Section 1: Week 1: Evaluate Cybersecurity

Nate Bachmeier

TIM-8301: Principals of Cybersecurity

April 5, 2020

North Central University

# Section I: Significant Problem

## What Problem Exists

Cybersecurity requires capabilities to defend against sophisticated attackers, which employs continuously evolving techniques that are funded by nation-states. These advanced persistent threats (APT) weaponize zero-day exploits, devise precise spear-phishing campaigns, and leverage vulnerabilities in unpatched software, among other strategies. As administrators operate within this ‘assume breach’ hostile environment, they need solutions that detect the onset of an attack and automatically augment the network topology. For example, a system might detect an unexpected resource is downloading sensitive information for exfiltration. That system could mitigate this traffic anomaly by provisioning firewall policies to stop the attack.

## How is this problem being addressed

One realization of this vision comes from machine learning, which provides mechanisms for rule association discovery, regression, classification, and clustering (Barua & Mondal, 2019). These primitives enable systems engineers to create adaptive technologies that react to implicit patterns versus explicit rules. For example, clustering algorithms can use the device’s open network ports to predict which other machines are most similar. An ensemble of algorithms could further enhance these clusters through regression analysis to detect traffic surges during off-hours and similar use-cases. This approach enables security teams to focus on human differentiating efforts, such as higher-level objectives and less mundane tasks.

## What challenges does this create

While machine learning appears to the naïve as science-fiction magic, it is statistics coupled with better marketing. These mindless algorithms possess a unique set of challenges where they do what we say, not necessarily what we mean (Fridman, 2017). A prerequisite to accurate forecasting requires that both the model’s specific question structure and supporting facts are extensively curated. When the training data contains missing or erroneous examples, then garbage-in/garbage-out results will surely follow (Snee, 2015). It can be nearly impossible for a team to enumerate every training scenario that occurs in the real-world. Consider how many different ways the previous dynamic firewall example could halt production environments. The organization might intentionally need to change the definition of normal by deploying new features. Meanwhile, an attacker could abuse these protections to introduce a denial of service by manipulating third-party traffic.

## Whom does it impact and why

When the network topology relies on automation to perform a task, then transparency and control are removed. This trade-off creates a double-edged sword where the administrators have fewer lower-level details but operate at higher-level business objectives. While the ability to participate in every decision is comforting, it does not scale efficiently across to large enterprise environments. However, at the same time, having black-box decision engines manipulating the state of production environments introduces risk across business continuity (Mickens, 2018). Since a sweet spot exists between extremes of fully autonomous and nothing, organizations need to determine how and where machine learning reduces explicitly overhead and increases business value.

# Section II: Cybersecurity Overview

## Goal of cybersecurity

A medical facility has a business requirement to collect private information from patients. While building a system that stores and retrieves this data is relatively trivial, several specific considerations influence the final implementation. Which users can issue queries against the datastore? What maintains the confidentiality of these records? How will auditing and compliance reporting work? Does this data have legal or regulatory implications? Answering these sorts of questions produces a model of acceptable risks and identifes of business policies that require cybersecurity enforcement. These enforcements protect the business against both negligent and malicious attacks that could harm the integrity or reputation of the brand.

## What challenges exist

A modern enterprise environment has abstract boundaries that blend across corporate resources, cloud providers, and bring your own devices (BYOD). Due to the heterogeneous nature of these devices, they span numerous operating systems and technology stacks. Given the range of device configurations, it stands to reason that a subset will contain malware or be compromised. With abstract borders, critical infrastructure such as Domain Name Services (DNS) and Lightweight Directory Access Protocol (LDAP) now might reside outside the corporate network (Paller et al., 2019). Internal applications are also migrating into the public cloud, where they encounter new attack surfaces, such as multi-tenant hardware and provider-specific integration limitations. While many of these vectors are manageable, social engineering attacks against the users remain highly effective (Hunt, 2019). Fighting phish attacks requires new technologies and protocols, as the current solutions rely on non-technical audiences to make highly technical decisions.

## Who produces these issues

The principal objective of any business is to execute on their mission in the most efficient manner possible. Delivering on that mission requires making choices between acceptable risks and desirable conveniences (Mickens, 2018) (Dai Zovi, 2019). For instance, many small to midsized business owners lack the expertise to run a domain controller or email service. Employing dedicated staff retracts from resources that could provide value differentiation towards its core competencies. Contracting a consulting firm would be less expensive but lacks the deep economy of scale discounts available from Microsoft Office365. While financial factors influence many decisions, the security and compliance teams need to assess the risks towards privacy and availability. Not all decisions originate from the leadership and often come from internal department requests. For instance, a data science team might require a Juypter Notebook server that has access to the production database. While that team has enough experience with the product to get it operational, they might lack a broader understanding of business continuity requirements. What physical host controls this instance? Does the database connection use encryption? How are backup and restore scenarios handled? Until assessing the risk to business continuity, it is not even possible to determine if a failed hard drive on the server will lose three minutes or years of productivity.

## What is the role of network security

The purpose of a computer operating system is to share a collection of resources amongst a set of processes. Each process has a security policy that dictates which files are accessible and how much capacity is available. Similarly, a network operating system expresses policies about nodes and how they interact (Azodolmolky, 2013). For instance, many wireless routers expose separate virtual networks for home and guest devices, where users of the guest network can only use X% of the bandwidth, cannot access management functionality, nor interact with the home devices. When network security is correctly leveraged, it provides primitives for containing the blast radius and preventing a cascade of failures across downstream systems.

## What is the role of assessment

The needs of an organization are dynamic, and this causes their network requirements to evolve. While meeting these product requirements, engineering teams will modify access policy or relax security controls with an expectation to revisit in future sprints. Even the static aspects of the system will eventually rot and require security patches and third-party software upgrades. Identifying these concerns requires network assessments that evaluate the current configuration against the desired configuration. When a deviation between current and desired states is detected, the business needs to create a plan and timeline to return into compliance. One of the challenges for many security professionals is understanding the balance between resolving issues and meeting existing contractual requirements (Dai Zovi, 2019). That is not to suggest deferring critical issues needlessly. However, sometimes missing a product deliverable *will* result in litigation, versus not fixing the *might* lead to an attacker compromising the email server. Unfortunately, not all risk decisions are perfect and require choosing the best of a bad hand. Mature organizations can reduce the likelihood of ending up between a rock and a hard spot by automating analysis tools, such as port scanners and patch management technologies. BY assessing the compliance of the environment on a regular cadence, issues can be detected shortly after introducing them. Often this is the least expensive point to resolve regressions as the context is still fresh and requires less investigation.

Baseline assessments are similar to unit tests, as they prevent regressions for known cases. However, like other software products, manual testing, and validation needs to discover unknown cases. Efficiently finding security defects requires a methodical approach that begins with threat modeling as a mechanism for identifying critical resources in the system and trust boundary interfaces. Since engineering resources are rarely unlimited, a prioritized list needs to consider elevation paths through the system. Afterward, using standard industry tooling like file fuzzing, and dynamic analysis monitors can confirm many specific classes of issues.

## What is the influence of team communication and culture

Traditional software organizations treat the roles and responsibilities of engineering and quality assurance personnel differently. Allspaw and Hammond (2009) dispute this approach because this encourages throwing code over the wall, and assuming someone else will handle it. Instead, they recommend a combined engineering solution where an individual team owns the entire lifecycle of the feature. Since responsibility resides on the team, there is more comradery around delivering a quality solution and involving everyone in decisions. Dai Zovi (2019) asks why the same unification does not happen with security engineering? Stating that companies like Square have been highly successful at creating a cultural shift that causes communication to freely flows between roles. This approach makes sense as those personal connections, encourage engineers to raise questions early, and seek confirmation on solutions. Reciprocally security team members that actively participate in the engineering cycle organizations know what changes are coming and how to prepare for them. Alternatively, waiting until release sign-off to raise issues turns into technical discussions into political battles that no one wins.

It can also be critical for success that teams understand the criticality of a defect in the context of the product. Moss (2019) describes how Chinese software companies are concerned about distributed denial of service (DDoS) attacks more than identity theft because farms sell their identity for 3,000 yen. While both scenarios are concerning, it needs to be the decision of the business what risks are acceptable (Krebs, 2019). If the security team communicates the risks, and the business is unwilling or unable to remediate the issue, there is little value in continuing the fight. Instead, the focus should transition towards mitigations to reducing the blast impact. Hunt (2019) provides an example where aspects of an electric vehicle could are remotely controllable through a mobile app that uses the VIN as the password. In this scenario, the impact was critical; however, fully mitigating the issue would be expensive. The vehicle manufacture could begin with disabling features, with security and privacy implications like GPS tracking, remote start, and remote unlock. Next, an authentication service could associate a username and password with the VIN to control API access. Additional aspects of the would need to be flushed out, but at least provides options for the business to evaluate and prioritize.

# References

Allspaw, & Hammond. (2009). Dev & Ops Cooperation at Flickr - 10 Deploys per day.

Azodolmolky, A. (2013). *Software Defined Networking with OpenFlow.*

Barua, H., & Mondal, K. (2019). A Comprehensive Survey on Cloud Data Mining (CDM) Frameworks and Algorithms. *CM Computing Surveys. Sep2019, Vol. 52 Issue 5, p1-62. 62p*, 1-62.

Dai Zovi, D. (2019). Every Security Team is a Software Team Now. *Blackhat USA 2019.*

Fridman, L. (2017, January 16). *MIT 6.S094: Introduction to Deep Learning and Self-Driving Cars*.

Hunt, T. (2019). Keynote: Hack to the Future. *NDC Conference.*

Krebs. (2019). Keynote by Christopher Krebs, Director, Cybersecurity and Infrastructure Security Agency. *ICCE 2019.*

Krebs, C. (2019, April 23). ICCE 2019 - Keynote by Christopher Krebs, Director, Cybersecurity and Infrastructure Security Agency.

Mickens, J. (2018, August 16). *Why Do Keynote Speakers Keep Suggesting That Improving Security Is Possible?* Retrieved from YouTube: https://www.youtube.com/watch?v=ajGX7odA87k

Moss, J. (2019). Blackhat USA Opening.

Paller et al. (2019, March 7). The Five Most Dangerous New Attack Techniques and How to Counter Them. *RSA Conference.*

Snee, R. (2015). Practical Approach to Data Mining: I Have All These Data; Now What Should I Do? *Quality Engineering Volume 27*, 477-487.