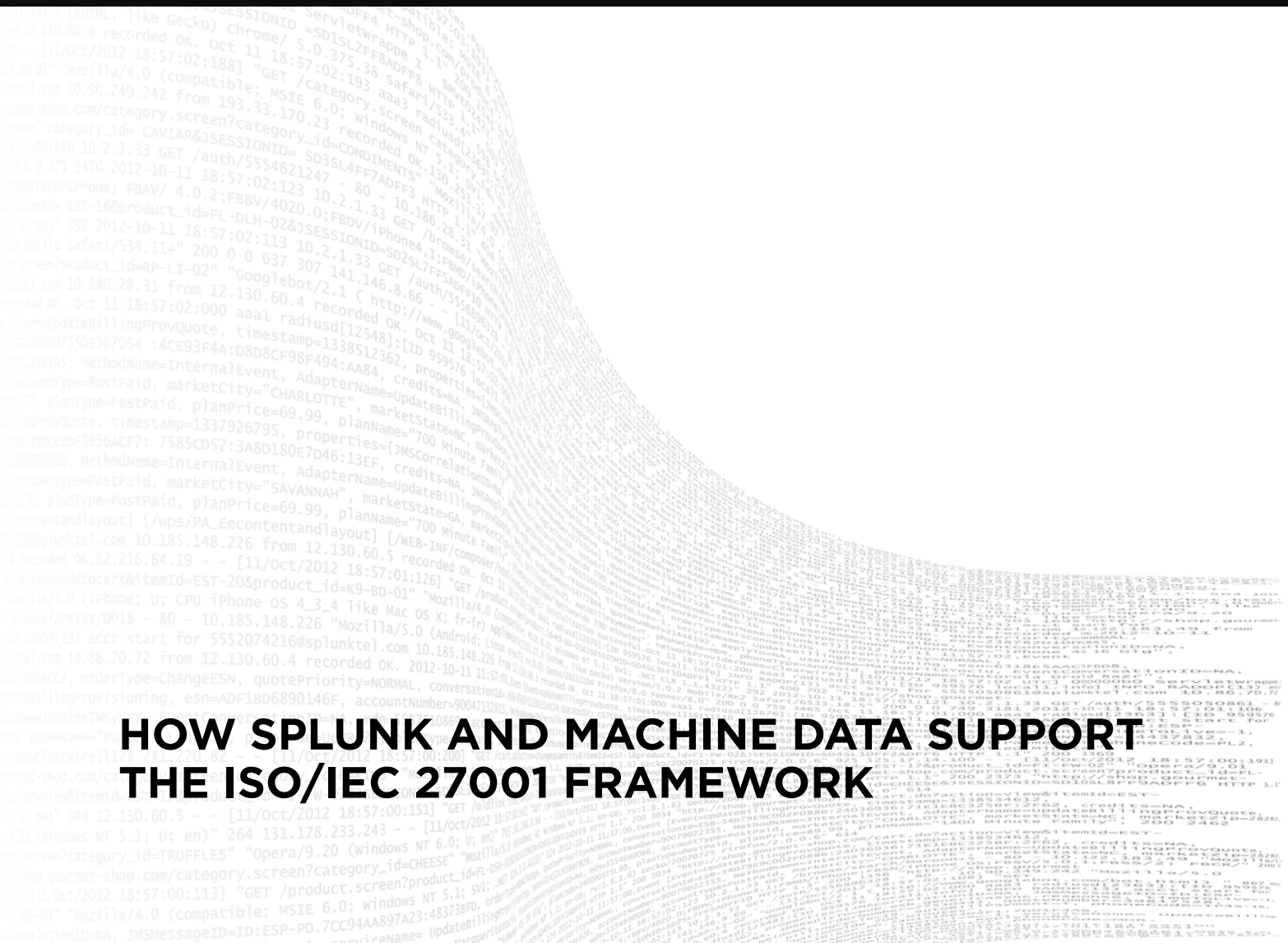
splunk>

WHITE PAPER

HOW SPLUNK AND MACHINE DATA SUPPORT THE ISO/IEC 27001 FRAMEWORK



Digital transformation, establishing customer trust and a patchwork of laws, regulations and standards is forcing organizations around the world to formalize their security programs. For years security was seen by the board of directors as only a technology problem. This has changed radically in recent years and IT governance and establishing an information security management system (ISMS), based on ISO 27001, is now top of mind for organizations.

The chief information security officer (CISO) needs to develop security strategies aligned to both the present and future business. The CISO is also responsible for the development and operation of the organization's information risk program. Organizations need security policies to be developed and put in place, new capabilities established, like incident response processes, and often more operational security functions need to be built.

This is achieved by implementing a suitable set of controls based on guidance provided by the information security standard ISO 27002.

Splunk software gives security teams of all sizes the ability to investigate, monitor, analyze and act on the insights gathered from machine data generated from every network, system, database, web server, application and internet connected device. Security teams relay on Splunk technology as a process enabler and force multiplier to accomplish more work in less time, less money and with greater accuracy.

The Splunk platform also offers a good return on investment for security teams by allowing them to solve problems beyond compliance with the same data used for compliance. The same machine data can be relevant for teams in IT operations, application development, business analytics and Industry 4.0/IoT.

The result is operational and security intelligence with a focus major such as, reputational risks, risks to core business functions that affect top-line revenues and compliance risks that affect reputation, customer trust and the bottom line.

How Splunk Helps

Splunk software is a big data platform for security and machine data that supports ISO 27002 by:

- Providing reporting on machine data as proof-of-compliance controls
- Protecting machine data against unauthorized viewing, modification or deletion and providing audit trails
- Offering day-to-day reviews of systems to compare behavior versus policy
- Monitoring of network devices, servers, applications and transactions for operational and security risks for business resilience
- The ability to perform root-cause investigations
- Supporting service electronic discovery requests by law enforcement
- Conducting HR investigations into an employee's activity
- The ability to access IT data ad hoc by compliance personnel
- Provide proof that audit data has integrity

How to Implement:

Myth: A specific set of reports will make me compliant.

Reality: Regulations almost never list specific reports. There are reports that can assist with particular requirements, such as the need to review failed logins, but they require fine-tuning for each unique environment. At best, a set of standard reports is a place to start. The dirty secret is that most compliance report packs are developed by product managers reading regulations and taking a guess at what reports might be helpful. The most recent auditing trend is to ask an IT representative to demonstrate an ad hoc query in response to an auditor request or requirement.

Each organization has a particular appetite for risk which might even differ between departments. This is why information security guidelines need to be defined, which will force an outcome-based approach. To implement the controls defined in an organization's information security guidelines into SIEM use cases for ISO 27002 the following steps are recommended:

1) Review the information security guidelines your company demands and identify if your SIEM can address each guideline
2) Identify which question needs to be answered and what organizational actions or escalation path needs to be taken to respond
3) Identify which systems, technical components or applications hold the data needed to get the needed answer
4) Collect machine data
5) Investigate machine data and find the right entries that hold the answer
   a) Identify that the logging standards and ensure the logging level is correctly configured on the data sources monitored
6) Define the required reporting logic and any enrichment needs
7) Write (or steal and adjust from predefined dashboards or reports) the Splunk Search Query
8) Decide on regular reporting vs. real-time security event alerting or both

Steps 5 to 8 are done in the Splunk platform usually in minutes thanks to the software's powerful search language, schema on the fly functionalities and more than 1,500 apps on **Splunkbase** with predefined dashboards and reports.

See the chart below for specific ways that machine data and the Splunk platform can support your efforts to comply with the ISO 27002 controls.

Key ISO 27002 Areas	How Machine Data and Splunk Support
6.1.2 Segregation of duties	It might be difficult for smaller organizations to implement segregation. Other controls, such as monitoring activities and keeping audit trails, should be considered. Splunk allows small organizations to capture the audit trails and monitor activities, and then segregate duties needed from any application or digitized process. Activity analysis can be performed to ensure the separation of duties between individuals and/or established roles. Splunk Enterprise supports role-based access-control so access to information is granted based on a user's specific role. User accounts in Splunk can be tied into Active Directory or LDAP for single-sign-on (SSO).
6.1.5 Information security in project management	Splunk allows the project team to explore at an early stage the unknown machine data generated by a digital service to identify necessary risks and controls to cover. It's key to understand what is visible in machine data, what kind of event's/actions might be missing, identify what normal looks like and establish recommendations on what to look for in terms of security monitoring in the production system.

Key ISO 27002 Areas	How Machine Data and Splunk Support
6.2.1 Mobile Device Policy	Splunk allows the collection and reporting from mobile device management systems as well as the collection from mobile email synchronization services to identify any new device registrations, update needs, reporting on policy enforcements and document the successful execution of remote wipe actions in case a phone gets lost or stolen.
6.2.2 Teleworking	Splunk allows organizations to maintain a complete audit trail of any component used for remote teleworking activities, like logins from VPN to the access of sensitive files on a file server through a terminal session and potential print jobs. This helps answer questions like: Who accessed what, when and how, and create alerts if security policies were violated.
7.1.2 Terms and conditions of employment	Splunk helps maintain a list of employees and contractors who have signed a non-disclosure or confidentiality agreement (NDA) and correlate it against access logs of confidential information. If any unauthorized user accesses sensitive data an alert can be triggered. The list of users can be set to synchronize automatically with any kind of database or application API to the legal/HR system, indicating that an NDA or confidentiality agreement was signed/revoked.
7.2.2 Information security awareness, education and training	Splunk can be used to monitor e-learning systems to confirm employee compliance with security awareness training. Additional response actions can be sent to assign based on behavior additional user training.
7.2.3 Disciplinary process	Splunk helps IT and security teams fulfill requests from HR or legal teams if an employee has committed an information security breach. They can conduct forensic investigations across systems and networks to either identify and backup the employee, if the technical user account has been compromised.
7.2.3 Disciplinary process	Splunk allows the IT-security management team to identify positive sanctions or incentives, with remarkable behavior, in regard to information security by creating reports about good behavior. They can identify things like which employees are changing passwords most often or reporting the most phishing e-mails to the IT-security mailbox.
8.1.1 Inventory of Assets	Splunk helps teams pull lists of assets from multiple systems, compare them for accuracy, identify any missing assets and then update them. For example, they could pull a list from the CMDB database that can be synchronized with what is in Active Directory, seen by the Vulnerability Scanner, DHCP requests and what shows up at the Endpoint Protection Management System.
8.1.2 Ownership of Assets	Splunk allows teams to maintain an asset list, which includes the asset owner, classification and notes on what needs to be updated regularly in Splunk Enterprise Security. Individual dashboards can be provided to the asset owner to scale and make information security more accessible.
8.1.4 Return of assets	During the period an employee or contractor is terminated, an organization should closely monitor any unauthorized copying of valuable information. Splunk can put users on a watch list and correlate them with unauthorized copy events like uploads to web storage platforms (e.g. Google Drive or Dropbox), emailing to private email domains (@gmail.com) or removable media usage. Additionally, historical forensic investigations can be made to identify any unauthorized copies of vital information that were made before an employee was terminated.

Key ISO 27002 Areas	How Machine Data and Splunk Support
8.3.1 Management of removable media	Splunk allows organizations to either directly collect data from endpoints or through third party protection tools (like device control/DLP). Copying of data to removable media can be monitored as well as stored as forensic evidence. Through unique device identifications from removable media, potential malware infections can be traced down by looking at things like where else was the USB stick connected to in the company's environment? Also, the overall use of the USB stick can be tracked, which in case of multiple uses could indicate the need for employees to be trained on security awareness.
8.3.2 Disposal of media	Splunk helps companies monitor and keep an audit trail of an eraser PC with its wiping software, which IT teams use to overwrite through standardized procedures media.
8.3.3 Physical media transfer	See 8.3.1 + to validate and prove that encrypted data was stored on removable media.
9.1.1 Access control policy	Splunk allows users to query via search commands or technical addons from third party systems access control lists, then store that information snapshot and provide it in dashboards to the responsible information owner. For example, with Splunk "sa-ldap search" a list of members within a group who are authorized access to classified information in Active Directory can be obtained, stored and reported on. This can be scheduled on a regular basis to keep and audit the configuration at any point of time.
9.1.1 Access control policy	Splunk allows users to collect audit logs from any application, authentication or identity management system, including administrative actions.
9.1.2 Access to networks and network services	Splunk allows users to maintain a complete audit trail of any involved component for accessing a network or network service. Splunk helps companies monitor the use of network services, which finds the answers to questions like: Who accessed what when and how. Admins can then send an alert if the activity was outside of corporate policy.
9.2.1 User registration and de-registration	Splunk helps companies keep an audit trail of the actions of users and hold them responsible for their actions. Things like the sharing of user accounts can be detected with out-of-the-box correlation searches from Splunk Enterprise Security. Exceptions can be made through whitelists.
9.2.1 User registration and de-registration	Splunk can do more than just allow companies to keep an audit trail of disabled or removed user accounts. Splunk can also enrich information about departing users directly from an HR application or ticketing system and alert in case organizational or technical processes have failed or missed one of the many systems that need to de-register a user account.
9.2.2 User access provisioning	Splunk allows users to collect event log data from an authorization system and report which administrator granted a user ID access to a specific information system or service.
9.2.3 Management of privileged access rights	Splunk can monitor privilege changes and monitor changes to metrics and access escalations.
9.2.4 Management of secret authentication information of users	Splunk can track and monitor the first use of user accounts, including validation that a default password was changed.

Key ISO 27002 Areas	How Machine Data and Splunk Support
9.2.5 Review of user access rights	Splunk can query applications and services to report on user access rights and provide an automated report for the asset owner. Splunk can also indicate any kind of changes in the user attribute compared to a previous report review.
9.2.5 Review of user access rights	Splunk can record and report on changes to privileged accounts and document the periodic review/access of a report through Splunk's own auditing.
9.2.6 Removal or adjustment of access rights	Splunk can monitor the process of removing or modifying access rights, for example when an employee moves between departments or is terminated. If a user is added or removed, Splunk can notify IT operations of the change so they can verify that it was authorized.
9.4.2 Secure Log-on procedures	Splunk helps monitor and report on two factor authentication systems, monitor single sign on solutions, query any identity provider or record from the wire authentication attempts.
9.4.2 Secure Log-on procedures	Splunk allows companies to collect unsuccessful and successful login attempts from almost any kind of application, service or system.
9.4.2 Secure Log-on procedures	Splunk can detect brute force activities through different analytical methods. From simple counting to baselining to machine learning–including the detection of slow attempts.
9.4.4 Use of privileged utility programs	The use of system utilities can be monitored and correlated with Splunk. Advanced detection mechanisms are available like dynamic peer group analysis/classifications as well as measuring the length of command line entries as an example.
9.4.5 Access control to program source code	Splunk can monitor software check-in systems for access and separation between development and QA teams.
10.1.2 Key management	Splunk can monitor PKI infrastructure and HSM crypto appliances, including key generation, exports, enrollments, verifications or revocations.
11.1.2 Physical entry controls	Splunk can be used to monitor physical access to facilities and monitor established access patterns for unauthorized access. Data from Active Directory, physical access data and VPN data can be correlated to determine if a user has "tail-gated" into the building.
11.2.1 Equipment siting and protection	Splunk can accept data in almost any format, including data from building HVAC systems to measure temperature change and monitor for related physical threats. Splunk can also accept and monitor data from RFID systems and GPS information, so it can monitor and track the use of (RFID/GPS tagged) company trucks or equipment to protect against theft.
11.2.2 Supporting utilities	Splunk can collect any kind of sensor data or security alerts from building devices to notify IT teams instead of just facility management having visibility.
10.2.8 Unattended user equipment	Splunk can monitor for host inactivity and monitor data, indicating the password screen saver is in use or doesn't launch within a specific length of time.

Key ISO 27002 Areas	How Machine Data and Splunk Support
12.1.1 Documented operating procedures	Splunk enables organizations to build a platform for machine data to use the same procedures and tool for almost any kind of use case. The software allows users to ask different questions of the same data for the needs of different teams. This allows teams to use the same tool (and data) for security investigations, security monitoring, compliance validation, threat detection, end-to-end service monitoring and further SIEM and IT Ops use cases.
12.1.2 Change Management	Splunk can be used to monitor changes to systems and when those changes occurred and who performed the work and why. This is useful when tracking emergency situations verses scheduled downtimes for particular systems. Risk can be assessed by the number of unauthorized changes and can be tracked over time to document the increasing or decreasing level of risk to the business. Correlations with change management tickets can also be performed.
12.1.3 Capacity Management	Splunk can monitor CPU utilization and other hardware performance information within a physical or virtual infrastructure. It can monitor thresholds over time to predict and detect early signs of performance degradation. Partial hardware failures, such as a fan breakdown or memory failure, can be detected and monitored to support resource planning and acquisition decisions. Services can be monitored for performance of transactions across the IT architecture. This data can inform investigations of the service delivery architecture and enrich customer satisfaction metrics. Splunk supports benchmarking against normal performance and alerting on all parts of the IP stack.
12.1.3 Separation of development, testing and operational environments	Splunk allows access to production system logs for troubleshooting without needing to log onto production systems. This is a key audit requirement and prevents unauthorized changes to systems.
12.2.1 Controls against malware	Splunk helps with the collection of inventory information like which packages or applications are installed and deployed. The information can be periodically refreshed and any changes can be reported on. Splunk helps searching for “known” and “unknown threats.” Splunk monitors all aspects of anti-virus deployment, host configuration, email security, web security products and next-generation firewalls. These are known threats reported by signature and rule-based systems. Splunk can augment this data with DNS, DHCP, physical access data, Active Directory log data, packet capture and flow data. Looking for time-based patterns that include geo-location data can identify malicious insiders and persistent malware. Security can become more aligned with the business by focusing on the most important data assets to the business.
12.2.1 Controls against malware	Splunk helps detect malicious websites by looking at firewall or web proxy traffic with third party threat intelligence URL correlation. Splunk can also report on blacklistings and prevention events from security deployed appliances.
12.2.1 Controls against malware	Splunk allows access to system logs for troubleshooting without needing to log onto production systems. Splunk also helps monitor malware protection, reporting on it and supporting the recovery process through automated response actions like quarantining the host (move into a VLAN), validating if a cleanup was successful and ensuring no further indicator of compromise or uncommon network behavior is seen from a cleaned host.

Key ISO 27002 Areas	How Machine Data and Splunk Support
12.2.1 Controls against malware	Splunk provides constantly updated information about new threat tactics and techniques on how to detect and respond to them through its community and Splunk Security Research Team.
12.3.1 Information backup	Splunk can easily monitor data backup solutions for performance, data integrity as well as data access to backups.
12.4.1 Event logging	Splunk can monitor security systems for changes to their configuration in change windows and monitor user behavior. Splunk can also provide a definitive record for compliance audits.
12.4.1 Event logging	Splunk collects any type of log data, if information is missing, Splunk can enrich the data through lookups from various sources. Splunk can also automatically add a timestamp and record which host the event log came from in case meta information is missing.
12.4.1 Event logging	Splunk allows different types and procedures for anonymization and pseudonymization. From the presentation layer only down to the raw logs stored on disc-based on organizational requirements.
12.4.1 Event logging	By default, Splunk is configured so nothing can be deleted or changed through the User Interface. Alerts can be configured in case data sources stop sending event logs or a logging policy change was configured.
12.4.2 Protection of log information	Splunk's user role concept, with strong user authentication, ensures only authorized users can work with event log data. Non-tampering can be proven through a Data Integrity feature, which hashes every slice of newly indexed raw data and writes it to a hash file, which can be also be secured. Log Event removals will be documented in an internal audit log and behavior when the storage capacity is reached can be configured.
12.4.2 Protection of log information	Splunk can be setup as a central platform that can either forward data to another Splunk solution or act as the outside system.
12.4.3 Administrator and operator logs	Splunk monitors all user activities and provides a complete log of activities.
12.4.4 Clock synchronization	Splunk can monitor systems to ensure they are synchronized using the NTP protocol. Splunk will also detect any kind of major time difference in the time stamps of data sources.
12.5.1 Installation of software on operational systems	Splunk can monitor access, configuration and the performance of operational software.
12.6.1 Management of technical vulnerabilities	Splunk can monitor the "half-life" of vulnerabilities in IT architecture and report on them as metrics for patching systems. The data of vulnerable systems can be correlated with IDS/IPS attack data to identify attempts to exploit vulnerable systems.
12.6.1 Management of technical vulnerabilities	Notable Events can be raised on a per system, per vulnerability basis and tracked until the issue is fixed, patched or removed.

Key ISO 27002 Areas	How Machine Data and Splunk Support
12.6.1 Management of technical vulnerabilities	Splunk provides out-of-the-box dashboards to document vulnerability operations dashboards, such as recording scan runs and hosts that weren't previously scanned.
13.1.1 Network controls	Splunk supports role-based access controls for different network teams. Splunk can monitor HTTP, HTTPS, SSL VPN and application layer protocols from AppFlow or other load balancing data. Splunk can also provide metrics for performance aspect of network hardware, configuration changes and network performance. Splunk can use log data to monitor data in transit for fidelity.
13.1.3 Segregation in networks	Splunk can monitor traffic between networks and watch for traffic that isn't allowed for network segregation.
14.2.6 Secure development environment	Splunk can monitor any changes to developer environments or changes to the code store therein.
14.3.1 Protection of test data	Splunk can provide a full audit trail of access to test data.
15.1.1 Information security policy for supplier relationships	Splunk can monitor the access channel a supplier uses and document any activities executed.
15.1.2 Addressing security within supplier agreements	Splunk acts as a centralized platform on which any incidents of access to third party sources can be granted for assistance and collaboration. Splunk can be used by the supplier to deliver compliance reports and prove the effectiveness of controls.
15.2.1 Monitoring and review of supplier services	If a company has access to log data from their service provider, SLAs can be monitored with Splunk. Also, the lifecycle for data hosted by third parties can be monitored up to the point of disposal. SLAs can be trended over time to support service acquisition decisions.
16.1.1 Responsibilities and procedures	Splunk helps security teams quickly, effective and orderly respond to information security incidents and provide management feedback of its scope and potential impact. Incident management activities can be logged within Splunk and put on a timeline.
16.1.1 Responsibilities and procedures	Splunk helps incident response teams quickly gather data and share information about incidents with external organizations as appropriate.
16.1.2 Reporting Information security events	The Splunk Enterprise Security provides security event management alerting and reporting.
16.1.4 Assessment of and decision on information security events	Splunk empowers teams to have a platform to investigate security events and assess if they are to be classified as information security incidents. Splunk allows information security incident response teams to make those decisions.

Key ISO 27002 Areas	How Machine Data and Splunk Support
16.1.5 Response to information security incidents	Splunk provides the functionality not just to detect and investigate incidents but Splunk also allows response actions to be documented in playbooks to execute automatically or orchestrate with an audit trail for later analysis.
16.1.5 Response to information security incidents	Splunk allows users to look back historically and identify massive amounts of machine data from potentially hundreds of different technologies to identify the source of an incident for a post-incident analysis.
16.1.6 Learning from information security incidents	Splunk Enterprise Security provides a complete record of the incident classification and ownership changes with all comment records.
16.1.7 Collection of evidence	Splunk stores the original raw logs generated by any kind of device or application and can perform event hashing to prove no tampering occurred.
18.1.2 Intellectual property rights	Splunk can be used to report on installed software or monitor license usage where there is no technical enforcement and notify upcoming license violations. Splunk can also be used to identify any unused licenses to put them back into an organization's license pool.
18.1.3 Protection of records	Splunk protects records through clustering and high availability concepts, the support of worm drives and file hashing.
18.1.3 Protection of records	Splunk allows different storage systems to utilize records, it allows file hashing as well as defining log retention and rotation.
18.2.2 Compliance with security policies and standards	Splunk allows the creation of dynamic dashboards, reports and alerts by managers to automate and speed up the regular review process.
18.2.3 Technical compliance review	Splunk allows organizations to automate the review of similar systems by capturing the information on what to look for from a competent, authorized person. It can also collect relevant measure points and establish continuous monitoring across the same type of applications to achieve consistency, time savings and increase security.