IT Technologies - Cybersecurity

Sean Atherton: Assignment 2 IT Report

What does it do?

Cybersecurity is generally considered the protection of computer systems and networks. What specifically falls under this umbrella is the hardware, software, and electronically stored data. The field has and still is becoming more relevant by the day with our increased reliance on computer systems and networks. Having something like a WAN (Wide Area Network) means that criminals will inevitably try to find exploits and vulnerabilities in the design, operation, and implementation.

There are several different types of Cybersecurity attacks. Some types of Cybersecurity threats and attacks are ***Phishing*** (Example: sending fraudulent emails that resemble emails from official sources and companies), ***Ransomware*** (Example: Blocking access to computer systems or files until a ransom is paid), ***Malware*** (Example: Software used to cause damage or gain access to computer systems or files etc.) and ***Social Engineering*** (Example: Using strategies and tactics to "trick" users into revealing sensitive information, this can be combined with other types of attacks) *(Cisco Systems, 2021)*

If you have ever set up a home network, then it is almost certain that some form of automation was used along the way to cut back on the time needed to get everything secure and up and running. This is something that has been happening for a long time not just in cybersecurity but is starting to take shape in areas that had previously required administrators and users to be involved in every step of the tedious process. In an article from Connected – Official Technology Community of Connection they stated that 'The Adoption of security automation technologies has increased 12% year over year, with signs of further growth' (Connected, 2020, para. 1).

Automated Cybersecurity's main purpose is to highlight and resolve common security events/alerts missed by the IT team which are usually attributed to human error, inexperience workload and negligence. According to research conducted by the ESG (ESG & Phantom, 2016), 'IT Teams ignore 74 per cent of security/alerts- even when they have security solutions in place.

The applications and roles that Security Automation fills are 'Threat Hunting' and 'Security Incident Response' (Red Hat, 2021). Threat Hunting would usually involve going through organizations IT environment and identifying potential openings and weaknesses prone to cybersecurity attacks ideally before they happen. A Security Incident response involves both detecting and containing a security breach. Both these processes are hardly viable to perform manually in a large business by a security team, however, with automated security, a business can identify, validate, and escalate threats faster without manual intervention (Red Hat, 2021).

Automated Security software can be created from scratch by a business but often is implemented and customized from an existing security playbook which provides existing configurations to automate responses to threats. An Automated IT Tool like a SOAR (Security Orchestration, Automation and

Response) combines both human inputs and administration with machine power to 'Help define, prioritize and drive standardized incident response activities' (Gartner Glossary, 2021, para 1). When using Security Automation, the Security team needs to communicate with the other IT departments and teams in an organization to allow automated responses to be carried out without always requiring direct approval for the immediate changes and solutions.

With the way Security Automation is developing and progressing I would estimate that it would be likely that the algorithms and machine learning could monitor and be fed large quantities of information and effectively be able to predict attacks by taking preemptive actions and adapting on the fly, operating almost entirely without the need for user intervention. Ultimately a system like this is very similar to AI-based learning close to the likes of Facial Scan technology being used to identify criminals.

What is the likely impact?

Since the implementation of these systems into Cybersecurity, organizations have been able to more specifically understand how to maximize their security investment and improve operations through automation. Reports and incidents can be recorded with more precise and important information when compared to more simplistic write-ups from the Security and IT teams. Although I doubt anytime soon that an organizations cybersecurity system and infostructure will be entirely automated, common sense and evidence suggest that these systems will no doubt improve and become more optimized for the lower-level threats and analysis freeing up cybersecurity teams focus and allowing them to become more productive and effective when monitoring and problem solving the higher-level security.

People working in positions and areas of Cybersecurity where the threats that they are monitoring and resolving are considered to be low-level threats and relatively unsophisticated in design will likely be made obsolete by automation and machine learning like other industries that once required humans to be hands-on. Although these positions will likely shift towards training and dealing with the Security Automation software and systems that now deal with the threats directly as opposed to the people who previously performed the tasks and responsibilities.

How will this affect you?

The impact and changes I will likely experience in my day-to-day life are abundances of identity and system verifications for my devices such as computers and phones and interacting with software and applications that monitor and report cyber-related threats and attacks instead of human support etc. If an organizations systems and data is breached/comprised the case of an attacker outmaneuvering the automated security will become more of a talking point in the media and reports.

When setting out to progress through a career in IT or any organization I will need to keep in mind that the demand for positions where the level of complicity and human input is almost null will become less and less. I will likely require training and education surrounding how these automated systems operate and how to work with and around them in an organization or business environment to improve

effectiveness. *'According to The US Bureau of Labor Statistics' Information Security Analyst's Outlook, cybersecurity jobs are among the fastest-growing career areas nationally. The BLS predicts cybersecurity jobs will grow 31% through 2029, over seven times faster than the national average job growth of 4%.'*(Bureau of Labor Statistics, 2021, para. 3). Based on this information demand for high-level Cybersecurity careers is only going to increase and grow as more companies look to develop their IT systems. Employers are prepared to hire and pay more for workers with the skills to prevent attacks before they occur rather than those how can work in an environment as attacks occur. So, going forward I would need to follow the recent changes and stay up to date on new strategies and threats if I wanted to pursue a career in Cybersecurity as companies begin to hand over tasks to automation to increase efficiency and avoid human error.

Reference List:

1. Cisco Systems 2021, *What Is Cybersecurity?*, Cisco Systems, viewed 5 April 2021, https://www.cisco.com/c/en_au/products/security/what-is-cybersecurity.html

2. Connected – Official Technology Community Connection, 'Will Cyber Security Become Automated?', *Connected,* 28 October 2020, viewed 6 April 2021, https://community.connection.com/will-cyber-security-become-automated/

3. ESG, Phantom 2016, *Phantom and ESG Research Finds Companies Ignore Majority of Security Alerts,* Industry report, BusinessWire, viewed 6 April 2021, BusinessWire database https://www.businesswire.com/news/home/20160315005555/en/Phantom-ESG-Research-Finds-Companies-Ignore-Majority

4. Red Hat Software 2021, *What is security automation?,* Red Hat Software, viewed 6 April 2021, https://www.redhat.com/en/topics/automation/what-is-security-automation

5. Gartner 2021, *Gartner Glossary – Security Orchestration, Automation and Response (SOAR),* Gartner 2021, viewed 6 April 2021, https://www.gartner.com/en/information-technology/glossary/security-orchestration-automation-response-soar

6. Bureau of Labor Statistics, U.S. Department of Labor, *Occupational Outlook Handbook*, Information Security Analysts, visited April 02, 2021, <https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm>