# Beyond Security Events and Compliance **With Splunk**

splunk>
turn data into doing™

The Splunk® platform is designed to investigate, monitor, analyze and act on data at any scale, from any source over any time period. We call this the Data-to-Everything™ Platform, which removes the barriers between data and action, so organizations — regardless of size or business — have the freedom to deliver meaningful outcomes across their entire organization.

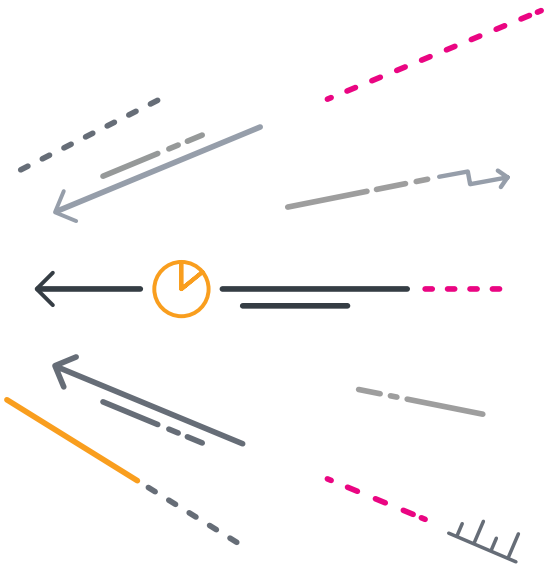
Splunk's unique approach to data has empowered companies to improve service levels, reduce operations costs, mitigate risk, enhance DevOps collaboration and create new product and service offerings.

Data is at the center of our ever-changing world, which brings both challenges and opportunities. These challenges are only going to grow as we enter a digital age with the complexity of cloud migration, networks moving from 4G to 5G, the number of connected devices nears 80 billion and automation becomes more integrated into our lives.

One of the most important — and often overlooked — resources that organizations can tap into to solve these challenges is data. The companies that are able to harness the power of these transformations and the data they create are going to be more efficient, profitable, innovative and ultimately more secure.

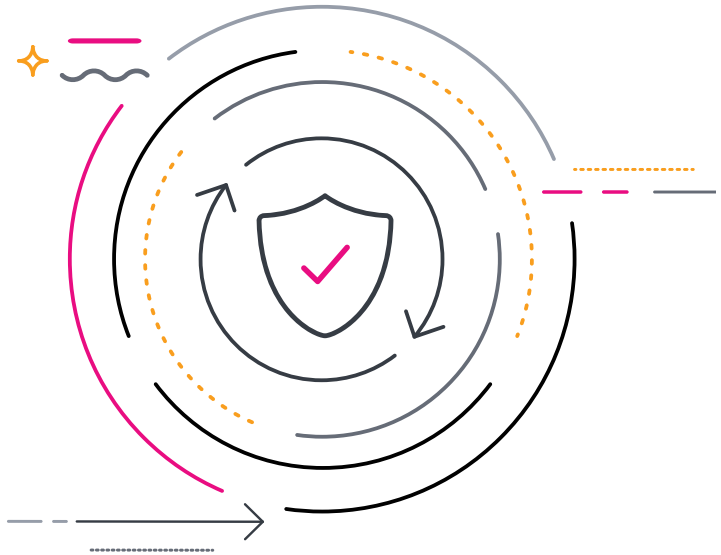
Specifically for electric utilities, Splunk is known for security events, as it came to industry attention with the expanded requirements of CIP version 5 in the years leading up to the standard's enforcement beginning in 2016.

This paper covers how Splunk increases the effectiveness of security programs, enables compliance programs and processes outside of the narrow applications of CIP-005 and CIP-007, and is a powerful tool for IT, OT and business operations groups.



# Table of Contents





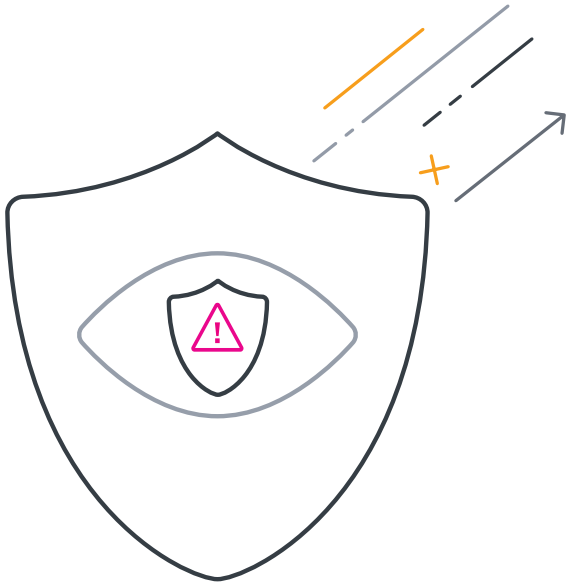
# Security Beyond Compliance, Enhancing Security and Visibility

Owners and operators in the North American electric grid are facing more challenges from industry-targeted cyberattacks. They are also dealing with wider threats, like ransomware and data theft, that are hitting global organizations of all sizes. This is all happening while the power industry trends towards increased computer automation of larger fleets of both transmission and distribution connected generation, energy storage, power flow optimization equipment and more granular energy market services.

Control rooms around the world are improving the visibility of the grid for better and timelier situational awareness, but the "invisible infrastructure" — the machines, people and processes that make modern control systems possible — might still be managed using paradigms from the last millennium. This leads to a host of challenges such as:

- Lack of visibility has long been known as a key factor in poor decision-making
- High-profile security failures like the infamous 2014 movie studio hack generated millions of alarms that were never seen by security analysts before it was too late
- The 2015 Ukraine blackout attack had for-profit attackers embedded in the control system networks for months before handing access to state actors
- The 2017 WannaCry panic found many utilities asking how many vulnerable systems they had and where they might be, with frighteningly limited answers as to where vulnerable Windows software was embedded
- Well-resourced APTs have the time and patience to transform minor security vulnerabilities into wide compromises and know the value of critical infrastructure

The expansion of controls that provide real-time access to larger transmission substations — even if they have been secured under the Critical Infrastructure Protection (CIP) standard and have the attention of engineering and technical resources due to their focal role in the operation of the Bulk Electric System (BES) — may result in an even greater attack surface to defend, even if the individual systems do not pose a great risk, as they are tied into Advanced Distribution Management Systems (ADMS) or Distributed Energy Resource Management Systems (DERMS).



# Operations Beyond Compliance

The Splunk platform can be used to power operations and shared business problems, including the duplication of labor to document processes instead of building the required documentation out of the workflows that get the job done.

Communication paths rarely fail without notice and will exhibit degradation long before they become unusable. Maintenance processes and automation can fail months before preventable damage occurs to equipment or data. Visibility isn't only to keep attackers out; it's also for looking inward and improving day-to-day operations and business processes.

Existing industry strategies often consolidate monitoring and management in narrowly scoped solutions like vendor-proprietary management software, or try to extend SCADA systems to cover telemetered data outside the traditional power operations and engineering requirements. While highly capable and well tested within their domains, real-time SCADA, historical data archiving, and monolithic vendor tools present the risk of over-extending critical software, processes, and staff to meet demands that poorly matched to their core functionality.

Splunk not only has greater adaptability to large-scale machine data analysis, but offers opportunities for cleaner integration of data from disparate departments, and as many owners and operators are finding the renewable energy space, frequently disparate responsible stakeholders spread across multiple independent companies.

# Building on CIP

## NERC, in brief

The North American Electric Reliability Council, originally established by the US FERC in 1968 (as the National Electric Reliability Council) and reformed in 2006 is the Electric Reliability Organization for the continental United States, Canada and portions of Baja California, Mexico. As a recognized international regulatory body, NERC has the authority to create and enforce regulations for the power system owners and operators that serve more than 400 million people.

The standards NERC has created cover responsibilities from generation scheduling to keeping trees and other vegetation in check and includes Critical Infrastructure Protection (CIP). CIP requires subject entities to secure and account for electronic devices that maintain the operation of the Bulk Electric System (BES), the electrical generators and high-voltage transmission grid that provides the power that modern cities and industries depend on.

First enforced in 2007 and significantly revised to meet a changing understanding of effective security processes and the threats faced by the BES, CIP includes:

| | | |
|---|---|---|
| CIP-002-5.1a | Cyber Security — BES Cyber System Categorization | 12/27/2016 |
| CIP-003-8 | Cyber Security — Security Management Controls | 4/1/2020 |
| CIP-004-6 | Cyber Security — Personnel & Training | 7/1/2016 |
| CIP-005-5 | Cyber Security — Electronic Security Perimeter(s) | 7/1/2016 |
| CIP-006-6 | Cyber Security — Physical Security of BES Cyber-Systems | 7/1/2016 |
| CIP-007-6 | Cyber Security — System Security Management | 7/1/2016 |
| CIP-008-5 | Cyber Security — Incident Reporting and Response Planning | 7/1/2016 |
| CIP-009-6 | Cyber Security — Recovery Plans for BES Cyber-Systems | 7/1/2016 |
| CIP-010-2 | Cyber Security — Configuration Change Management and Vulnerability Assessments | 7/1/2016 |
| CIP-011-2 | Cyber Security — Information Protection | 7/1/2016 |
| CIP-014-2 | Physical Security | 10/2/2015 |

*(Additional standards for Supply Chain Management to be enforced starting October 1st, 2020.)*

Forward-thinking organizations understand that CIP provides a necessary floor for security, but is only the beginning for creating a security posture to protect their assets, facilities and the electric grid at large. The threat of fines for gross violations makes noncompliance expensive, but failures to maintain reliable and secure operations result in far greater losses in revenue, recovery costs, and detracts from life-safety equipment and critical infrastructure.

## CIP-002 and CIP-003

| | |
|---|---|
| CIP-002-5.1a<br>BES Cyber System Categorization | To identify and categorize BES Cyber Systems and their associated BES Cyber Asset … |
| CIP-003-8<br>Security Management Controls | To specify consistent and sustainable security management controls … |

Splunk may not have a one-button solution for performing CIP-002, but the resultant categorizations and BES Cyber System names, impacts and associated Electronic Security Perimeters (ESPs) can be loaded from a variety of external results of those processes. Not only can this clearly display compliance information for reporting and dashboards, but it can also be tied with in-depth analysis for people and automation.

For larger utilities that may have BES Cyber Systems across dozens of substations or generation ties, this clarity can help separate what might be minor low impact device alerts from critical medium impact alerts with required response times.

## CIP-004

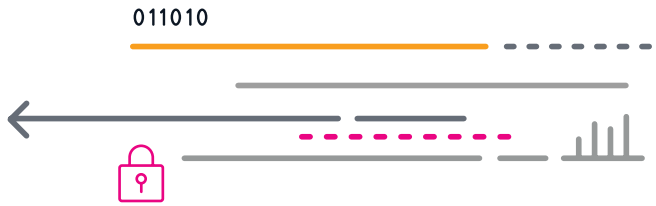
| | |
|---|---|
| CIP-004-6<br>Personnel & Training | … personnel risk assessment, training, and security awareness in support of protecting BES Cyber-Systems |

CIP-004 programs are heavily influenced by human resources and other business administration teams and interface with a lot of people problems in a unique way compared to most computer security standards. Splunk's Data-to-Everything Platform enables organizations to bring together the results of purely people processes, HR databases, and learning management systems to track and present compliance targets holistically.

Splunk is designed to ingest disparate data sets and answer questions like, "Were any of the people with recorded interactive logins within an ESP not on the list of authorized individuals as was current at that time?"

CIP-004-6 R4 quarterly access reviews are frequently one of the largest time costs and common sources of human errors for the responsible individuals in CIP programs

The same automation that facilitates such access reviews can also populate compliance metrics for managers and compliance personnel, including those who would not normally have access to BES Cyber System Information repositories, and may even be leveraged for reporting purposes entirely outside of CIP.



## CIP-005

| | |
|---|---|
| CIP-005-5<br>Electronic Security Perimeters | To manage electronic access to BES Cyber Systems by specifying a controlled Electronic Security Perimeter |

Aggregating firewall and IDS/IPS feeds is only the start of what Splunk can provide to utility data network operations.

The most recent revision of CIP-005 added additional requirements for detecting potentially malicious traffic. While Intrusion Detection/Prevention Systems only perform traffic inspection, Splunk can analyze events with a wider perspective to emphasize novel threats and tie in vulnerability alerts from MITRE or ES-ISAC to correlate network event data with global threat awareness, giving Network Operations better insights and automatically cataloging data for compliance reporting.

Integrating advanced query capabilities can provide reporting on potential ESP traffic flow problems, verify that Remote Access is compliant with CIP-005 R2 encryption and Intermediate System requirements and provide all of that as scheduled or on-demand evidence.

## CIP-006

| | |
|---|---|
| CIP-006-6<br>Physical Security of BES Cyber-Systems | To manage physical access to Bulk Electric System (BES) Cyber Systems by specifying a physical security plan … |

As with many of the purpose-driven processes and systems that implement CIP-004 controls, Splunk offers rich query and reporting opportunities that are not available in the many vendor-proprietary solutions common in the Access Control market. Beyond tracking which badge was used where, Splunk can integrate multiple access control vendors' logging to combine PSP and Visitor Management reporting, alerting for CIP and non-CIP facilities or use orchestration to tie links to video monitoring applications or external contact information for regional emergency services or law enforcement.

## CIP-007

| | |
|---|---|
| CIP-007-6<br>System Security Management | To manage system security by specifying select technical, operational, and procedural requirements … |

While detective controls around access logs and malware alerts may be what drives the adoption of Splunk within the power industry, those are only a small fraction of event data that can be used for awareness and analysis. The tremendous volumes of machine data that modern computers and even simple purpose-built substation automation equipment can produce are often too vast for administrators and managers to handle, and much of it is ignored by necessity.

Advanced data analytics and orchestration like Phantom playbooks provide the ability to for limited staff to cope with an increasingly computerized world and can help alleviate the labor-intense creation of evidence associated with CIP-007 R2 patch management, change management related security control testing and deviations from the ports and services associated with a Cyber System's baseline.

## CIP-008

| | |
|---|---|
| CIP-008-5<br>Incident Reporting and Response Planning | To mitigate the risk to the reliable operation of the BES as the result of a Cyber Security Incident by specifying incident response requirements. |

With event data for CIP-005 and CIP-007 compliance, Splunk starts off as a leading detective control, investigative tool and data preservation mechanism for CIP Incident Response.

Splunk can include CVE or ES-ISAC alerts to associate with potentially correlated events, and integrating Splunk to a corporate or cloud instance with BESCI obfuscation can bring more resources and visibility to any investigation.

Phantom can initiate automatic evidence gathering or common investigative actions to give analysts more situational awareness and a head start on incident response.

## CIP-009

| | |
|---|---|
| CIP-009-6<br>Recovery Plans for BES Cyber-Systems | To recover reliability functions performed by BES Cyber Systems by specifying recovery plan requirements … |

Automated backup failure notification and integrity checking may seem like a problem from the 1990s, but lack of visibility in IT infrastructure automation (like backups or data archiving) is a recurring theme in data loss incidents. In ICS and SCADA environments when systems might run for years without direct human interaction, instrumentation is even more vital.

Not only does Splunk provide its rich analysis and archiving capabilities, but properly implemented, Splunk can produce the evidence necessary for compliance as part of normal operations, including the retention of security data in recoveries and tracking real recovery events. Modern orchestration tools like Splunk Phantom can even perform automated test plans.

## CIP-010

| | |
|---|---|
| CIP-010-2<br>Configuration Change Management and Vulnerability Assessments | To prevent and detect unauthorized changes to BES Cyber Systems by specifying configuration change management and vulnerability assessment requirements … |

Alongside patch management, baseline management is one of the most labor-intensive technical controls required by CIP. Integrating Splunk with CIP-010 R1 Baseline state via databases, applications or even simple spreadsheets provides enormous savings in time and effort for analysts and support staff by effectively automating and centralizing the tracking of system elements required by CIP-010.

For high impact systems, baseline monitoring with live event data can track to verify that changes on QA match with Production and turn that tracking into evidence. Splunk Phantom playbooks can be built into change control as repeatable and testable steps in configuration management or software deployment.

For organizations with many transient cyber assets or removable media, deep analysis of network or device-level events like USB plug-ins can be transformed from labor-intensive to build-once-and-apply-everywhere.

## CIP-011

| | |
|---|---|
| CIP-011-2<br>Information Protection | To prevent unauthorized access to BES Cyber System Information … |

BES Cyber System Information (BESCI) includes much of the data that a Splunk index for CIP environments considers key fields. While Splunk includes the necessary access controls to serve as a repository for BES Cyber System Information, it can also transform that data, which has profound implications for integrating Splunk with tools and services outside of CIP.

Combinations of BESCI criteria on event data can be avoided by rewriting new events for a corporate or cloud index, and critical obfuscated CIP events forwarded to Splunk Enterprise for enterprise-wide analysis and centralized alerting. The same effort building detective controls and analytics can benefit Low Impact or No Impact Transmission, Generation or even Distribution operations, IT environments and future fleets of Distributed Energy Resources or AMI. (See reference to BESCI Practices)

## CIP-013

| | |
|---|---|
| CIP-013-1 | Verification of software integrity and authenticity |

Splunk's support of software integrity features, app review process, vulnerability and patch alerting and management not only enables compliance for the Splunk technology stack but creates the same rich analysis and reporting for potentially dangerous software, as it can with approved baseline configuration management.

# BES Cyber System Information Practices

CIP programs create barriers to sharing technology stacks between OT and IT business units, because of concerns that CIP-011 and CIP-004 requirements will expand CIP programs well outside the operational business.

Splunk can meet the CIP-011 requirements for the protection of BES Cyber System Information, but that perceived barrier remains. Using obfuscating event-creation integrated Splunk indices allows an enterprise to scale their data analysis and awareness capabilities while keeping CIP tightly corralled. This corralling allows for the integration of cloud services or mobile apps — which are normally out of the question as part of an OT strategy because of the CIP barrier— opening up capabilities that are often dismissed as unavailable or considered cost-prohibitive in CIP environments.

# Broadening Tools and Workflows for CIP Low Impact

The enforcement of the CIP Low Impact requirements is now on the horizon for owners and operators both large and small. While these substations and generation facilities may not need to meet the same stringent requirements as more critical infrastructure, the security and operational capabilities of advanced data analytics and orchestration can be extended to such goals as:

- Tracking transient cyber assets at field locations
- Tracking vendor or other third-party remote access
- Aggregate and normalized alerting
- Verifying unapproved communication patterns are not present

# Integrating IT and OT Workflows

While security is a necessary starting point, major organizations use Splunk for their business operations from software development and testing to troubleshooting to engineering operations and customer data analysis, and so can utilities.

A common inefficiency in tools comes from their implementation for a set of narrow goals — only a small fraction of the tool's capabilities are used, and processes have to be designed around that limited utility. Splunk was conceived as a tool for distilling large volumes of machine-generated data into meaningful information for programmatic actions as well as human analysis and understanding, not just a SIEM.

In both IT and OT environments, the lack of revenue-driven impetus to assign scarce experts to analyze and act on the firehose of low-impact informational events, intermittent warnings and periodic but recoverable errors leaves the valuable insights submerged inside that data flow out of reach. This results in minor problems getting left unfixed for months or years until they snowball into major problems, a lack of predicted failure mitigation and heavily siloed technology solutions providing value to small teams.

The same teams that are doing security event monitoring are often the primary administrators and support staff for operational environments. Expanding Splunk's capability gives these teams the intelligence and automation to respond to daily tasks and troubleshooting while providing managers and compliance analysts access to the same sources without creating additional reporting solely for compliance.

# Learn more.

Technologies can be used to address immediate challenges like complying with security regulation, positioning organizations of all sizes and more. But decisions are often made by focusing on direct requirements and total cost of ownership.

This is why it is important for organizations to know that a software solution can address multiple use cases simultaneously before they make an investment. Some software provides capabilities that do more than meet requirements for a specific task, offering transformative power to meet the next set of goals as well.

The Splunk platform is built for problems beyond proving compliance. For organizations that use the software as a SIEM solution, they may find incredible opportunities to leverage Splunk to improve their security posture and reporting and to answer operational challenges in an increasingly data-driven world.

Ready to learn more about how Splunk can help your organization be more secure and achieve compliance mandates? Speak with an expert or download the app on Splunkbase.



20-14512-SPLK-Beyond Security Events and Compliance with Splunk-108-EB

splunk> turn data into doing™