: How can analytics and decision support improve cybersecurity?

by Daniel J. Power

Editor, DSSResources.COM

Protecting digital data and information is crucial to organizational survival. Failing to anticipate and then prevent or detect cybersecurity (or cyber-security) breaches can cause permanent harm. Analytics and decision support can protect the integrity of networks, software and data from attack, damage or unauthorized access. Decision support can help assess preventative security measures and conduct vulnerability assessment. Analytics can monitor unauthorized network access and identify suspicious network traffic patterns. Decision support tools, especially ones based upon AI and knowledge, can also monitor for phishing scams that attempt to obtain sensitive information such as usernames, passwords, and credit card details. Decision support systems can also assist in "visualizing" threat activites.

Vendors offer software to detect multiple security problems, including malware, ransomware and phishing. These threats are becoming more common and more sophisticated. In 2016, cybersecurity spending in the U.S. was estimated at $31.5 billion for tools and services, cf., IDC (Vanian, 2016). Every managers should understand these threats.

A major problem is malware. Malware is a portmanteau of the two words malicious software. It is a broad term that refers to any software that is intended to do harm. Malware includes viruses, spyware, adware, bots, bugs, rootkits, Trojan horses, keyloggers, worms, and other harmful programs. According to Norton (us.norton.com), "Malware is software that is specifically designed to gain access or damage a computer without the knowledge of the owner." Antivirus or anti-malware software uses a database of virus signatures and checks executable files for these signatures. US-CERT (2015) explains anti-malware or anti-virus software "looks for patterns based on the signatures or definitions of known malware."

The United States Federal Trade Commission (FTC) explains that "Phishing is when a scammer uses fraudulent emails or texts, or copycat websites to get you to share valuable personal information – such as account numbers, Social Security numbers, or your login IDs and passwords. Scammers use your information to steal your money or your identity or both." When a user responds to a phishing message, the malicious actor achieves their purpose of getting the victim to provide sensitive information. It is important that people learn to spot these fraudulent messages. Korolov (2016) reviews training and simulations provided by vendors to help employees recognize phishing attacks and make good decisions to avoid harmful consequences. Check some examples of phishing.

Rees et al. (2011) "describe a decision support system for calculating the uncertain risk faced by an

organization under cyber attack as a function of uncertain threat rates, countermeasure costs, and impacts on its assets. The system uses a genetic algorithm to search for the best combination of countermeasures, allowing the user to determine the preferred tradeoff between the cost of the portfolio and resulting risk."

MITRE Corporation has a Common Vulnerabilities and Exposure (CVE) index (https://cve.mitre.org/) that is the industry standard for vulnerability and exposure identifiers. Roldán-Molina et al. (2017) use the CVE index as part of a decision support system called Nexpose. MITRE's Common Vulnerabilities Scoring System (CVSS) Version 2 is also used. According to Roldán-Molina et al. (2017), "Nexpose uses CVSS metrics to compute the risk of a vulnerability on an asset. It defines different risk strategies which are based on different importance/weight of factors such as likelihood of compromise, impact of commitment, and asset
importance, when computing risk." The system is targeted for use by Chief Information Security Officers. The software is intended to support cyber risk and cyber threat
analysis of an information and communications technology infrastructure.

Guavus, a Thales company, uses AI to augment threat hunting and detection. According to its website (https://guavus.com/), "Guavus empowers security operations teams with the analytics they need for effective threat detection, hunting and remediation. Ingesting and combining security data that is separated in isolated devices and systems, Guavus correlates this information with other key data sources to get a comprehensive view of the network. Using artificial intelligence, Guavus automatically detects analogous behavior to show security analysts where threats may be imminent without overwhelming them with false positives."

According to Shackleford (2016), a number of technologies and tools have been developed for detection of security incidents including: centralized logging, network device event logging from firewalls, proxies, routers and switches, access control rules, firewall rules and authentication logging, network intrusion detection and prevention systems (IDS/IPS), host-based IDS/IPS, antivirus agents, File Integrity Monitoring (FIM) and Whitelisting, and Security Information and Event Management (SIEM).

Cybersecurity solution providers fall into niche categories, cf. Breeden (2016). Based upon visiting websites and reviews the following are interesting security tool vendors. Network security vendor BluVector (www.bluvector.io/) is using AI to sense and respond to network threats in real time. Seceon's (seceon.com) Open Threat Management Platform processes large amounts of streaming data to provide real-time visualization of networked computing assets and their interactions. Bricata (bricata.com) provides Intrusion detection. Alert Logic (alertlogic.com) Cloud is a fully managed cloud-based suite of security and compliance solutions for hybrid IT infrastructure delivered as-a-service. Local IT staff can inspect their cloud deployments for evidence of hidden threats or breaches.

Contrast Security (contrastsecurity.com) provides application security. Applications automatically detect and fix vulnerabilities, identify attacks, and defend themselves. Digital Guardian (digitalguardian.com) and enSilo (ensilo.com) provide Endpoint security. Insight Engines (insightengines.com) Cyber Security Investigator for Splunk (CSI) is optimized for cybersecurity use cases, enabling analysts to search data in Splunk to detect, investigate, and visualize cyberthreats.

Mantix4 (mantix4.com) provides threat hunting tools for use by clients, but it also takes threat hunting into the software as a service (SaaS) realm. RiskIQ (riskiq.com) Digital Footprint creates a risk reporting score. As security remediation tasks are performed, those changes impact the vulnrerability score. RiskIQ is a vulnerability management tool.

Finally, Intellicta Platform from TechDemocracy (techdemocracy.com/) offers enterprises a real-time holistic assessment of the cyber risk, security and governance (CRSG) tools to provide a consolidated view of the organization’s risk posture.

Blockchain, a distributed ledger, can also potentially improve cybersecurity. Barzilay (2017) provides three examples of leading edge uses of Blockchain. Guardtime (https://guardtime.com) uses Blockchain to detect and mitigate cyberattacks in real-time. Obsidian (https://obsidianplatform.com) is a C# blockchain that provides secure and private communications. Finally, REMME (https://remme.io) uses blockchain so businesses can authenticate users and devices without the need for a password. This Blockchain approach eliminates people from the authentication process.

Organization insiders, that is employees, are in general the biggest cyber security risk. Naive employees get duped into clicking on links, sharing sensitive information that helps "bad actors" invade a company's IT infrastructure, or otherwise compromising cybersecurity. Training is the first level of defense to counter this risk and reduce the threat. Knowledgeable, trained and vigilant employees, and documented, tested processes, are as important as technology in combating cybersecurity threats. All three approaches, people, processes, and technology, are needed to provide multi-layered security for key IT infrastructure, data, and systems. When people, processes and technology are integrated and working effectively, then threats are minimized.

More needs to be done in the areas of detecting and preventing intrusion, insider threats, collusion detection, real-time Malware detection, and security activity visualization and monitoring. A goal of security analytics should be the "capability of predicting future trends based on past and current user and attacker behavior," cf., Shackleford (2016). Finally, risk-informed decision making is a starting point for increasing cybersecurity, more analytics and decision support is part of a risk reduction response.

References

Author Unknown, "Malware," Norton, at URL https://us.norton.com/internetsecurity-malware.html

Barzilay, O., "3 Ways Blockchain Is Revolutionizing Cybersecurity," Forbes, August 21, 2017 at URL https://www.forbes.com/sites/omribarzilay/2017/08/21/3-ways-blockchain-is-revolutionizing-cybersecurity/#4a5d571f2334.

Breeden II, J., "Best security software: How 12 cutting-edge tools tackle today's threats," CSO from IDG June 5, 2018 at URL https://www.csoonline.com/article/3206685/security/best-security-software-how-cutting-edge-tools-tackle-todays-threats.html .

Carrascosa, I. P., H. K. Kalutarage, and Y. Huang (Eds.), Data Analytics and Decision Support for Cybersecurity: Trends, Methodologies and Applications, Springer, 2017 at URL https://www.springer.com/us/book/9783319594385.

Chi, J., Matching information security vulnerabilities to organizational security profiles: a genetic algorithm approach, Decision Support Systems, 41 (3) (2006) 592–603.

Combofix, How Does an Antivirus Program Work to Protect Your Computer? at URL https://combofix.org/how-does-an-antivirus-program-work.php

Federal Trade Commission (FTC), "Phishing," at https://www.consumer.ftc.gov/articles/0003-phishing

Fielder, A., E. Panaousis, P. Malacaria, C. Hankin, F. Smeraldi, "Decision support approaches for cyber security investment," Decision Support Systems 86 (2016) 13–23.

Korolov, M., "10 companies that can help you fight phishing," CSO from IDG, May 5, 2016 at URL

https://www.csoonline.com/article/3066532/phishing/10-companies-that-can-help-you-fight-phishing.html

Legg, P., "Visualizing the insider threat: Challenges and tools for identifying malicious user activity," In: IEEE Symposium on Visualization for Cyber Security, Chicago, Illinois, USA, 26 October 2015. IEEE Symposium on Visualization for Cyber Security (VizSec) 2015: IEEE Available from: http://eprints.uwe.ac.uk/27441

López-Peréz, D., A novel risk assessment and optimisation model for a multi-objective network security countermeasure selection problem, Decision Support Systems, 53 (3) (2012) 599–610.

Mell, P., K. Scarfone and S. Romanosky, "CVSS: A Complete Guide to the Common Vulnerability Scoring System Version 2.0," June 2007 at URL https://www.first.org/cvss/cvss-v2-guide.pdf

Mitre, "About CVE," Last Updated or Reviewed: January 17, 2018 at URL https://cve.mitre.org/

Phish Protection at URL https://www.phishprotection.com/

Rakes, T. R., J.K. Deane, L.P. Rees, IT Security planning under uncertainty for high-impact events, Omega: International Journal of Management Science 40 (1) (2012) 79–88.

Rees, L.P., J.K. Deane, T.R. Rakes, W.H. Baker, Decision support for cybersecurity risk planning, Decision Support Systems, 51 (3) (2011) 493–505 at URL https://www.sciencedirect.com/science/article/pii/S0167923611000728.

Roldán-Molina, G., M. Almache-Cueva, I, Yevseyeva, C, Silva-Rabadão, and V. Basto-Fernandes, "A Decision Support System for Corporations Cybersecurity Management," 2017 at URL https://www.dora.dmu.ac.uk/xmlui/bitstream/handle/2086/15670/Paper_CISTI_2017_04_04_En.pdf

Rue, R., S. Lawrence Pfleeger and D. Ortiz, "A Framework for Classifying and Comparing Models of Cyber Security Investment to Support Policy and Decision-Making," Rand Corporation 2007 Workshop on the Economics of Information Security, 2007 at URL http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.139.5962&rep=rep1&type=pdf

Shackleford, D., "Using Analytics to Predict Future Attacks and Breaches," SANS Whitepaper, January 2016 at URL https://www.sans.org/reading-room/whitepapers/analyst/analytics-predict-future-attacks-breaches-36720

Stein, G., B. Chen, A. S. Wu and K. A. Hua, "Decision tree classifier for network intrusion detection with GA-based feature selection," ACM-SE 43 Proceedings of the 43rd annual Southeast regional conference, Volume 2, March 18 - 20, 2005, Pages 136-141.

Udeagwu, C. P., S. Sotiriadis, E. Asimakopoulou, N. Bessis, and M Trovati, "Analysis of Techniques for Visualizing Security Risks and Threats," 2015 10th International Conference on P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC), Nov. 4-6, 2015 at URL https://ieeexplore.ieee.org/document/7424632/.

US-CERT, "Security Tip (ST04-005): Understanding Anti-Virus Software," Original release date: June 30, 2009, Last revised: June 05, 2015, at URL https://www.us-cert.gov/ncas/tips/ST04-005

U.S. Homeland Security, "Cybersecurity," at URL https://www.dhs.gov/topic/cybersecurity

Vanian, J., "Here's How Much Businesses Worldwide Will Spend on Cybersecurity by 2020," Fortune, October 12, 2016 at URL http://fortune.com/2016/10/12/cybersecurity-global-spending/ .

Stein et al. abstract states "Machine Learning techniques such as Genetic Algorithms and Decision Trees have been applied to the field of intrusion detection for more than a decade. Machine Learning techniques can learn normal and anomalous patterns from training data and generate classifiers that then are used to detect attacks on computer systems. In general, the input data to classifiers is in a high dimension feature space, but not all of features are relevant to the classes to be classified. In this paper, we use a genetic algorithm to select a subset of input features for

decision tree classifiers, with a goal of increasing the detection rate and decreasing the false alarm rate in network intrusion detection. We used the KDDCUP 99 data set to train and test the decision tree classifiers. The experiments show that the resulting decision trees can have better performance than those built with all available features."

Author: Daniel Power
Last update: 2018-06-26 06:28