Enhancing Election Infrastructure Security With Splunk

A National Security Challenge

Cyberthreats remain one of the most strategic risks for the United States and its long-term national security. Nation states and independent threat actors have increasingly grown the sophistication and frequency of their attacks over the last several years. These actors have been deploying and using their advanced cyber capabilities to undermine U.S. critical infrastructure, including threatening American democracy through attempts to manipulate elections, according to the Department of Homeland Security.

Since the 2016 U.S. presidential election, multiple U.S. intelligence agency assessments have concluded that a foreign nation state sought to interfere with the election and influence its outcome. In January 2017, as a response to this interference and broader cyberthreat activity from multiple external aggressors, the Secretary of Homeland Security designated election infrastructure as a sub-sector within the Government Facilities Critical Infrastructure Sector.

Election Infrastructure as Critical Infrastructure

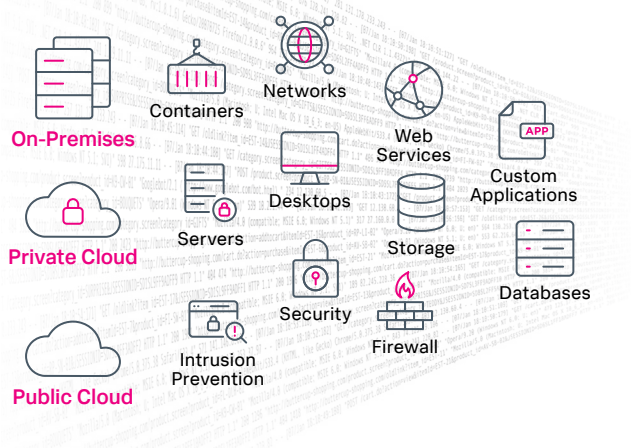
The U.S. Department of Homeland Security secretary's designation described election critical infrastructure as a diverse set of assets, systems and networks that are critical to the administration of the election process. Protecting this infrastructure introduces complex challenges for election officials and places new burdens on budgets that are often already tight.

In recognition of these challenges, the FY2018 Omnibus Appropriations Bill made $380 million in grants available to states to support election security. These grants, in part, are focused on raising the security of election assets, systems and networks, and also specify provisions for cybersecurity training for state and local election officials.

Gaining visibility into the security posture of these assets, systems and networks is often difficult, even for smaller municipalities. Diverse distributed infrastructure, often common in large local

Fast time to insight – Raising Visibility into Election Infrastructure Security

Universal, vendor agnostic platform for analysis



splunk>

Key Insights

- Vulnerability Status
- Privileged Account Activity
- Deviations from Baseline
- Spurious Authentications
- Near Real-Time Visibility

governments, presents an even greater challenge for understanding vulnerabilities, threats and exposures. States and election officials require a prescriptive solution to rapidly address these challenges and the threat actors that exploit them.

State election officials require:

- Highly-scalable monitoring and audit logging of activity across election assets, systems, and networks to enable detection of attacks and automated threat analysis
- Consolidated, vendor-agnostic visibility across assets, systems, and networks from a single screen
- Applied Machine Learning for analytic baselining of activity across the environment and automated identification of deviations from the baseline
- Near real-time insights into system vulnerabilities and exposures to drive prioritization of patching and mitigation
- Technical training that enables staff to effectively leverage the solution to improve the overall security of the election infrastructure

Enter Splunk

Splunk® is helping states address these challenges by providing a vendor agnostic package of analytics and visualizations, built on Splunk® Enterprise software and driven by machine learning. These capabilities enable quick-start operationalization of data analysis related to election assets, systems and networks — including system vulnerabilities, network activity and audit of privileged account accesses.

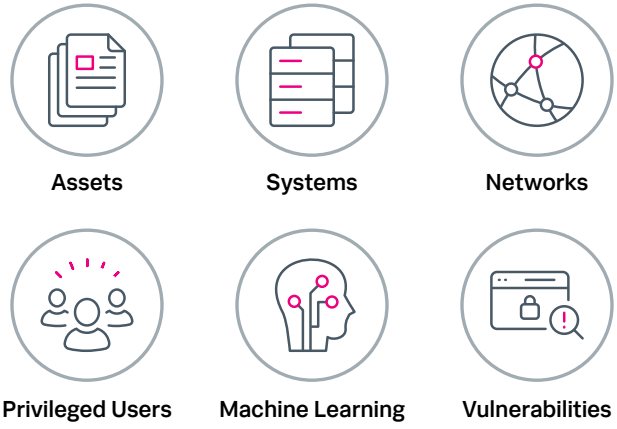
Many of the processes and methodologies applied in this package are already employed at the federal level as part of Splunk's foundational support for the Department of Homeland Security's (DHS) Continuous Diagnostics and Mitigation (CDM) program for Information Security Continuous Monitoring (ISCM). Through this package of pre-built analytics and training, focused on cybersecurity best practices, state election officials now have a direct and rapidly deployable path to raise the security of their election infrastructure in alignment with the U.S. Election Assistance Commission grant guidance.

Anticipated Impact

States and municipalities who deploy this package of capabilities and training should expect a solution that rapidly delivers insights focused on the fundamentals required to improve the cybersecurity of election infrastructure.

Visibility into vulnerabilities, privileged account actions and indications of intrusion, as they are identified across the environment, will aid in fostering a proactive culture oriented around near real-time awareness and risk mitigation. The native machine learning-driven analysis, baselining, alerting, and automation capabilities of Splunk Enterprise will support proactive defense and reduce the workload on election officials' security teams.

Training packaged with the solution will ensure that security teams protecting election infrastructure have the skills necessary to effectively leverage these new capabilities to detect and respond to threats, understand where vulnerabilities have been identified, and proactively drive risk mitigation — raising the overall security posture of election-critical infrastructure.



Want to learn more about how Splunk solutions can help secure election infrastructure? Contact us to learn more.

20-15098-SPLK-Enhancing Election Infrastructure Security-102-TB