SECNOLOGY

CUSTOMERS USE CASES

100 EXAMPLES ON CUSTOMERS USE CASES

Thanks to SECNOLOGY's wide range and easy to use technology, it doesn't take long for clients to benefit from the vast range of functionality.

1. Detect and analyze fluctuations and potential weaknesses on the information system
2. Maintain a flow chart to identify all communications in the information system. e.g. network, protocol, applications, server, services, department, or company level
3. Identify users who haven't logged in within a two week period
4. Filter only the important events from a large data volume
5. Separate useful and irrelevant data
6. Track the number of users who accessed a website and how often, the most frequently viewed, the most frequent users and user nationality
7. Monitor and control the security policies at workstation level or server level
8. Identify the top 20 users who surf the Internet and the 10 sites they visit most often
9. Monitor the duration colleagues spend on the internet, from start time to end time
10. Monitor any configuration changes and the changes that were made on the critical servers or security devices
11. Compare and contrast the number of transactions carried out on a group of servers and/or a certain population looking at the current and previous year's transactions
12. Compare and contrast memory and CPU utilization on all production machines
13. Trace the progression of different sessions for each protocol from the point of internet access
14. Analyze the firewall configuration and identify any rules that are no longer used, objects which no longer exist, and the sequence in which the rules must run and improve the performance of the firewall
15. Identify who accessed a particular server at a certain time, for example, Human Resources Server between 13:00 and 14:00 on November 20th 2004
16. Obtain a global overview of all events on one Central Server
17. Analyze the configurations of all routers and check for inconsistencies with the level 4 switches
18. Collect, extract and convert raw data to meaningful data for a 3rd party application
19. Receive alert notifications whenever there is a major change on a device
20. Analyze the PABX (Private Automatic Branch eXchange) logs for communication management, right management, and billing management to get a more accurate understanding of how their subscribers use the content or applications they are providing in order to adjust their subsribers' billing plans
21. Better control of third party services that may jeopardize Telco's existing revenue streams (e.g. Skype) over a GSM/3G network and to accurately measure third party service usage in order to provide the basis for checking and adjusting the SLAs put in place with Content Providers
22. Control the networks' increasing complexity and enable the building of richer quality of service (QoS) measurement and trouble-shooting solutions for the both the enterprise and carrier markets
23. Perform data log extraction to process key selected business information over IP networks in order to significantly improve their business critical application performances
24. Analyze both signaling and voice transfer sessions and facilitate correlation between protocols to enable MOS computation per call, per group of calls, per location, etc. in order to improve the experience of their VoIP service users.
25. Understand network behavior, why traffic may be experiencing delays and how subscribers use their network
26. Deliver more detailed and valuable data for clients in order to refine and adjust media investment strategies by measuring all valuable information produced in the digital world
27. Extract accurate information at user level to manage the quality of the user experience (QoE) and profile usage, in order to provide specifically customized and targeted offers
28. Carry out accurate and reliable IPTV audience measurements with a user-friendly plug-andplay solution, in order to optimize IPTV viewer profiling and generate extra revenue
29. Provide full visibility on all peer-to-peer transfers enabling the entertainment industry to prevent huge revenue leakage from piracy

TURN DATA INTO ACTIONS

30. Detect and prevent unauthorized information transmission from corporations' computer systems to outsiders
31. Analyze all Internet communications (websurf, chat, webmail, file transfert, etc.) and help Law Enforcement Agencies (LEAs) to enhance their Internet interception offers
32. Empower data retention solutions to record all communication details while saving storage capacity. Telecom operators are legally required to make detailed information, describing communication transiting through their network, available to government authorities
33. Anticipate malfunctions by being proactive
34. Evaluate potential opportunities by projected forecasts
35. Compare and correlate events from several devices and different sources (applications, systems, users)
36. Ensure that data is traced in real time and that all actions have been carried out
37. Categorize and list any unusual activities
38. Identify a dead lock loop in the email system, eliminate it and alert the messaging administrator
39. Analyze all communication logs to ascertain whether a user, an application or a process has tried to access a number of times a device which it doesn't have authority to
40. Save, track and protect all traces, files and configurations from all source devices
41. Carry out horizontal and vertical investigations and correlations
42. View in a clear and concise manner all events that take place on security devices
43. View in real time what is happening at security level
44. Verify that the security rules are being implemented correctly with no inconsistency amongst all security devices
45. Identify the security rules that aren't being used, ones that are used often as well as those used least
46. Identify the security rules that have been recently added and the objects they are applied to
47. Scan for any inconsistencies between different security rules
48. Access to business views
49. Awareness of how system security will react to an audit
50. Audit data and control with an audit trail
51. Access an original security trace at a given time
52. Analyze and trace attacks on 15 regional agencies for a given period
53. Compare the real impact of a new device or new architecture on the information system
54. React automatically and appropriately to a particular set of structured events, behavior or circumstances
55. Automate the traceability and retention period according to the type of data and according to countries legislation
56. Filter only useful information (parameters, thresholds, conditions, circumstances, etc)
57. Present a comprehensible technical support synopsis for the management hierarchy
58. Identify what is happening on the information system and protect it from any unknowns
59. Evaluate to what extent the information system is vulnerable
60. Interrogate the log content of any device, operating system, or application
61. Achieve and maintain regulatory law compliance (PCI-DSS, SoX, GLBA, FISMA, HIPAA, ISO27XXX, etc.) while replacing tedious manual processes as well as incomplete processes with full and detailed reports
62. Collect all available information so as to speed up the investigation process of an incident
63. Measure the qualities of services rendered and have access to all factual information
64. Correlate several events from several different sources of devices, systems and applications
65. Qualify the threat and quantify the risk on critical platforms
66. Anticipate needs to aid quick responses to new business requirements
67. Set up an SLA based on key flags or parameters from applications, systems, network devices, or telecom switches
68. Reorganize documents automatically, sorting them according to policy or strategy
69. Have access to a powerful robot that is able to perform several tasks at once, according to its directives
70. Set up a tool that measures the online functionality of internet sites
71. Execute a collection of static data from file systems or databases
72. Monitor the network devices

TURN DATA INTO ACTIONS

73. Measure and audit outsourced maintenance services handling printers and network devices all over the world vs the contracted SLA
74. Track the flow in a complex Firewall Load Balancing architecture framework
75. Reformat the data file or amend the format of the file data
76. Receive alert notifications if a device or application doesn't restart
77. Manage remote user's connection to know who is connected to the network and at what time and for how long
78. Know which applications, systems, networks have had production problems and for how long, in order to improve their service quality management and troubleshooting
79. Reduce the operating cost and the restoration times of service incidents
80. Profiling all types of data source
81. Find, clean (duplicates, inconsistency, caducity), restructure, and enhance all or some of the business data
82. Use data link between several processes and heterogeneous applications
83. Manage non SNMP networks
84. Extract data from a non-structured environment to save into a structured one
85. Monitor several processes in real time depending on department, business type or application type
86. List all executable programs installed on the servers and workstations
87. Categorize and reorganize all files on servers' clusters
88. Create a monthly catalog of any newly available applications on the network
89. Create a symptomatic plan of the company data, to establish who has access to what data, a well as who has modified the data and when
90. Reinforce the availability, integrity, and confidentiality of the data
91. Generate a common data reference to all business applications and follow up its consistency
92. Execute a random and immediate audit of events in the ordering area
93. Enable all business users to generate requests on their own department's data from a simple web navigator
94. Build a SOC (Security Operation Center) to allow Remote Security Management Services (MSSP)
95. Monitor all critical applications 24H/24 365 days a year
96. Collect and analyze the logs from a huge number of Solar Flow units around the world to tune predictions either on demand or on a monthly basis
97. Discover and convert all existing EBCDIC files of the information system into ASCII files and save them on the SAN
98. Migrate Checkpoint security rules into Juniper or Palo Alto security rules

There is a very strong probability that you are already interested in what some of our customers did with SECNOLOGY. Find out for yourself how SECNOLOGY can cater to your specific needs. Contact us!

Corporate Headquarters
747 El Granada Boulevard Suite 2547
El Granada, CA 94018
(415) 762-1820
info@secnology.com

EMEA Office
22 rue Victor Hugo
78350 Jouy-En-Josas, France
+33 (0)1 4645-4610
emea@secnology.com