Cybernomics – Changing the Economics of Cyber Defense

Snehal Antani
Ravi Iyer

Cyber defense is on an unsustainable trajectory. Thanks to freely distributed and automated attack tools, cheap labor in countries from which attacks are launched, and stolen computing resources assembled into botnets, the cost of cyber-attack is estimated to be one-tenth to one-one hundredth the total cost of cyber defense. Despite the increased investment in cyber defense, breaches are still occurring, and organizations are still subjected to financial and reputational risk, moreover, cybersecurity has moved beyond a corporate issue, and is now a national security matter. The emerging national urgency to protect us from cyber-attacks will transform into a movement that will fundamentally alter the economics of the problem. Cyber will become the '*Space Race*' of our generation, and victory will require tremendous collaboration across government, academia, and the private sector.

There are six primary areas of focus needed to shift the economics of cyber defense:

1. ORGANIZATIONS MUST SHIFT LEFT—CATCH SECURITY VULNERABILITIES EARLIER IN THE TECHNOLOGY LIFECYCLE.

Shifting left incorporates the following four key concepts: First is Continuous Delivery, which promotes early and continuous software testing including static and dynamic security analysis tools; Second is Architecture-as-Code, which eliminates *snowflake* systems—manually configured system components that are unique in some way ± through standardization and automation; Third is End-to End Instrumentation connecting the dots across software development, systems deployment, and systems operations; and Fourth is a Continuous Improvement Process that reviews and prioritizes the resolution of Reliability, Availability, Serviceability, and Security (RASS) issues identified by operations. A litmus test for success is when leaders can convey in real time: who are their best/worst developers, best/worst contractors, which developers/contractors are struggling to write secure code. If a developer or contractor is sent off to learn how

Snehal Antani serves as the SVP/GM of Business Analytics & IoT for Splunk. He joined Splunk in 2015 as CTO, where he helped drive the long term vision and strategy for the company across Business Analytics and the Internet of Things. Prior to Splunk, he served as CIO of GE Capital's Distribution Finance business, as well as Chief Architect for GE Capital North America. In 2016, Antani was recognized as a Premier 100 award winner by Computerworld, for the digital transformation he drove while at GE, evolving IT from a back-office function to a core part of the value delivered to customers. Snehal started his career as a software engineer at IBM, where his work led to 11 patents spanning systems optimization, data processing, and large-scale transaction systems. Snehal holds a Bachelor's Degree in Computer Science from Purdue University, and a Master's Degree in Computer Science from Rensselaer Polytechnic Institute (RPI).

to write secure software, IT leaders should see a quantifiable return on that investment of time. That level of data-driven transparency ensures that technology systems are shipped when ready, and not restricted to a date; more importantly, those technology systems are secure by design, versus discovering and trying to remediate issues later in the delivery lifecycle.

2. ORGANIZATIONS MUST HAVE THE RIGHT OPERATIONAL MODEL IN PLACE TO EFFECTIVELY DETECT AND REMEDIATE A VULNERABILITY OR BREACH.

The optimal strategy driving your Security Operations Center (SOC) should be governed by analytics, including critical elements such as quick detection, thorough investigation, and rapid remediation. In addition, the processes that govern how security analysts operate must be frictionless.

Quick Detection relies on the ability to monitor complex IT and security systems for security threats in real-time while providing security practitioners visual insights into that data. The capability to correlate events in near real time while measuring against baseline relationships is key. This enables quick detection by practitioners by identifying previously unknown relationships in messages or events generated by devices, systems or applications, based on characteristics such as the source, target, and protocol or event type.

Thorough investigation requires the ability to correlate real-time data with historical data to examine and determine how harmful, how widespread and how deep within the organization an attack can penetrate. This requires validating against well-known threat intelligence to gain additional context of attacker's tactics, techniques, and procedures (TTPs). Mechanisms that speed up the investigation portion of an alert are critical to fast and thorough security investigations.

Ravi Iyer is the Senior Director, Security Product Management, in Splunk's–Security Markets group. Prior to Splunk, Ravi has held various Engineering, Product Management and Product Marketing positions at startups and blue chip companies. Most recently as SVP of Products at Vorstack/BrightPoint (acquired by ServiceNow), VP of PM/PMM at WhiteHat Security and as Sr. Director of PM at Good Technology (acquired by RIM). Ravi started his career as an engineer for network management products at AT&T–Bell Labs. Following that he was the lead engineer in the Directory Services (LDAP & DNS) group for multiple Solaris releases following which he went on to lead Product Management for Solaris OS at Sun Microsystems. Ravi holds a Bachelor's Degree from Bangalore University and an MS in Computer Science from University of Missouri.

Rapid Response requires customizable workflows that integrate the detection and investigation phases of security operations with the response phase. Typically, this involves providing integration with ticketing systems that assign tasks and monitor the completion of these tasks. Many organizations are embracing automation within their SOC to respond to threats quicker than ever before.

3. ORGANIZATIONS MUST EMPLOY SECURITY ANALYTICS TO MAXIMIZE THREAT HUNTING.

The maturation of machine learning technologies and their ability to detect security threats has significantly enhanced the capabilities of security analysts. When analysts monitor the behavior of users, hosts, and networks, unsupervised machine learning can produce high fidelity alerts for investigation, which reduces the noisy but benign alerts that plague the daily life of security analysts. A tiered strategy is optimal here, where classic machine learning models first identify anomalies, and advanced data science techniques, as well as security threat expertise, are later applied to generate threat models that yield high-fidelity threats.

Employing such data science techniques make it possible to identify remote account takeovers, attacker dwell time, lateral movement with compromised credentials and advanced persistent threats (APT's) such as data exfiltration with malware.

Advanced user-behavior analytics solutions provide a significant additional capability that includes peer group analytics, workflows that enable analyst investigations (hunter-centric), and kill-chain visualization.

4. EXPEDITE INCIDENT RESPONSE BY INTRODUCING AUTOMATION.

By our count in the field, the security vendor portfolio of most organizations is typically made up of more than seventy technologies—an astonishing number. To optimize the investments you are making in these technologies, diverse domain expertise is required across every team. But because we see such a skills shortage in cyber security, the ability to make well-informed decisions quickly remains the biggest and most expensive challenge facing security teams today.

When large teams of different skill sets are brought together to investigate, observe and characterize a threat, the challenge of short-term containment and mitigation combined with long-term policy modification can pose significant challenges. This unprecedented complexity grinds down the efficiency of security operations.

Cyber will become the *Space Race* of our generation, and victory will require tremendous collaboration across government, academia, and the private sector.

Automating many of these functions can significantly boost operational effectiveness. Efficient security operations typically implement a playbook approach for investigation and remediation of various types of alerts. Analogous to reflexes in the human body, operational effectiveness can be dramatically increased by automating these playbooks, with scale varying depending on the maturity level of your SOC. Organizations lower on the maturity curve may employ only the most basic of security automation, while more mature security operations may employ complex orchestration that forms the basis of multi-step investigation and remediation.

5. ORGANIZATIONS MUST ACCELERATE ANALYST PRODUCTIVITY.

As mentioned above, the security skills gap is a very real thing. Corporations and government agencies struggle mightily to fill cyber defender jobs. In addition to requiring tremendous technical breadth across a myriad of topics including networking, operating systems, and the latest attack vectors, cyber defenders spend the bulk of their time investigating issues across a number of emerging security technologies, which analysts must continue to learn and master.

Each of these technologies has nuanced search languages that require specialized training, which further leads to a scarcity of trained talent and a longer ramp to productivity. To combat all of this, organizations are turning to natural language and advanced visualizations to help accelerate the ramp to productivity for a cyber defender.

Natural language search allows security analysts to ask questions that are more intuitive, e.g., *How many users logged in yesterday,* which is then dynamically transformed into an optimized search and executed against the data. The insights derived can be conveyed through advanced visualizations and data storytelling techniques, enabling the analyst to quickly dissect the data and come up with the next question to ask. Decreasing the required training time to search data and time to synthesize search results accelerates the ramp-to-productivity, enabling organizations to have access to a larger talent pool of cyber defenders.

6. ORGANIZATIONS MUST BECOME A MOVING TARGET TO DISORIENT AND DECEIVE ATTACKERS.

An attacker spends most of their time in reconnaissance mode—studying the network topology and systems architecture of the target to identify angles of attack. There are two key emerging technologies that disrupt an attacker's ability to conduct reconnaissance: shape-shifting networks and deception techniques.

The static nature of systems enables an attacker to attack at their leisure. Shape-shifting networks leverage software-defined networking to dynamically change the network configuration of a system, decreasing the window of attack and increasing the cost to probe. Deception techniques mimic the target system, creating the illusion that an attacker has found an exploited an angle of attack.

Shape-shifting networks, combined with deception techniques, can serve as a powerful solution for dramatically increasing the cost of attack.

Shape-shifting networks, combined with deception techniques, can serve as a powerful solution for dramatically increasing the cost of attack, making it economically unfeasible for a hacker to spend precious time to exploit. This truly turns the economics of a hack in its head.

CONCLUSION

Clearly, organizations have strategies available to them today to shift the balance of cyber economics in their favor. New trends in automation, machine learning, and analytics have created a golden opportunity for organizations to flip Cybernomics in a way that has never been possible before, but changing the economics goes beyond emerging technology, where ecosystem and collaboration across ecosystem members are critical. As organizations take a look at their security landscape in 2017 and beyond, it will be paramount to determine if the strategies outlined above are being embraced to shift the balance of cost from defender to hacker. Moreover, embracing these concepts enables

organizations to have the agility of a start-up, with the resources of an enterprise. These organizations can rapidly create new capabilities faster than their competitors or adversaries, and take advantage of opportunities that help drive mission success.