# Adopting a "Detect to Protect" Philosophy to Safeguard our Democracy

## Preventing Election Hacking remains unachievable; however, identifying unauthorized access reaches an unprecedented level of detection and adversarial attribution.

*By: Brent Cobb, President, Cybraics*

The Department of Homeland Security's "Detect to Protect," (D2P) programs for chemical, biological, radiological, nuclear and explosive threats, should also be applied to cybersecurity. The D2P philosophy focuses on the understanding that these threats are potentially devastating, where prevention alone is insufficient to protect the population, minimize damage, and save lives. Early detection is the key to prevention. While compromise of an election system may not result in loss of life, the manipulation of our democratic process has the potential to have far more significant and broad-reaching long-term implications.

### The Failure of Traditional Security Solutions

The vast majority of cybersecurity solutions focus on preventing threats. These solutions range from traditional firewalls, intrusion prevention systems (IPS), and virus protection to more sophisticated approaches such as sandboxing, end-point protection, and next-gen firewall solutions. While these solutions are helpful, and serve as a basic security mechanism to prevent the large numbers of unsophisticated attacks, they have repeatedly proven to be ineffective at preventing breaches. The challenge with these solutions is that they rely on rules and signatures, requiring prior knowledge of what to block.

In recent years, security organizations have deployed a SIEM (Security Information and Event Management) as a centralized way to collect and organize security logs. Similar to traditional security systems, the SIEM is still rule and signature-based, flagging events that match particular known signatures or actions which violate predefined rules based on past threats. A SIEM creates thousands of alerts per month, which can take an analyst 20 to 30 minutes per alert to triage. This is further exacerbated by requiring four to eight hours to conduct in depth review of each alert. These unintelligent machines often have an average false positive rate of 50% or more, requiring either an in increase in staff or acknowledgement that some threats will remain undetected. Security Operations Centers (SOC) are inundated with alerts and are under-resourced to prioritize them or review them efficiently.

While there has been tremendous innovation in the security community, the black hat coalition continues to innovate at an accelerated pace, constantly devising ways to bypass security measures and gain unauthorized access to systems. As evidenced by recent breaches seen at organizations from Equifax to Yahoo to Oracle, and government organizations such as OPM, the FBI, and CIA, even the best defensive security posture has been shown to be penetrable.

## Hacking the Electoral

The obvious reason for hacking the electoral is to manipulate the outcome of an election and erode the confidence of the election process. There is a strong belief that because we have not adopted Internet-based voting systems, we remain relatively immune to such manipulation. It is true that no widespread vote tampering has been proven, but these hypotheses are based on what is known. Similar to the limitations of traditional security systems, we only know what we know. If an adversary has devised a method to compromise these systems without our knowledge and detection, it is reasonable to assume that we may be unaware of a compromise.

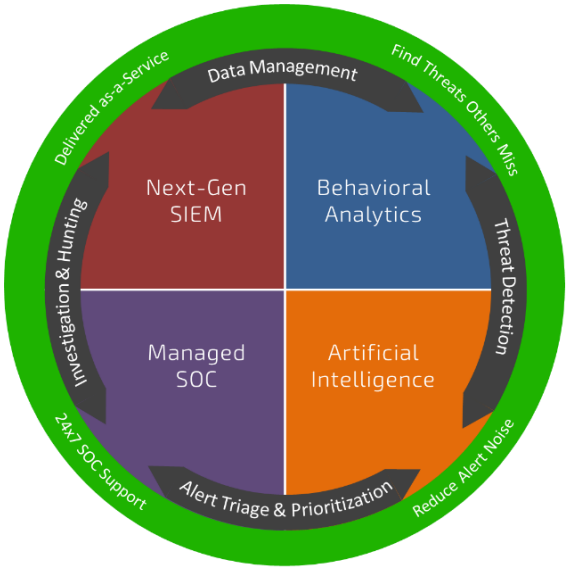
Election manipulation may sensationalize well in the press, but a more immediately lucrative target for adversaries is not in the manipulation of an election but obtaining the personal information of registered voters. With over 200 million registered voters in the US, and the increasing adoption of online voter registration, these systems are a prime target for adversaries. Similar to other online systems, these voter registration systems get protected by traditional security measures which are largely rule- and signature-based, and have proven ineffective at preventing breaches.

## Detection Leads to Protection

Most breaches are a culmination of a sophisticated sequence of attacks consisting of multiple tactics executed over an extended period of time. According to research conducted by Verizon, Ponemon and others, adversaries have been inside environments for an extended period before a breach is discovered. Traditional security tools can only find what they know, which means that to create new "protection rules" a security incident must occur first. While traditional security tools and the SIEM are inadequate in addressing the challenges of detecting these discreet behaviors, the lack of alternative solutions perpetuates the deployment of these tools.


To address this, a collective best-of-class technology from across big data, Artificial Intelligence (AI), analytics, and cloud is needed. This comprehensive collection of technology should combine multiple modes of machine learning (ML) with an advanced AI engine to discover and prioritize behavioral anomalies and integrate human context through a SOC to provide real-time scalability of security analysts. The Machine Learning, which is based on sophisticated algorithms, analyzes data from across multiple sources, implementing a combination of user and network behavior analysis techniques to detect discreet patterns of misbehavior. By adding an artifical intelligence (AI) engine that learns from security analysts and across environments, the system is able to apply human context to interpret those patterns and detect unknown, advanced and insider threats as well as targeted attacks. Detection of the adversaries' discreet behaviors after they have bypassed traditional security and penetrated the environment acts as an early warning system, allowing the discovery of malicious activity before a breach or damage is caused. The integration of a managed Security Operations Center (SOC) completes the system, creating a revolutionary new "machine + human" approach to security that combines the speed and analytical power of the most sophisticated machine learning and AI with the intuition and experience of cyber analysts and threat hunters.

Delivering this system through a secure cloud provides economies of scale which allow each state to individually acquire these capabilities for a fraction of the cost of building it themselves, while also potentially replacing legacy systems, such as SIEMs, or MSSPs that implement more rudimentary threat hunting mechanisms prone to human error. Furthermore, the anonymized nature of the system allows anonymous sharing of threat patterns between states, accelerating the systems ability to learn and protect.




This unique approach brings an all-new arsenal to security teams, allowing them to deliver on the promise of protecting their organization, customers, and data in ways never before possible with a traditional security solution. By detecting threats to the environment, decisive action can be taken to remediate the threat and protect the organization. The data gathered can also often provide significant forensic information, allowing authorities to proactively investigate the source of the threat.

## Conclusion

The increasing sophistication of cyber threats has revealed the real limitations of traditional security monitoring and response technologies. Organizations must be able to discover compromised users, gain insight into malicious insiders, support advanced threat hunting efforts, and efficiently investigate incidents. Failing to do so allows for a level of uncertainty and risk that most organizations find undesirable, and is certainly unacceptable when dealing with the integrity of our democracy. The modern cyber machinery is rife with shortcomings. By marrying the speed, efficiency, and accuracy of an AI engine to the intuition and expertise of a SOC analyst, billions of events can be evaluated timely to provide the most effective recommendations for human review. In turn, this drastically reduces the false positive rate and detects threats undetectable by traditional security solutions or humans alone.