Protecting election systems requires protecting the State, Local, Territorial & Tribal (SLTT) networks on which they run on. This requires a broad-based view of threat intelligence and a holistic approach that combines proactive prevention with detection and response. In this white paper, we will explore how SLTT organizations can combine the detection and response capabilities provided by the Albert IDS sensors and monitoring service with a threat intelligence-driven proteciton service to bolster the security of SLTT networks and election systems.

A HOLISTIC INTELLIGENCE-DRIVEN APPROACH TO PROTECTING ELECTION SYSTEMS AND GOVERNMENT NETWORKS

Cyber attacks have become a “new norm” in our everyday life. While our “connected world” has allowed businesses (and us as a society) to evolve and innovate faster than ever before, this connectivity has also created a very real danger to our daily life – cyber warfare. Never before have we seen such insidious and pervasive attacks on the very way we live. This is evident in the continued cyber attacks on our election systems.

ELECTION SYSTEM ATTACKS

In July of 2018, twelve Russian military intelligence agents from a group known as Fancy Bear, were indicted as part of the 2016 Democratic National Committee Email leak. These emails were subsequently published by DCLeaks in June and July 2016 and by WikiLeaks on July 22, 2016, ahead of the 2016 Democratic National Convention.

These emails were leaked with the expressed purpose of preventing Hillary Clinton from winning the election. In 2019, the U.S. Senate, along with multiple U.S. Intelligence agencies, released a report on Russian Active Measures Campaign and Interference in the 2016 U.S. Election. During its investigation, the committee identified multiple scans and reconnaissance attacks against the networks and systems of state, local, tribal, and territorial (SLTT) networks, attempting to gain access or map systems, “with the sole purpose of undermining the integrity of elections and American confidence in democracy.” Additionally, according to the report, Russia employed a social media disinformation campaign aimed at sowing discord.

These attacks shine a light on a very real threat to our election voting systems, the networks on which they run, and the individuals that use them - whether public officials, civic employees, volunteers or voting citizens. One only need look to the 2020 election to see the next target.

SLTT NETWORKS AS AN ELECTION SYSTEM ATTACK VECTOR

Our election and voting systems are not wholly autonomous, meaning that they connect into and are run on, SLTT government networks. As these networks extend into various functional aspects of the IT infrastructure, they therefore broaden the attack surface for threat actors.

> “At the end of the day, attacks on our election systems are nothing more or less, than cyber terrorism”

Simply put, cyber attacks can target any and all entry points into the network as a whole, in an attempt to gain access to and disrupt our election systems, specifically. These attacks may include:

- Scanning and reconnaissance efforts in an attempt to discover vulnerabilities into a network as a whole, and election systems specifically
- Email phishing attacks meant to compromise and leverage a single user or host in order to gain access and propagate throughout the network
- Social engineering attacks meant to spread disinformation, discord, or gain access
- Botnet and DDoS attacks, designed to bring down systems during critical times, such as during polling hours.
- Various botnet and malware attacks that exploit unpatched system vulnerabilities, meant to cripple networks, or hide injection attempts

Key to understanding these threats is the understanding that they will be concerted and strategic, across multiple vectors, utilizing various means. Threat actors (including highly organized state-sponsored actors) succeed by knowing that they need not alter voting results across a nation, but that by attacking and infecting a relatively small number of systems they can create doubt regarding the legitimacy of an election in its entirety – causing fear and mistrust and sowing the seeds of political unrest. At the end of the day, this is nothing more or less than cyber terrorism.

PROTECTING SLTT NETWORKS WITH ALBERT SENSORS AND MS-ISAC & EI-ISAC THREAT INTELLIGENCE

> More SLTT networks are adopting Albert IDS sensors & managed detection & response service provided by DHS & CIS

The U.S. Department of Homeland Security (DHS) has been on the leading edge of delivering broad protections that secure our nation from the many threats faced on multiple fronts. One such threat is cybersecurity. Working in conjunction with Center for Internet Security (CIS), DHS offers Albert Sensors to SLLT organizations. As an extension of DHS’ Einstein program, the Albert Sensor is a network Intrusion Detection System (IDS) designed to provide network security alerts when malicious activity is detected on SLTT networks, including election agency networks. The Albert Sensor is powered by threat intelligence from DHS and CIS, which operates the Multi-State Information Sharing & Analysis Center (MS-ISAC) and the Elections Infrastructure ISAC (EI-ISAC).

Once deployed on the network perimeter, typically outside the firewall, the Albert Sensor uses IDS signatures and behavior-based detection to identify malicious or potentially harmful network activity. The Albert sensor also has historical analysis capabilities, with the ability to correlate threat data against historical logs. The threat intelligence that powers Albert is tailored to protect SLTT environments and includes threat intelligence from DHS, MS-ISAC, and election-specific threat intelligence from EI-ISAC.

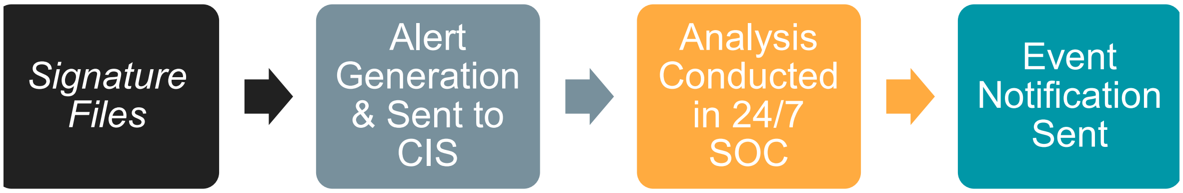
The Albert sensor is deployed as part of a managed security service that combines the technology with analysis, monitoring and incident response expertise, provided by the MS-ISAC and EI-ISAC security operations centers (SOCs). Services include 24/7 SOC monitoring, threat notifications, incident response assistance, analysis and vulnerability analysis, updated IDS signatures, and MS-ISAC and EI-ISAC delivered actionable threat intelligence feeds to member organizations.

ALBERT IS A DETECTION & MONITORING SERVICE

Fundamentally, the combination of the Albert sensor and SOC services from CIS is a detection and monitoring solution, or in today's vernacular, managed detection and response (MDR). The Albert IDS sensor is a passive sensor that collects network data. When an alert is verified as actionable, CIS sends an event notification and signature updates, providing agencies the information they need to begin taking countermeasures. This is illustrated in Figure 1.

DETECTING ATTACKS IS IMPORTANT, BUT IT'S ALSO CRITICAL TO PREVENT THREATS THROUGH PROACTIVE BLOCKING OF MALICIOUS AND UNWANTED NETWORK CONNECTIONS.

FIGURE 1.


Signature Files
Alert Generation & Sent to CIS
Analysis Conducted in 24/7 SOC
Event Notification Sent

SOURCE: CIS

The Albert Sensor and overarching Albert Service, provide an important layer of protection for SLTT networks but Albert alone is insufficient to protect SLTT and election networks from cyber threats.

THE NEED FOR THREAT INTELLIGENCE-DRIVEN PROTECTION

While detecting attacks and malicious activity on SLTT and election networks is important, it's equally important to prevent threats through proactive blocking of malicious and unwanted network connections. It's also critical that government and election-specific threat intelligence is combined with a broader-based view of threat intelligence.

IT'S CRITICAL THAT GOVERNMENT AND ELECTION-SPECIFIC THREAT INTELLIGENCE IS AUGMENTED WITH A BROADER-BASED VIEW OF THREAT INTELLIGENCE.

In fact, to truly combat today's cyber threats, more SLTT entities are increasingly adopting threat intelligence as a critical component of their security strategy. These organizations are incorporating broad-based threat intelligence spanning commercial, open source, industry, and government sources such as the aforementioned MS-ISAC (government specific) and EI-ISAC (election specific) threat intelligence. In addition to providing a much needed, broader view of the threat landscape, threat intelligence also delivers valuable contextual information that can improve an SLTT organization's ability to prevent, detect, and rapidly respond to cyber threats. This includes information regarding threat actor tactics, techniques, procedures, and the resources (i.e. IP addresses, domains, and other indicators) from which they attack.

CORE ELEMENTS OF THREAT INTELLIGENCE-DRIVEN PROTECTION

To implement a threat intelligence-driven protection approach, SLTT organizations must take three steps:

- Aggregate threat intelligence from multiple external sources
- Integrate threat intelligence from existing security controls and non-security systems into security efforts
- Act on threat intelligence proactively to protect the network

STEP 1: AGGREGATE THREAT INTELLIGENCE FROM MULTIPLE SOURCES

While government and election-specific threat intelligence is critical to protecting SLTT networks, this intelligence alone is insufficient. To protect against today's cyber threats requires a broad based view of threat intelligence that spans multiple, high fidelity sources including

- Commercial threat intelligence
- Open source threat intelligence (OSINT) from sources
- Government threat intelligence such as DHS' Automated Indicator Sharing (AIS) and Cyber Information Sharing and Collaboration Program (CISCP)
- Industry threat intelligence from ISACs like MS-ISAC, EI-ISAC, FS-ISAC, and others

AGGREGATING, INTEGRATING, AND ACTING ON THREAT INTELLIGENCE ARE THE THREE CORE ELEMENTS OF THREAT INTELLIGENCE-DRIVEN PROTECTION

An important consideration in aggregating threat intelligence is managing it. Centralizing and automating the aggregation and management of threat intelligence feeds is critical, particularly given the highly dynamic nature of threat feeds. Progressive users of threat intelligence have deployed threat intelligence platforms (TIPs) to solve the aggregation and management challenge as well as to apply analytics. The challenge with TIPs, however, is that they require significant resources (budget & people) to acquire and operate.

STEP 2: INTEGRATE THREAT INTELLIGENCE INTO SECURITY EFFORTS TO IMPROVE PROTECTION

Once you have aggregated threat intelligence the next step is integrating it into your security operations with the goal of improving protection. This includes the threat intelligence an organization has aggregated as well as the threat intelligence that is being produced by other security systems like SIEMs and IDS and non-security systems like help desk systems. Similar to aggregation, automation is critical to efficiently integrate threat intelligence into security operations. This requires the use of open application programming interfaces (APIs) and the use of open standards like STIX/TAXII to connect and exchange threat intelligence among systems. Security Orchestration & Automated Response (SOAR) solutions are being used by progressive, well resourced security organizations to enable the automated integration and exchange of threat intelligence between multiple security controls.

STEP 3: ACT ON THREAT INTELLIGENCE IN REAL TIME

> THE CRITICAL THIRD STEP OF THREAT INTELLGENCE-DRIVEN PROTECTION, IS TO TAKE ACTION WITH THREAT INTELLIGENCE IN REAL TIME TO PROTECT YOUR NETWORK.

The critical third step of implementing threat intelligence-driven protection, is to take action with threat intelligence in real time to protect your network. This means using threat intelligence proactively to prevent (block) malicious and unwanted network connections. When it comes to taking action, a common challenge organizations face is the ability to integrate third-party threat intelligence into existing network security controls like next-generation firewalls (NGFWs). Simply put, due to performance issues and a lack of incentive (i.e. reliance on their own proprietary threat intelligence), existing network security controls have limited abilities to integrating and taking action using third-party threat intelligence.

Fortunately, the emergence of threat intelligence gateways (TIGs) technology has served to alleviate the challenges of taking action using threat intelligence in real time “on the wire.” TIGs are purpose-built to filter network traffic based on a massive volumes of third-party, threat intelligence indicators. TIGs not only alleviate the threat intelligence-capacity limitations of NGFWs but also offer easier and simpler management of dynamic blacklists, access control lists, and enforcement policies. An important point is that TIGs complement NGFWs providing another layer of protection and in many instances, the deployment of TIGs yields benefits for NGFW deployments by reducing the load on NGFWs.

SUMMARY

Protecting SLTT networks and election systems requires a proactive and concerted, intelligence-driven effort. This effort must incorporate a broad-based view of threat intelligence and a holistic approach that combines proactive prevention, detection and response. Combining Albert IDS sensors and the Albert service with the threat intelligence-driven protection approach outlined in this white paper will help SLTT organizations improve the security of both their networks and election systems.

ABOUT BANDURA CYBER

Bandura Cyber helps organizations protect their networks by making threat intelligence actionable in an easy, open, automated, and scalable way. Our cloud-based Threat Intelligence Protection platform aggregates threat intelligence from multiple sources, integrates threat intelligence from any source in real time, and takes action on threat intelligence at near line speed. Organizations are using Bandura Cyber’s solution to strengthen network protection, reduce manual staff workload and increase ROI on existing security investments including threat intelligence and next-generation firewalls.

RESOURCES

To learn more about the Bandura Cyber Threat Intelligence Protection platform visit www.banduracyber.com and download our Solution Brief and our white paper Operationalizing Threat Intelligence: An In-Depth Guide to Threat Intelligence Gateways.