Netsurion | EventTracker

SANS Top 20 CIS Critical Security Control Solution Brief Version 7

www.netsurion.com/eventtracker

SANS Top 20 CIS

About Netsurion

Netsurion powers secure and agile networks for highly distributed and small-to-medium enterprises and the IT providers that serve them. In such environments, the convergence of threat protection and network management are driving the need for greater interoperability between the NOC (network operations center) and the SOC (security operations center) as well as solutions that fuse technology and service to achieve optimal results. To this end, Netsurion has converged purpose-built network hardware, innovative security software, and flexible managed services.

Netsurion's SD-Branch solution, BranchSDO, is a comprehensive network management and security solution consisting of SD-WAN, next-gen security, cellular, Wi-Fi, and PCI DSS compliance tools and support. At the heart of the solution is the CXD, Netsurion's SD-WAN edge appliance.

Netsurion's Security Operations solution, EventTracker, delivers advanced threat protection and compliance benefits in a variety of deployment options: a SIEM platform, a co-managed SIEM service with 24/7 SOC, and a managed SIEM for MSPs.

SANS Top 20 CIS Critical Security Control Overview

The 20 Critical Security Controls were developed in the U.S. by a consortium led by the Center for Strategic and International Studies (CSI).

The Consensus Audit Guidelines (CAG), also known as the 20 Critical Security Controls, is a publication of best practices relating to computer security that essentially encompass twenty (20) core controls. Today's growing cyber security threats are posing serious challenges for organizations regarding the confidentiality, integrity and availability (CIA) of their networks, ultimately requiring comprehensive measures to protect critical assets and infrastructure. What's interesting to note about the 20 Critical Security Controls is its formation itself, which came about due to a collaborative effort amongst a number of well-known entities, including U.S. government agencies, information security forensics experts and others.

Protective Monitoring

The policy is not reproduced here and public sector bodies should obtain it from the CESG. However, in summary, the logging requirements regarding user access to your network and systems include recording the following events:

- Unauthorized application access (where applicable)
- File access attempts to protectively marked information (e.g. RESTRICTED data).
- Unsuccessful login / logout
- Successful login / logout
- Privileged system changes (e.g. account management, policy changes, device configuration)

Logs should be kept for at least 6 months. This may include the use of backup tapes, but logs should be easily available for use as part of your incident response policy, as well as help with an investigation. In practice this may need a system which maintains logs readily recoverable from any archive.

EventTracker Provides a Full View of the Entire IT Infrastructure

EventTracker SIEM improves security, helps organizations demonstrate compliance and increases operational efficiencies. EventTracker SIEM 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 offering that enhances 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 SIEM 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 Knowledge Base, which contains log definitions for thousands of types of log events, and automatically identifies which events are critical to security standards.

EventTracker SIEM 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 SIEM is available on premises 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.

SANS Top 20 CIS Critical Security Control Version 7 Requirements

Requirements	EventTracker Solution	EventTracker Reports	EventTracker Alerts
CSC-1 Inventory and Control of Hardware Assets Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.	EventTracker can import from asset databases, and correlate actual devices present on the network against lists of approved devices. EventTracker can also collect logs from DHCP servers to help detect unknown or unauthorized systems. EventTracker supports the Control 1 Metric by identifying new unauthorized devices being connected to the network in near real time (for example via DHCP logs).	Yes	Yes
CSC 2: Inventory and Control of Software Assets Actively manage (inventory, track, and correct) all software on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.	EventTracker monitors for the installation or execution of software. EventTracker can also create and maintain dynamic lists of approved software based on behavioral monitoring that may be operated in the environment. EventTracker supports the Control 2 Metric by identifying attempts to install authorized/unauthorized software (for example via Windows application logs/Application monitoring feature), by identifying attempts to execute unauthorized software (by monitoring process startups).	Yes	Yes
CSC 3: Continuous Vulnerability Management Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers.	EventTracker collects logs from vulnerability scanners. It is able to correlate event logs with data from vulnerability scans. EventTracker can monitor the use of the account that was used to perform the vulnerability scan. EventTracker supports the Control 4 Metric by collecting logs and data from vulnerability scans. This enables EventTracker to correlate both the data from the scan and the logs about the scan, providing the basis to report on progress of the vulnerability scan, and of any devices where the scan did not take place. EventTracker can also collect logs relating to patch installation, and can trigger an alert based on successful completion.	Yes	Yes
CSC 4: Controlled Use of Administrative Privileges The processes and tools used to track/ control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.	EventTracker collects logs from almost any device and can monitor the use of default, generic, service and other privileged accounts. EventTracker supports the Control 5 Metric by collecting logs on administrative activities from across the infrastructure. EventTracker offers out-of-the-box Privileged User Monitoring, which simplifies the task of tracking and monitoring accounts with elevated privileges and automates a number of tasks that are generally done manually. EventTracker can be used in combination with multiple operating systems (various Linux distributions, Windows, Solaris, etc.) in addition to MS Exchange server 2007 and 2010. EventTracker's unique ability to simultaneously correlate data across multiple applications and devices strengthens privileged user monitoring and exposes suspicious activity performed by administrative accounts.	Yes	Yes
CSC 5: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers Establish, implement, and actively manage (track, report on, correct) the security configuration of laptops, servers, and workstations using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.	EventTracker monitors the use of privileged or generic accounts, the startup of services, the use of ports, and the application of patches. EventTracker can also detect changes to key files through its Change Audit feature. EventTracker supports the Control 3 Metric by identifying changes to key files, services, ports, configuration files, or software installed on the system.	Yes	Yes

Requirements	EventTracker Solution	EventTracker Reports	EventTracker Alerts
CSC 6: Maintenance, Monitoring, and Analysis of Audit Logs Collect, manage, and analyze audit logs of events that could help detect, understand, or recover from an attack.	EventTracker provides a comprehensive platform for the maintenance, monitoring and analysis of audit logs. EventTracker supports the Control 6 Metric by collecting all events from across the network. EventTracker performs extensive processing of every log that is collected, assigning a common event and establishing a risk based priority for each log. EventTracker's patented real-time analytics technology can baseline behavior of users, hosts and data from across the network. Once a baseline is established, abnormal behavior can be detected and alerted on.	Yes	Yes
CSC 7: Email and Web Browser Protections Minimize the attack surface and the opportunities for attackers to manipulate human behavior though their interaction with web browsers and email systems.	EventTracker can collect logs from email and web-content filtering tools. EventTracker is tightly integrated with MS Exchange, Office 365 and many more.	Yes	Yes
CSC 8: Malware Defenses Control the installation, spread, and execution of malicious code at multiple points in the enterprise, while optimizing the use of automation to enable rapid updating of defense, data gathering, and corrective action.	EventTracker collects logs from malware detection tools and correlate those logs with other data collected in real time to eliminate false positives and detect blended threats. EventTracker can also collect logs from email and web-content filtering tools. Via its advanced agent, EventTracker can detect and report data copied to removable storage devices. EventTracker is tightly integrated with industry-leading security vendors including FireEye, Fortinet and Palo Alto, among many others. EventTracker supports the Control 8 Metric by continually collecting and monitoring logs from a wide variety of malware detection tools, in addition to its own agent technology.	Yes	Yes
CSC 9: Limitation and Control of Network Ports, Protocols, and Services Manage (track/control/correct) the ongoing operational use of ports, protocols, and services on networked devices in order to minimize windows of vulnerability available to attackers.	By collecting logs from port scanners, EventTracker is able to detect open ports on the network. EventTracker can also collect logs on protocols in use and services starting up on individual devices. EventTracker supports the Control 9 Metric by collecting logs from across the environment and baselining the behavior patterns observed over a period of time. Using this baseline, deviations from normal or expected behavior can be detected and alerts generated.	Yes	Yes
CSC 10: Data Recovery Capability The processes and tools used to properly back up critical information with a proven methodology for timely recovery of it	EventTracker collects logs from Windows and other backup systems. EventTracker can detect backups that did not successfully complete, or backups that did not start.	Yes	Yes
CSC 11: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches Establish, implement, and actively manage (track, report on, correct) the security configuration of network infrastructure devices using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.	EventTracker collects logs from any network device that generates syslog or SNMP. EventTracker supports the Control 11 Metric by collecting logs from network devices and correlating changes against a change control system to identify and alert on any unauthorized changes.	Yes	Yes

Requirements	EventTracker Solution	EventTracker Reports	EventTracker Alerts
CSC 12: Boundary Defense Detect/prevent/correct the flow of information transferring networks of different trust levels with a focus on security-damaging data.	EventTracker collects logs from a wide variety of boundary defense devices for correlation or compliance purposes. EventTracker supports the Control 12 Metric by collecting logs from boundary defense devices. EventTracker can build trends of data flows based on observed behavior and alert on deviations from normal behavior. By understanding the internal network infrastructure, internal and external context can be added to alerts, helping identify unexpected traffic flows such as a website in the DMZ communicating directly with a SQL database, rather than communicating via the application layer. EventTracker also offers out-of-the-box support for third party threat lists and custom IP address blacklists, and can alert in real-time when connections are made to any blacklisted IP address or host.	Yes	Yes
CSC 13: Data Protection The processes and tools used to prevent data exfiltration, mitigate the effects of filtrated data, and ensure the privacy and integrity of sensitive information.	EventTracker collects logs from both endpoints and network perimeter devices in order to assist in the detection of data loss incidents. EventTracker supports the Control 13 Metric by collecting logs from endpoints, authentication systems, boundary defense devices, proxies and email servers, amongst others. EventTracker is able to detect abnormal activity in real time. EventTracker's patented, real-time analytics technology, is able to establish baselines of behavior.	Yes	Yes
CSC 14: Controlled Access Based on the Need to Know The processes and tools used to track/control/prevent/correct secure access to critical assets (e.g., information, resources, systems) according to the formal determination of which persons, computers, and applications have a need and right to access these critical assets based on an approved classification.	EventTracker collects audit logs from across the network. Fully integrated Change Auditing capabilities monitor for and alert on a variety of malicious behaviors, including improper user access of confidential files to botnet related breaches and transmittal of sensitive data. EventTracker supports the Control 14 Metric by collecting logs of all attempts by users to access files on local systems or network accessible file shares without the appropriate privileges. EventTracker's Change Audit can also be used to establish a baseline of normal behavior against a file or file set, and can alert on deviations from that behavioral baseline.	Yes	Yes
CSC 15: Wireless Access Control The processes and tools used to track/control/prevent/correct the security use of wireless local area networks (LANS), access points, and wireless client systems.	EventTracker collects logs from a variety of wireless devices and management systems. In conjunction with logs collected from DHCP servers, wireless clients may be detected when connecting to the organization's network. EventTracker supports the Control 15 Metric by collecting logs from wireless devices, wireless management systems, and DHCP. Real-time correlation of these logs enables the identification of unauthorized wireless devices or configurations.	Yes	Yes

Requirements	EventTracker Solution	EventTracker Reports	EventTracker Alerts
CSC 16: Account Monitoring and Control Actively manage the life cycle of system and application accounts -their creation, use, dormancy, deletion -in order to minimize opportunities for attackers to leverage them.	EventTracker collects audit logs from across the network for both local and network accounts. EventTracker supports the Control 16 Metric by collecting logs of all user activity and correlating this with lists of privileged, generic and service accounts, and also with lists of accounts for users that are terminated. Using Change Audit, lists can be automatically maintained when changes take place in the environment. EventTracker can alert when the use of terminated accounts is observed, and offers extensive reporting capabilities in this area. EventTracker can also establish baselines of normal account behavior. For example, EventTracker can track which servers a user normally connects to, and alert on a deviation from that norm.	Yes	Yes
CSC 17: Implement a Security Awareness and Training Program For all functional roles in the organization (prioritizing those mission-critical to the business and its security), identify the specific knowledge, skills, and abilities needed to support defense of the enterprise; develop and execute an integrated plan to assess, identify gaps, and remediate through policy, organizational planning, training, and awareness programs.	SANS Control 17 is policy-based and focuses on skills and training. EventTracker is able to monitor user compliance with policy and send alerts in real time when credentials are used in an abnormal manner. Since all user activity is logged and collected, correlation and reporting are effective methods for monitoring the adherence to policy.	Yes	Yes
CSC 18: Application Software Security Manage the security life cycle of all in-house developed and acquired software in order to prevent, detect, and correct security weaknesses.	EventTracker collects logs from web application firewalls and from vulnerability scanners. EventTracker supports the Control 18 Metric through its ability to correlate across various applications and device logs at once. It is especially well positioned to create meaningful, relevant alerts around suspicious web log data. EventTracker provides out-of-the-box alerts for detecting suspicious URL characters and malicious user agent strings, in addition to automatically populating an "attacking IPs list." This list enables reporting to be done on source IPs that is attacking the web applications. EventTracker collects logs from WAFs and IDS/IPS systems, in addition to vulnerability scanners. All security event logs are correlated in real time.	Yes	Yes
CSC 19: Incident Response and Management Protect the organization's information, as well as its reputation, by developing and implementing an incident response infrastructure (e.g., plans, defined roles, training, communications, management oversight) for quickly discovering an attack and then effectively containing the damage, eradicating the attacker's presence, and restoring the integrity of the network and systems.	SANS Control 19 is policy-based and focuses on having a clear Incident Response policy. EventTracker has an integrated incident management capability, providing real-time updates on an incident's status (i.e., working, closed, etc.). Status and commentary can be attached to each alert and progress reports can be generated on demand.	Yes	Yes

Requirements	EventTracker Solution	EventTracker Reports	EventTracker Alerts
CSC 20: Penetration Tests and Red Team Exercises Test the overall strength of an organization's defenses (the technology, the processes, and the people) by simulating the objectives and actions of an attacker.	EventTracker collects logs from across the environment. It is a valuable monitoring tool during any penetration test, or red team exercise. EventTracker enables the accounts used in the penetration test to be automatically monitored for legitimate use. EventTracker also enables the detection of unusual behavior and may be used to detect the attempts to exploit the enterprise systems during penetration testing.	Yes	Yes

References:

https://www.cisecurity.org/critical-controls.cfm

https://www.sans.org/critical-security-controls