Leveraging Splunk to Operationalize CISA Directives

Background

The Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA) issues binding operational and emergency directives for Federal Executive Civilian agencies. CISA directives provide compulsory cybersecurity guidance to improve the risk posture of the Federal Government's Information Technology (IT) infrastructure. The directives are based on observed risks and active threats and are therefore highly applicable to Federal IT contractors who are responsible for protecting government data. State and local agencies, the Department of Defense, and other organizations considering cybersecurity best-practices should also implement CISA's guidance to raise their overall security posture.

Three Key Challenges to Responding Effectively

In the real-world, implementation of CISA guidance can be challenging at times. In some cases, agencies may experience difficulty when implementing business processes needed to operationalize directives guidance. In other cases, agencies may lack the agility required to adapt to the constant change across their environments and struggle to continuously monitor their posture. Lastly, maintaining consolidated visibility across an agency's software and hardware assets often presents an ongoing challenge, even before considering the specifics of any guidance from CISA.

Difficulty implementing business processes

CISA directives require agencies to stand-up business processes to analyze and address identified issues. These new processes often require new data collection, investigation, analysis, and reporting actions. These actions may require multiple stakeholders, several discussions, and agreement to execute; all of which delay the implementation of directive guidance.

Once a process is accepted, individual stakeholders may require unique analysis and reporting to perform their actions, which adds complexity. Agencies need a common platform that streamlines new process stand-up and execution to meet directive guidance.

Lack of agility adjusting to constant change

Agencies must also grapple with constant changes within their IT environments to address and maintain directive guidance. Constant change across diverse IT environments makes analysis and monitoring challenging in the best of times. The inherent diversity of vendors and data sources present further adds to the complexity. As changes occur, it is also essential that the environments are continuously monitored to ensure that the risk posture is not weakened. Legacy monitoring tools rely on rigid data schemas that must be refactored after each environment change. Agency leaders need a dynamic solution to improve their agility in responding to changing environment variables and to provide insight into their risk, relevant to the threats and vulnerabilities captured in the CISA directives.

Maintaining consolidated visibility across assets

Agencies must monitor and assess CISA directive guidance across their entire portfolio of software and hardware assets. In many cases, agencies' asset monitoring is divided across a series of point-solutions. Both the overall scope of data involved, and the siloed nature of point-solutions adds complexity and latency to the goal of asset visibility. Agencies need immediate, consolidated visibility into asset and risk posture to proactively mitigate threats and vulnerabilities.

Splunk Approach

Splunk® worked closely with several customers responding to CISA Emergency Directive 19-01. During these interactions, customers highlighted a need for a better approach for monitoring past CISA directives. In response to these requests, Splunk has developed a turnkey solution to help agencies address the challenges associated with these past directives.

The Splunk for CISA Directives solution provides a pre-packaged capability that streamlines the operationalization of the technical guidance from multiple, past CISA directives. The solution provides an out-of-the-box, prescriptive framework for continuous monitoring and extensible analytics that directly align with the guidance from CISA while delivering a vendor-agnostic, consolidated view of agency IT asset security posture.

Enabling streamlined, unified business processes

The solution, built on Splunk Enterprise, enables agencies to streamline processes by providing **investigate > monitor > analyze > act** capabilities within a single pane of glass. The solution minimizes process latency while providing an extensible platform for IT, security operations, and compliance teams to collaborate on proactive monitoring and remediating CISA findings.

Gaining agility around constant change

Built on Splunk Enterprise, the Splunk for CISA Directives solution provides a vendor-agnostic platform for agencies. This platform enables agility through automatic data normalization -- providing a Rosetta stone that standardizes data from multi-vendor environments. This normalization ensures that the analytics, reports, and dashboards in the solution remain up-to-date, even when software and hardware changes occur in the environment.

The solution includes more than twenty automated alerts, tailored to directive guidance, to highlight negative trends or deviations as they occur. The solution enables agencies with automation and greater agility to overcome analysis and monitoring challenges driven by constant change.

Providing consolidated visibility across assets

The Splunk for CISA Directives solution provides consolidated visibility of agency hardware and software assets, regardless of size or technology diversity. At the same time, Splunk's vendor agnostic approach enables a unified, single-pane view that consolidates point-solution data from across the enterprise to provide operators with efficiency through enhanced visibility. By improving visibility, the Splunk for CISA Directives solution enables agencies to understand their real-time risk posture and rapidly respond to issues.

Anticipated Impact

1. **Streamlined, prescriptive implementation for continuous monitoring of past CISA directives**
   - Pre-built monitoring of CISA directed guidance
   - Gain shared capability for data-driven operations and decision making
2. **Enhanced agility to change as dynamically as your environment does**
   - Extensible, flexible, vendor-agnostic solution for automation and continuous monitoring of threats and risks in CISA guidance
3. **Consolidated visibility of assets, regardless of organizational size or scale**
   - Efficiency and visibility; a single pane of glass view into the near real-time risk posture of hardware and software assets

Learn more about Splunk Public Sector Use Cases. Email us to learn more about Splunk for CISA Directives Solution.

splunk>

Learn more: www.splunk.com/asksales

www.splunk.com