more relevant.

Conduct Phishing Simulations:

Perform periodic phishing simulations to assess the effectiveness of training and identify areas for improvement. Simulated phishing attacks can help employees recognise and avoid falling victim to actual threats.

Establish a Strong Security Culture:

Foster a culture of cybersecurity awareness throughout the organisation. Encourage employees to be proactive in reporting suspicious activities and make them aware of the critical role they play in maintaining a secure environment.
Use Multi-Factor Authentication (MFA):

Implement multi-factor authentication wherever possible to add an extra layer of security, especially for accessing sensitive systems and data. This helps protect against unauthorised access even if credentials are compromised.

Regularly Update and Patch Systems:

Keep all software, operating systems, and applications up to date with the latest security patches. Regular updates help address vulnerabilities that could be exploited by attackers.

Endpoint Protection:

Deploy advanced endpoint protection solutions to defend against malware, ransomware, and other threats. Solutions like antivirus software, intrusion detection/prevention, and behaviour-based analysis can enhance overall endpoint security.

Network Security:

Implement robust network security measures, including firewalls, intrusion detection/prevention systems, and secure Wi-Fi configurations. This helps protect the organisation's network infrastructure from various cyber threats.

Secure Email Gateways:

Use secure email gateways to filter out malicious emails, phishing attempts, and other email-borne threats. This helps prevent employees from falling victim to social engineering attacks delivered through email.

Incident Response Plan:

Develop and regularly update an incident response plan to ensure a swift and effective response in the event of a security incident. This plan should outline roles and responsibilities, communication procedures, and steps to contain and mitigate threats.

Data Backup and Recovery:

Regularly back up critical data and ensure that recovery procedures are in place. This helps mitigate the impact of ransomware attacks and other data loss incidents.

Access Controls:

Implement the principle of least privilege by granting employees access only to the resources necessary for their roles. Regularly review and update user access permissions to reduce the risk of unauthorised access.

Regular Security Audits:

Conduct regular security audits and assessments to identify vulnerabilities and weaknesses in the organisation's systems, processes, and policies.

Stay Informed About Threat Landscape:

Stay informed about the latest cybersecurity threats and trends. Follow industry news, participate in relevant forums, and consider threat intelligence services to understand evolving risks.

Collaborate with Security Experts:

Engage with cybersecurity experts, either internally or externally, to assess the organisation's security posture and receive guidance on implementing best practices.

Guides and Resources:

Here are some resources and training programs available to educate employees about social engineering threats.

Here are some examples:

Social Catfish:

Offers comprehensive training sessions for employees to educate them about social engineering tactics, their potential impact on the organisation, and how to recognise and respond to them. These sessions can include real-life examples, case studies, and interactive activities to enhance learning and engagement.

https://socialcatfish.com/scamfish/social-engineering-awareness-in-the-workplace-educating-employees-to-prevent-attacks/

SecurityMetrics:

Offers a white paper that provides an overview of social engineering, common social engineering techniques, and 5 steps to train your workforce on social engineering.

https://www.securitymetrics.com/learn/how-train-your-workforce-social-engineering

MetaCompliance:

Provides a guide to educating employees about social engineering tactics and techniques. The guide outlines best practices for a successful program of social engineering education.

https://www.metacompliance.com/blog/cyber-security-awareness/educating-employees-social-engineering

Mimecast:

Offers social engineering training to help defend against sophisticated phishing attacks. The training educates and trains employees to prevent a socially engineered attack.

https://www.mimecast.com/blog/social-engineering-awareness-training-for-employees/

These resources can help organisations create a culture of security awareness and promote a sense of responsibility among employees. Adequate training on social engineering can help employees recognise potential threats, avoid common pitfalls, and understand how to respond to suspicious activities.