International Journal Of Multidisciplinary Research In Science, Engineering and Technology (IJMRSET)

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 4.988

| Volume 4, Issue 4, April 2021 |

Computational Intelligence Techniques for Security Systems

Dr. Parisha

Assistant Professor, Dept. of Computer Science, MNS Government College, Bhiwani, Haryana, India

ABSTRACT: Computer security, cybersecurity or information technology security (IT security) is the protection of computer systems and networks from information disclosure, theft of or damage to their hardware, software, or electronic data, as well as from the disruption or misdirection of the services they provide.The field is becoming increasingly significant due to the increased reliance on computer systems, the Internet and wireless network standards such as Bluetooth and Wi-Fi, and due to the growth of "smart" devices, including smartphones, televisions, and the various devices that constitute the "Internet of things". Owing to its complexity, both in terms of politics and technology, cybersecurity is also one of the major challenges in the contemporary world.Security information and event management (SIEM) has evolved to include advanced analytics such as user behavior analytics (UBA), network flow insights and artificial intelligence (AI) to accelerate detection as well as integrate seamlessly with security orchestration, automation and response (SOAR) platforms for incident response and remediation. SIEM can be enhanced by consulting and managed services to help with a threat management program, policy management and augmenting security staff. Anomali Cyber Watch, a weekly intelligence digest published by Anomali Threat Research, provides summaries of significant cybersecurity and threat intelligence events, analyst comments and recommendations to increase situational awareness, and the associated tactics, techniques, and procedures (TTPs) to empower automated response actions proactively. Intelligence in Anomali Cyber Watch covers current concerns and active threats, including botnets, breaches, misconfigurations, ransomware, threat actors and groups, vulnerabilities, campaigns, and trends. The IOCs related to these events are also included in Anomali Cyber Watch, providing immediately actionable intelligence. Recently, cryptology problems, such as designing good cryptographic systems and analyzing them, have been challenging researchers. Many algorithms that take advantage of approaches based on computational intelligence techniques, such as genetic algorithms, genetic programming, and so on, have been proposed to solve these issues.

I.INTRODUCTION

As a security leader, you need more from your threat intelligence. That's why we've put together an on-demand webinar with Dark Reading, featuring leading threat research and intelligence experts who'll show you how to:
Apply the intelligence lifecycle process and automation to deliver operational and strategic intel
Level up your threat intel program with best practices and practical use cases[1,2]
Drive better decisions in your organization and maximize returns on your threat intel investments
Whether you have some background in tech or are interested in learning more about IT and technical risks this class if for you. No technical experience is required.
Learn how to apply existing frameworks and cybersecurity standards to organizational settings
Perform threat modeling and cyber risk assessment projects
Acquire the skills to craft cyber incident response plans and risk sharing strategies
And expand your network of professionals in cybersecurity and risk management
As threat intelligence for example Factal is the only company that detects, verifies and geolocates early signals of breaking news at the speed of social media. Then our platform shows how your organization is impacted in real time around the globe – minus all the noise and misinformation.[3,4]
Respond faster:Through a hybrid of AI and experienced journalists, Factal delivers the facts you need to make fast, confident decisions. Stop sifting through the noise.
Pinpoint what matters: Get just the breaking news that matters to your organization, drawn from thousands of open-data sources and geolocated down to the meter.

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 4.988

| Volume 4, Issue 4, April 2021 |

Collaborate live:Join a secure chat with Factal editors and the largest community of security, crisis and disaster response pros in the world, 24 hours a day.[5,6]
The computer integrated data security architecture keeps your data secure,from the moment it is discovered and classified to the process of being protected and analyzed.No matter where your sensitive unstructured data is in the ever-changing IT environment, including repositories, endpoints, databases, printouts, email and mobile devices,it remains secure to meet various security requirements of the different stages in the document lifecycle.[7,8]
A vulnerability is a weakness in design, implementation, operation, or internal control. Most of the vulnerabilities that have been discovered are documented in the Common Vulnerabilities and Exposures (CVE) database. An exploitable vulnerability is one for which at least one working attack or "exploit" exists. Vulnerabilities can be researched, reverse-engineered, hunted, or exploited using automated tools or customized scripts. Cybersecurity is a fast-growing field of IT concerned with reducing organizations' risk of hack or data breach.[9,10]

II.DISCUSSION

Threat intelligence is evidence-based information about cyber attacks that cyber security experts organize and analyze. This information may include:
Mechanisms of an attack
How to identify that an attack is happening
Ways different types of attacks might affect the business
Action-oriented advice about how to defend against attacks [11,12]

Many forms of cyber attacks are common today, including zero-day exploits, malware, phishing, man-in-the-middle attacks, and denial of service attacks. Different ways of attacking computer systems and networks are constantly evolving as cyber criminals find new vulnerabilities to exploit. Cyber threat intelligence (CTI) helps organizations stay informed about new threats so that they can protect themselves. Cyber security experts organize, analyze, and refine the information they gather about attacks to learn from it and use it to better protect businesses. Threat intelligence (or security intelligence) also helps stop or mitigate an attack that is in progress. The more an IT team understands about an attack, the better they will be able to make an informed decision about how to combat it.There are different types of threat intelligence, from high-level, non-technical information to technical details about specific attacks. [7]

Here are a few different kinds of threat intelligence:
Strategic: Strategic threat intelligence is high-level information that puts the threat in context. It is non-technical information that an organization could present to a board of directors. An example of strategic threat intelligence is the risk analysis of how a business decision might make the organization vulnerable to cyber attacks.
Tactical: Tactical threat intelligence includes the details of how threats are being carried out and defended against, including attack vectors, tools, and infrastructures attackers are using, types of businesses or technologies that are targeted, and avoidance strategies. It also helps an organization understand how likely they are to be a target for different types of attacks. Cybersecurity experts use tactical information to make informed decisions about security controls and managing defenses. [6]

Operational: Operational threat intelligence is information that an IT department can use as part of active threat management to take action against a specific attack. It is information about the intent behind the attack, as well as the nature and timing of the attack. Ideally this information is gathered directly from the attackers, which makes it difficult to obtain.
Technical: Technical threat intelligence is specific evidence that an attack is happening or indicators of compromise (IOCs). Some threat intelligence tools use artificial intelligence to scan for these indicators, which might include email content from phishing campaigns, IP addresses of C2 infrastructures, or artifacts from known malware samples.
Threat intelligence and cyber threat tools help organizations understand the risks of different types of attacks, and how best to defend against them. Cyber threat intelligence also helps mitigate attacks that are already happening. An organization's IT department may gather its own threat intelligence, or they may rely on a threat intelligence service to gather information and advise on best security practices. Organizations that employ software defined networking (SDN) can use threat intelligence to quickly reconfigure their network to defend against specific types of cyber attacks.

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 4.988

| Volume 4, Issue 4, April 2021 |

III.CONCLUSION

For years, threat intelligence has focused on collecting tactical indicators of compromise (IOCs) like domains, IP addresses and hashes.As a security leader, you need more from your threat intelligence. That's why we've put together an on-demand webinar with Dark Reading, featuring leading threat research and intelligence experts who'll show you how to:
Apply the intelligence lifecycle process and automation to deliver operational and strategic intel
Level up your threat intel program with best practices and practical use cases
Drive better decisions in your organization and maximize returns on your threat intel investments
In addition, we'll walk you through uncovering, identifying and defusing a recent threat operation as well as how to improve the ROI from your threat feeds.[11,12]
Threat intelligence allows organizations to be proactive instead of reactive when it comes to cyber attacks. Without understanding security vulnerabilities, threat indicators, and how threats are carried out, it is impossible to defend against cyber attacks effectively. Threat intelligence can prevent and contain attacks faster, potentially saving businesses hundreds of thousands of dollars. Threat intelligence can augment enterprise security controls at every level, including network security and cloud security.
Security personnel can often find indications that an attack is happening or has happened, if they are looking in the right places for unusual behavior. Artificial intelligence can help tremendously with this effort. Some commons IOCs include:
Unusual privileged user account activity: Attackers often try to gain higher account privileges or move from a compromised account to another account that has higher privileges.
Login anomalies: After-hours logins that attempt to access unauthorized files, logins in quick succession to the same account from different IPs around the world, and failed logins from user accounts that do not exist are all good indicators that something is amiss.
Increases in database read volume: Seeing a large increase in database read volume could indicate that someone is extracting an unusually large amount of data, such as all of the credit card numbers in a database.
Unusual domain name system (DNS) requests: Large spikes in DNS requests from a specific host and patterns of DNS requests to external hosts are both red flags because they could mean someone from outside the organization is sending command and control traffic.
Large numbers of requests for the same file: A large part of cyber criminal activity involves repeated attacks, which can indicate that someone is searching for a vulnerability. Seeing 500 requests for the same file could indicate that someone is trying different ways to find a weakness.
Unexplained configuration or system file changes: While it is difficult to find a credit card harvesting tool, it is easier to find system file changes that happen from the tool being installed.
A variety of threat intelligence tools are for sale or available at no cost through the open source community. They all have slightly different approaches to threat intelligence gathering:
Malware disassemblers: These tools reverse engineer malware to learn how it works and help security engineers decide how to defend against future, similar attacks.
Security information and event management (SIEM) tools: SIEM tools allow security teams to monitor the network in real time, gathering information about unusual behavior and suspicious traffic.[13]
Network traffic analysis tools: Network traffic analysis tools collect network information and record network activity to provide information that makes detecting an intrusion easier.
Threat intelligence communities and resource collections: Freely accessible websites that aggregate known indicators of compromise and community generated data about threats can be a valuable source of threat intelligence. Some of these communities support collaborative research and provide actionable advice on how to prevent or combat threats.[14]
Organizations that are aware of emerging threats and know how to avoid them can take action to prevent an attack before it happens. Gathering and reviewing threat intelligence should be part of the enterprise security strategy for every organization.

REFERENCES

1. A Cybersecurity Agenda for the 45th President. (2017, January 5). Retrieved from https://www.csis.org/news/cybersecurity-agenda-45th-president
2. An Examination of the Cybersecurity Labor Market. (n.d.). Retrieved from http://www.rand.org/content/dam/rand/pubs/research_reports/RR400/RR430/RAND_RR430.pdf

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 4.988

| Volume 4, Issue 4, April 2021 |

3. Applications Now Available for City Colleges of Chicago's New Cyber Security "Boot Camp". (2017, March 18). Retrieved from http://www.ccc.edu/news/Pages/Applications-Now-Available-for-City-Colleges-of-Chicagos-New-Cyber-Security-Boot-Camp-.aspx
4. ApprenticeshipUSA Investments. (2017, June 22). Retrieved from https://www.dol.gov/featured/apprenticeship/grants
5. Assante, M., Tobey, D. (2011, February 4). Enhancing the Cybersecurity Workforce. Retrieved from http://ieeexplore.ieee.org/document/5708280/
6. Assessment Act. Retrieved from https://www.congress.gov/bill/114th-congress/senate-bill/2007/text
7. ATE Centers. (n.d.). Retrieved from http://www.atecenters.org/
8. ATE Centers and National Science Foundation. (n.d.). ATE Centers Impact Report. Retrieved from http://www.atecenters.org/wp-content/uploads/PDF/ATEIMPACT_2016-17.pdf
9. ATE Centers and National Science Foundation. (n.d.). ATE Programs and Overview. Retrieved from http://www.atecenters.org/wp-content/uploads/2016/07/ATE_Overview_2016.pdf
10. AUSTRALIA'S CYBER SECURITY STRATEGY Enabling innovation, growth & prosperity [PDF]. (n.d.). Retrieved from https://cybersecuritystrategy.pmc.gov.au/assets/img/PMC-Cyber-Strategy.pdf
11. Baltimore Cyber Range and Cyberbit Open New Cybersecurity Training and Simulation Center. (2017, August 3). Retrieved from https://www.cyberbit.com
12. Bessen, J. (2014, August 25). Employers Aren't Just Whining – the "Skills Gap" is Real. Harvard Business Review. Retrieved from https://hbr.org/2014/08/employers-arent-just-whining-the-skills-gap-is-real
13. Best in Class Strategies for Entry-Level Employee Retention Prepared for 100K [PDF]. (2016, October). FSG Reimagining Social Change. Retrieved from https://www.100kopportunities.org/2016/10/14/best-in-class-strategies-for-entry-level-employee-retention/
14. Best Places to Work for Cyber Ninjas. (2017, May). Retrieved from https://www.sans.org/best-places-to-work-for-cyber-ninjas?ref=195285