EventTracker
Actionable Security Intelligence

FFIEC-NCUA/CFPB Solution Brief

EventTracker | 8815 Centre Park Drive, Columbia MD 21045

FFIEC-NCUA/CFPB

About EventTracker

EventTracker delivers business critical software and services that transform high-volume cryptic log data into actionable, prioritized intelligence that will fundamentally change your perception of the utility, value and organizational potential inherent in IT audit and event log files. EventTracker's award winning solutions provide capabilities to implement Security Information and Event Management (SIEM), Log Management, and real-time Threat Intelligence to help optimize IT operations, detect and deter costly security breaches, and comply with multiple regulatory mandates.

EventTracker software is designed to be implemented for organizations with 25 to 25,000 assets such as servers, firewalls, other network and security devices, workstations and applications. SIEMphonic managed services are right-sized to assist you with system administration, incident analysis and compliance activities through "self- half- or full-service" options.

The Federal Financial Institutions Examination Council (FFIEC)

The Federal Financial Institutions Examination Council (FFIEC), having been tasked with providing guidance and enforcement, has documented the necessary controls for compliance in their "FFIEC Information Security Handbook". The remainder of this paper lists the specific control requirements taken from both the FFIEC Information Security Handbook and associated Examination Procedures. For each control requirement, an explanation of how EventTracker supports compliance is provided.

The Council is a formal interagency body empowered to prescribe uniform principles, standards and report forms for the federal examination of financial institutions by the Board of Governors of the Federal Reserve System (FRB), the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA), the Office of the Comptroller of the Currency (OCC) and the Consumer Financial Protection Bureau (CFPB), and to make recommendations to promote uniformity in the supervision of financial institutions. In 2006, the State Liaison Committee (SLC) was added to the Council as a voting member. The SLC includes representatives from the Conference of State Bank Supervisors (CSBS), the American Council of State Savings Supervisors (ACSSS) and the National Association of State Credit Union Supervisors (NASCUS).

The Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 included the creation of and Congress established the new Consumer Financial Protection Bureau (CFPB) to consolidate in one agency the responsibility for regulating consumer financial products and services under the federal consumer financial laws. July 21, 2011 was the "designated transfer date" for the CFPB, and as of that date, certain new authorities of the CFPB became effective, such as the authority to prohibit unfair, deceptive and abusive practices, and other agencies transferred certain existing functions to the CFPB. Those functions include writing consumer financial protection regulations, and supervising very large banks, thrifts and credit unions (those with over $10 billion in assets) and their affiliates to ensure their compliance with federal consumer financial law. They also have supervisory authority for certain nonbank subsidiaries.

EventTracker Provides a Full View of the Entire IT Infrastructure

EventTracker improves security, helps organizations demonstrate compliance, and increases operational efficiencies. EventTracker enables your organization to be more aware of potential security risks and internal/external threats. It provides you with the ability to respond to a security incident with comprehensive data and forensic tools for analysis. The time required to investigate and mitigate security incidents can be greatly reduced, minimizing potential exposure and costs.

SIEMphonic is our managed services offerings to enhance the value of EventTracker implementations. Our expert staff can assume responsibility for some or all EventTracker SIEM-related tasks, including system management, incident reviews, daily/weekly log reviews, configuration assessments, and audit support. We augment your IT Security team, allowing you to focus on your priorities by leveraging our expertise, discipline and efficiency.

Scalable, Log Collection and Processing with Notifications based on Criticality

EventTracker provides automatic consolidation of thousands or even millions of audit events to meet the needs of any size organization. The inbound log data is identified by EventTracker's built-in manufacturers Knowledge Base, which contains log definitions for thousands of types of log events, and automatically identifies which events are critical to security standard.

EventTracker provides real-time and batch aggregation of all system, event and audit logs from your firewalls, IDS/IPS, network devices, Windows, Linux/Unix, VMware ESX, Citrix, databases, MS Exchange web servers, EHRs and more.

Ease of Deployment and Scalability

EventTracker is available on premise or as a highly scalable cloud-based SIEM and Log Management solution. It offers several deployment options to meet the needs of organizations with a few dozen systems or those with thousands of systems spread across multiple locations. EventTracker Cloud is available as an AMI on Amazon EC2, Microsoft Azure or your cloud infrastructure provider of choice. It supports multi-tenant implementations for MSSP organizations serving the needs of smaller customers.

FFIEC/NCUA/CFPB Compliance Requirements

Requirements	EventTracker Solution	EventTracker Reports	EventTracker Alerts
Access Rights Administration Control-1: Determine that administrator or root privilege access is appropriately monitored, where appropriate. Management may choose to further categorize types of administrator/root access based upon a risk assessment. Categorizing this type of access can be used to identify and monitor higher-risk administrator and root access requests that should be promptly reported.	EventTracker collects all account management and account usage activity. The creation of privileged accounts (i.e., administrator, root) or granting of privileged rights is easily and automatically monitored, alerted and reported on.	Yes	Yes
Authentication Control-1: Determine whether access to system administrator level is adequately controlled and monitored.	EventTracker collects all account management usage activity. The creation of privileged accounts (i.e., administrator, root) or granting of privileged rights is easily and automatically monitored, alerted and reported on.	Yes	Yes
Network Security Control-1: Determine whether logs of security-related events and log analysis activities are sufficient to affix accountability for network activities, as well as support intrusion forensics and IDS. Additionally, determine that adequate clock synchronization takes place.	EventTracker can collect logs from network devices, IDS/IPS systems, A/V systems, firewalls and other security devices. EventTracker provides central analysis and monitoring of intrusion related activity across the IT Infrastructure. EventTracker can correlate activity across user, origin host, impacted host, application and more. EventTracker can be configured to identify known bad hosts and networks. EventTracker's Personal Dashboard provides customized real-time monitoring of events and alerts. EventTracker's Investigator provides deep forensic analysis of intrusion related activity. EventTracker's integrated knowledge base provides information and references useful in responding to and resolving intrusions.	Yes	Yes
Control-2: Determine whether logs of security-related events are appropriately secured against unauthorized access, change and deletion for an adequate time period, and that reporting to those logs is adequately protected.	EventTracker helps ensure audit trail are protected from unauthorized modification. EventTracker collects logs immediately after they are generated and stores them in a secure repository. EventTracker servers utilize access controls at the operating system and application level to ensure that log data cannot be modified or deleted. EventTracker completely automates the process of re-taining the audit trail. EventTracker creates archive files of all collected log entries. These files are organized in a directory structure by day making it easy to store, backup and destroy log archives based on the policy.	Yes	Yes

Requirements	EventTracker Solution	EventTracker Reports	EventTracker Alerts
Control-3: Determine whether remote access devices and network access points for remote equipment are appropriately controlled. • Remote access is disabled by default, and enabled only by management authorization. • Management authorization is required for each user who accesses sensitive components or data remotely. • Authentication is of appropriate strength (e.g., two-factor for sensitive components). • Modems are authorized, configured and managed to appropriately mitigate risks. • Appropriate logging and monitoring takes place. • Remote access devices are appropriately secured and controlled by the institution. – Remote access devices are appropriately secured and controlled by the institution.	EventTracker collects network device logs. EventTracker's analysis & reporting capabilities can be used for reviewing network activity to ensure only authorized communications occur. EventTracker alerts can be used for detecting unauthorized communications. EventTracker collects remote access activity for VPN, SSH, telnet, etc. EventTracker reports provide easy and independent review of remote access to information systems.	Yes	Yes
HOST Security Control-1: Determine whether access to utilities on the host is appropriately restricted and monitored.	EventTracker can collect audit logs reporting on the access and use of utilities on hosts for monitoring and reporting. Additionally, EventTracker's file integrity monitoring capability can be used to independently detect access and use of utilities.	Yes	Yes
Control-2: Determine whether the host-based IDSs identified as necessary in the risk assessment are properly installed and configured, that alerts go to appropriate individuals using an out-of-band communications mechanism, and that alerts are followed up.	EventTracker can collect logs from IDS/IPS systems. EventTracker provides robust alerting and notification capabilities that help ensure alerts are routed to the appropriate individuals. EventTracker's integrated incident management capabilities provide accountability and reporting on alarm resolution.	Yes	Yes
Control-3: Determine whether logs are sufficient to affix accountability for host activities and to support intrusion forensics and IDS and are appropriately secured for a sufficient time period.	EventTracker helps ensure audit trail are protected from unauthorized modification. EventTracker collects logs immediately after they are generated and stores them in a secure repository. EventTracker servers utilize access controls at the operating system and application level to ensure that log data cannot be modified or deleted.	Yes	Yes
Application Security Control-1: Determine whether appropriate logs are maintained and available to support incident detection and response efforts.	EventTracker completely automates the process of retaining your audit trail. EventTracker creates archive files of all collected log entries. These files are organized in a directory structure by day making it easy to store, backup and destroy log archives based on your policy. EventTracker detects the incident automatically and alerted on.	Yes	Yes

Requirements	EventTracker Solution	EventTracker Reports	EventTracker Alerts
Software Development and Acquisition Control-1: Evaluate whether the software acquired incorporates appropriate security controls, audit trails, and activity logs and that appropriate and timely audit trail and log reviews and alerts can take place.	EventTracker collects logs from commercial and custom applications. EventTracker provides central analysis, reporting, and alerting for application logs.	Yes	Yes
Security and Monitoring Control-1: Identify the monitoring performed to identify non-compliance with institution security policies and potential intrusions. • Review the schematic of the information technology systems for common security monitoring devices. • Review security procedures for report monitoring to identify unauthorized or unusual activities. • Review management's self-assessment and independent testing activities and plans.	EventTracker can collect logs from IDS/IPS systems, A/V systems, firewalls, and other security devices. EventTracker provides central analysis and monitoring of intrusion related activity across the IT infrastructure. EventTracker can correlate activity across user, origin host, impacted host, application and more. EventTracker can be configured to identify known bad hosts and networks. EventTracker's Personal Dashboard provides customized real-time monitoring of events and alerts. EventTracker's Investigator provides deep forensic analysis of intrusion related activity. EventTracker's integrated knowledge base provides information and references useful in responding to and resolving intrusions. EventTracker ensures audit trails are protected, retained, and can be easily restored years later.	Yes	Yes
Control-2: Determine whether logs of security-related events are sufficient to support security incident detection and response activities, and that logs of application, host and network activity can be readily correlated.			
Control-3: Determine whether logs of security-related events are appropriately secured against unauthorized access, change and deletion for an adequate time period, and that reporting to those logs is adequately protected.			
Control-4: Determine whether logs are appropriately centralized and normalized, and that controls are in place and functioning to prevent time gaps in logging.			
Control-5: Determine whether an appropriate process exists to authorize employee access to security monitoring and event management systems and that authentication and authorization controls appropriately limit access to and control the access of authorized individuals.	EventTracker provides centralized secure access to all log data. EventTracker leverages application and database level controls to restrict user access to authorized data and functions. EventTracker includes discretionary access controls for restricting users to a defined subset of the log data collected.	Yes	Yes

Requirements	EventTracker Solution	EventTracker Reports	EventTracker Alerts
Control-6: Determine whether appropriate detection capabilities exist related to: • Network related anomalies, including – Blocked outbound traffic – Unusual communications, including communicating hosts, times of day, protocols and other header related anomalies – Unusual or malicious packet payloads • Host-related anomalies, including – System resource usage and anomalies – User related anomalies – Operating and tool configuration anomalies – File and data integrity problems – Anti-virus, anti-spyware, and other malware identification alerts – Unauthorized access – Privileged access	EventTracker can collect logs from hosts, network devices, IDS/IPS systems, A/V systems, firewalls and other security devices. EventTracker provides central analysis and monitoring of network and host activity across the IT infrastructure. EventTracker can correlate activity across user, origin host, impacted host, application and more. EventTracker can be configured to identify known bad hosts and networks. EventTracker's alarming capability can be used to independently detect and alert on network and host based anomalies via sophisticated filtering, correlation and threshold violations.	Yes	Yes

References

https://www.ffiec.gov/exam/InfoBase/documents/02-ncu-12_cfr_748_app_a_safeguard_info-010100.pdf

http://ithandbook.ffiec.gov/media/26895/nuca_2%20cfr_pt_748_%20appx_%20a_b.pdf

http://ithandbook.ffiec.gov/media/26901/nuca_appc_a_12_cfr_pt_749.pdf