Privacy Impact Assessment
for
Splunk

12/12/2019

System/Business Owner

Juned Shaikh

Reviewing Official

Charles Cutshall
Chief Privacy Officer
Commodity Futures Trading Commission

I. SYSTEM OVERVIEW

1) Describe the purpose of the system/collection:

The Splunk solution will function as a Security Information and Event Management (SIEM) tool for the CFTC Enterprise Security Operations Center (eSOC). Splunk will be used to collect, index, and search machine log files from across the CFTC network. It will generate automated alerts based upon events within various indexed datasets; allow automated and ad hoc searching of CFTC log files; and create greater visibility into the day-to-day security condition of the CFTC network.

The system collects log data from the public facing CFTC internet domain, such as IP address, that when combined with other information could identify an individual. It also collects log data from CFTC information technology (IT) devices and systems, which includes information that is linked or linkable to CFTC employees and contractors.

CFTC eSOC analysts use log data produced by these sources to detect, correlate, and respond to potential malicious activity (such as malware) on CFTC IT devices and networks. Splunk correlates alerts and events from eSOC security tools and allows for quicker time-to-detection, incident response, and mitigation of malicious activity. Information will be maintained for security event monitoring in near real-time and historical data will be retained for correlation of current and past malicious activity on CFTC IT devices and networks.

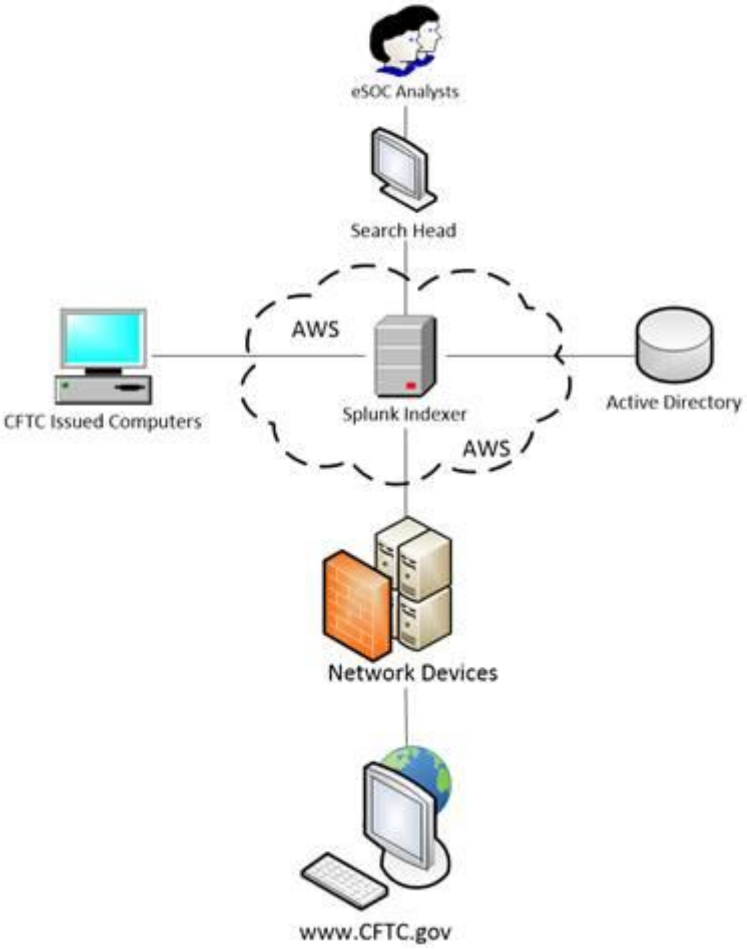
2) Provide a data map or model illustrating how information is structured or is processed by the system throughout its life cycle.

Splunk collects, uses, and maintains the following data from CFTC issued devices, network devices, and Active Directory.

- CFTC issued Devices:
  - Windows – Application logs, Security Logs and System logs
  - Linux – Linux system logs

- Network Devices:
  - Syslog data

- Active Directory:
  - Windows event logs



II. AUTHORITY AND PURPOSE

1) What is the legal authority to collect, use, maintain, and share information in the system?

The Federal Information and Security Modernization Act (FISMA) provides authority to collect and use this information to ensure the security of CFTC issued devices and IT systems.

III. INFORMATION TYPES

1) What information will be collected, maintained, used, and/or disseminated?

Identifying Numbers	
☐ Social Security Number	☐ Truncated or Partial Social Security Number
☐ Driver's License Number	☐ License Plate Number
☐ Patient ID Number	☐ File/Case ID Number
☐ Student ID Number	☐ Health Plan Beneficiary Number
☐ Passport Number	☐ Federal Student Aid Number

☐ Employee Identification Number	☐ Taxpayer Identification Number
☐ Professional License Number	☐ Legal Entity Identifier
☐ Credit/Debit Card Number	☐ National Futures Association ID
☐ Personal Bank Account Number	☐ Other ID if it can be traced back to an individual
☐ Personal Device Identifiers or Serial Numbers	
Contact Information	
☐ Personal Mobile Number	☐ Business Phone Number
☐ Personal E-mail Address	☐ Business E-mail Address
☐ Home Phone Number	☐ Personal or Business Fax Number
☐ Home Mailing Address	☐ Business Mailing Address
Sole Proprietors	
☐ Business Taxpayer Identification Number	☐ Business Mailing Address
☐ Business Credit Card Number	☐ Business Phone or Fax Number
☐ Business Bank Account Number	☐ Business Mobile Numbers
☐ Business Device identifiers or Serial Numbers	
Biographical Information	
☐ Name	☐ Gender
☐ Date of Birth	☐ City or County of Birth
☐ Country of Birth	☐ Zip Code
☐ Citizenship	☐ Military Service Information
☐ Spouse Information	☐ Academic Transcript
☐ Group/Org. Membership	☐ Resume or Curriculum Vitae
☐ Location Data (e.g., GPS)	☐ Nationality
☐ Employment Information	☐ Marital Status
☐ Mother's Maiden Name	☐ Children Information
Biometrics/Distinguishing Features/Characteristics	
☐ Fingerprints	☐ Height
☐ Retina/Iris Scans	☐ Voice/Audio Recording
☐ Hair Color	☐ Eye Color
☐ Video Recording	☐ Photos
☐ Weight	☐ Signatures
Active Directory/Device Information	
☒ IP Address	☒ MAC Address
☒ CFTC Asset Number	☒ Device Identifiers or Serial Numbers
☒ Username	

IV. COLLECTING INFORMATION

1) How is the information in this system collected?

Splunk collects information in the following ways:

a) Log data from CFTC endpoints (workstations, laptops, servers) is created locally on devices and forwarded to Splunk.

b) Network and Network Security devices (Switches, Routers, Firewalls, IPS, Web Proxy, etc.) send data to a Splunk via Syslog protocol over the CFTC network. The data is then parsed into a standard format which Splunk uses to index and display events.

V. INFORMATION USE

1) Will information in the system be retrieved using one or more of the data elements listed in Section III?

Yes. User name login credentials, device hostnames, and IP addresses that can be linked to or identity an individual are retrieved from event logs by the Splunk collector (in the case of firewalls or other security devices), or from the Splunk Universal Forwarder (in the case of event logs from desktops and servers). These data feeds are then sent to the Splunk user interface as alerts. Typically these alerts do not contain personally identifiable information (PII), but an eSOC analyst (dependent on permissions) would be able to further investigate the log information from the security device or system that generated the event that contains information that can identify an individual.

2) If the information in the system is retrieved using one or more of the identifiers, what CFTC System of Records Notice (SORN) covers the information?

SORN CFTC-35, *General Information Technology Records* (81 FR 67327) covers the information in this system.

VI. ACCESS & SHARING

1) With which internal CFTC Offices or Divisions is the information shared? For each Office or Division, what information is shared and for what purpose?

The information is typically not shared outside of the eSOC. However, when responding to an incident, it may be necessary to share information with other CFTC offices included the CFTC Privacy Office, Office of General Counsel, or Office of Inspector General.

2) With which internal CFTC Offices or Divisions is the information shared? For each Office or Division, what information is shared and for what purpose?

The information is typically not shared outside of the eSOC. However, when responding to an incident, it may be necessary to share information with other CFTC offices included the CFTC Privacy Office, Office of General Counsel, or Office of Inspector General.

3) How is the information shared internally?

If information needs to be shared in response to an incident, the information will be shared on a case-by case basis. Individuals with a need to know may receive copies of specific log files, summary reports including the information, or access to dashboards.

4) With which external organization(s) is the information shared?

   The information may need to be reported to the Department of Homeland Security (DHS) US-CERT as required by FISMA.

5) How is the information shared externally?

   If required to be reported to DHS US-CERT, the information will be shared on a case-by case basis and in a secure format.

VII. TRANSPARENCY

1) How are individuals notified as to how their information will be collected, used, and/or shared within this system?

   The CFTC webpage Privacy Policy describes the information collected by the CFTC on its public facing webpages. Internally, when a CFTC staff member logs into the CFTC network, they are presented with a warning screen that they must read and accept that details the CFTC's need to monitor network activity for security purposes.

2) Is a SORN is required? If so, explain how the use of the information in this system is limited to the use specified in the SORN?

   Yes, a SORN is required as referenced in Section V above (SORN CFTC-35, *General Information Technology Records* (81 FR 67327)). The information is limited to the uses described in the SORN by policy rules assigned to specific roles and responsibilities, and access privileges granted to eSOC analysts based on their role in analyzing the information.

VIII. INDIVIDUAL PARTICIPATION

1) Is the information collected directly from the individual?

   No. The information is collected from logs from CFTC IT devices and systems.

2) Is the collection mandatory or voluntary? If voluntary, what opportunities do the individuals have to decline to provide information?

   The collection of the information is mandatory to ensure the security of CFTC IT devices and systems.

3) Do individuals have an opportunity to consent to a particular use of the information? If so, how do they provide consent for a particular use?

An individual does not have an opportunity to consent to a particular use. The collection of the information is necessary and required to be able to properly protect CFTC IT systems. Individuals accessing external webpages are notified of the collection via the CFTC website Privacy Policy, and internal network users are presented with a banner each time they log on to the CFTC network that indicates monitoring and collection activities are required for security purposes.

IX. DATA MINIMIZATION

1) What steps were taken to minimize the collection of PII in the system?

Log information is collected and correlated based on specific criteria to determine if an activity warrants further review or investigation. The system is designed to only process information necessary to determine whether an activity requires further review.

X. DATA QUALITY AND INTEGRITY

1) How is data quality ensured throughout the information lifecycle and business processes associated with the use of the information?

☒ Cross referencing data entries with other systems
☐ Third party data verification
☐ Data taken directly from individuals
☐ Character limits on text submissions
☐ Numerical restrictions in text boxes
☐ Other:

XI. RETENTION

1) What are the retention periods for the information?

Per the National Archives and Records Administration approved records retention schedule, GRS 3.2, item 030, records in the system are temporary. CFTC maintains the records for one year.

XII. SECURITY

1) What types of administrative safeguards protect the information?
   ☒ Contingency Plan
   ☒ User manuals for the system
   ☒ Rules of Behavior
   ☒ Non-Disclosure or other contractual agreement
   ☐ Other:

2) What types of physical safeguards protect the information?
   ☐ Guards
   ☒ Identification Badges
   ☐ Biometric
   ☐ Cameras
   ☒ Physically secured space with need to know access
   ☐ Other:

3) What types of technical safeguards protect the information?
   ☒ User Identification
   ☒ Firewall
   ☒ Virtual Private Network (VPN)
   ☒ PIV Cards
   ☒ Passwords
   ☒ Encryption
   ☐ De-Identification
   ☐ Anonymization
   ☐ Other:

4) What monitoring, recording, and auditing safeguards are in place to prevent or detect unauthorized access or inappropriate use of the information?

   Splunk logs system activity to detect unauthorized access or inappropriate use of the information.

5) Is this system hosted by a Cloud Service Provider (CSP)? Yes.
   a. If yes, which one? Amazon Web Services Commercial East
   b. If yes, has the system obtained a FedRAMP Authorization? Yes.

XIII. TRAINING

1) What privacy training is provided to users of the system?

   All CFTC staff take annual Privacy and Security training. eSOC staff are required to sign privileged rules of behavior and also take additional incident handling training.