its co

powered by STRATOZEN

ITSco Comprehensive Cybersecurity Monitoring and Compliance

919.674.0044 ext. 527
info@itsco.com | itsco.com

BUSINESS CHALLENGE

Cybersecurity threats are on the rise and only getting more dangerous. It seems every day there's a new headline about another data breach. And it's no longer only large enterprises that must be concerned. Recent ransomware incidents have shown that small and medium-size businesses are also highly vulnerable to today's threats, and the impact can be enormous. If infected by ransomware, you may be forced to pay tens of thousands of dollars to get your data back. And the average cost of a data breach is now over $5.9 million.

However, most organizations don't have the technology or personnel to even detect these emerging cybersecurity threats. In fact, the average time between a data breach and discovery is 205 days – that's over 7 months! Simply implementing security tools such as firewalls or anti-virus isn't enough. This is even more true for organizations that fall under PCI, HIPPA, SOX, or FFIEC regulations. For those companies, compliance with various guidelines and mandates is absolutely critical to avoid fines or worse.

Today's threats and compliance guidelines require organizations of all sizes to collect, correlate, and analyze security information from all IT systems to enable rapid detection and remediation. That technology is known as security information and event management (SIEM), and it provides deep security intelligence for your IT environment. A proper SIEM solution combined with human oversight by an expert Security Operations Center can help answer critical questions that are vital to your cybersecurity protection – questions such as:

- A user login has failed multiple times; did the employee forget their password or is this a brute force attack?
- Sensitive files on a server were accessed last night; is this normal business use or did we just get breached?
- A typical firewall can send out 864,000 events per day; how do I know which of these (if any) are important?
- New wireless access points have been added to the network; where are they and was this intentional?
- Are our employees going to sites – intentionally or not – that put us at risk for malware infection?
- Regulatory compliance requirements are changing constantly; do we have the data needed to properly comply?

SOLUTION OVERVIEW

Our comprehensive SIEM-as-a-Service solution offers automated consolidation, correlation, and analysis of security events across your entire network coupled with manual daily reviews performed by security analysts in our Security Operations Center (SOC). The result is instant notifications to the support team when cybersecurity threats are detected, plus human oversight to find hidden threats and trends that a fully automated system can't detect on its own. Together, the SEIM and SOC provide organizations 24x7 cybersecurity threat detection and compliance reporting without any of the headache or capital investment of legacy solutions.

The advanced automation available with today's technology allows us to monitor every critical device in your environment for less than what you would pay another MSSP to manage and monitoring a single firewall. And the daily SOC reviews, along with purpose-built reports, are specifically designed to meet regulatory requirements for cybersecurity monitoring with PCI, HIPAA, GLBA, and other compliance mandates. No other solution provides a comprehensive, cost-effective cybersecurity monitoring solution with full compliance support that is completely integrated with support from a trusted managed service provider.

Key Features

A turnkey cyber threat detection and compliance solution, fully configured and managed by security experts.

- Fully Hosted, Redundant, and Managed SIEM Platform
- In-Depth Behavioral and Anomalous Activity Monitoring
- Proprietary, Pre-Tuned Rules Matrix and Customized Rules for Your Organization
- Ongoing Rule Tuning and False Positive Reduction
- Customized, Enriched Notifications Including Remediation Guidance
- Integrated Global Threat Database from multiple Threat Feeds
- Automated Notifications, 24x7x365
- Daily SOC Review for Human Oversight
- Forensic Investigation and Compliance Assistance
- Tier 3 Incident Response Escalation Support
- Event Log Consolidation and Management
- Network, Virtualization, and Application Intelligence
- Configuration Change Management
- Over 2,200 Pre-Built Compliance and Standards-Based Reports
- Custom Report Creation and Scheduling
- Comprehensive Device Support
- Weekly Device Discovery Validation
- Audit / Exam Support

SECURITY OPERATIONS CENTER (SOC)

The Security Operations Center includes 24x7x365 automated monitoring and alerting through advanced log correlation, contextual analytics, big data analysis, and our custom-tuned rule database. Automated notifications are sent directly to your team for response. But many organizations do not have in-house security experts to properly analyze security data. Building and maintaining a SOC in-house is prohibitively expensive for most organizations. Hiring a team of expert security analysts is very costly and turnover is notoriously high for in-house SOC teams. In addition, many organizations do not consider the ongoing training and professional development costs required to keep up with ever-changing technologies and threats. To address this need, our solution automatically includes daily reviews by our SOC team.

SOC Features

Items Reviewed by SOC Analysts	
Individual reports manually and escalate anything suspicious or inaccurate information	✓
SIEM system and collector health, verifying proper operation and that events are correctly flowing from each device	✓
All automated Notifications to confirm they were triggered, sent, and delivered	✓
All High, Medium, and Low Incidents to ensure proper categorization, look for suspicious trends, and determine if any Medium or Low Incidents should be escalated	✓
Summary information for all logs from every device looking for any "hidden" activity that should have created an Incident	✓
Additional Features	
Incident Response Support	✓
Complies with PCI, HIPAA, and FFIEC guidelines	✓
Reviews performed once per day, 7 days per week, 365 days per year	✓

Our daily SOC review provides cost-efficient SOC monitoring and response that meets regulatory requirements for PCI, GLBA, and HIPAA. With this service, you receive an expert team of security analysts who perform daily review of your logs, reports, and notifications, 7 days a week, 365 days a year. Each day's review is tracked and logged to prove regulatory compliance. If any significant issues are found during the daily review, a manual notification is created and sent to you immediately.

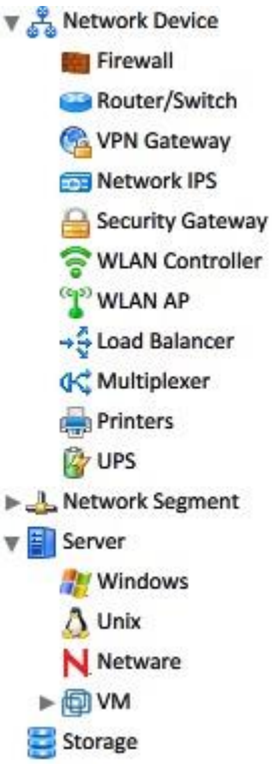
SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM)

Detailed SIEM Capabilities

With an integrated and cross-correlated view into your network, devices, apps and user logs, we simplify the collection of information that impacts your business. With a powerful analytics engine, automated Configuration Management Database (CMDB) and event consolidation, smart anomaly detection, identity and location binding, and flexible data management, we redefine the next generation of Security Information and Event Management.

SIEM Features

- Mainstream device support
- Event source monitoring
- Event log and network flow data consolidation
- Comprehensive, extensible analytics
- Network, virtualization, and application intelligence
- Identity and location intelligence
- Configuration and configuration change monitoring
- In-depth database security, availability and anomalous activity monitoring
- Powerful, layer 7 rules engine
- Real-time and historical cross-correlation
- Prioritized, valid security incidents with correlated and raw details
- Dynamic dashboards, topology maps and notification
- Real-time and long-term search with web-like query and iterative filtering
- Directory service integrated and custom asset and user grouping
- Compliance and standards-based reports
- Optimized event repository
- Event log data integrity secured by HMAC
- Unlimited online data retention
- As needed performance and coverage capacity



- Network Device
  - Firewall
  - Router/Switch
  - VPN Gateway
  - Network IPS
  - Security Gateway
  - WLAN Controller
  - WLAN AP
  - Load Balancer
  - Multiplexer
  - Printers
  - UPS
- Network Segment
- Server
  - Windows
  - Unix
  - Netware
  - VM
- Storage

Logging

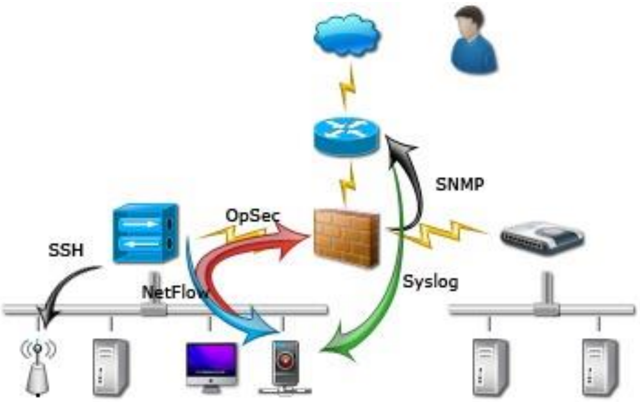
Event log management / security information event management (SIEM) is considered an IT best practice, and for regulated industries, an audit compliance requisite.

The challenge is how to consistently aggregate, decipher and normalize non-standard log formats; manage massive volumes of event log data for real-time and historic analysis; correlate and consolidate complex event log data to yield actionable intelligence; and maximize event log value to support IT service reliability.

Some equate log management to log aggregation, display, and storage – a simple approach that fails to address these complex challenges. Most SIEM products offer basic event consolidation, simple correlation rules, limited real-time analysis, poor reporting and investigation flexibility, and no identity or infrastructure context. Many still require special collectors, add-on modules, additional systems and significant expertise. None of this is required for our industry leading SIEM solution.

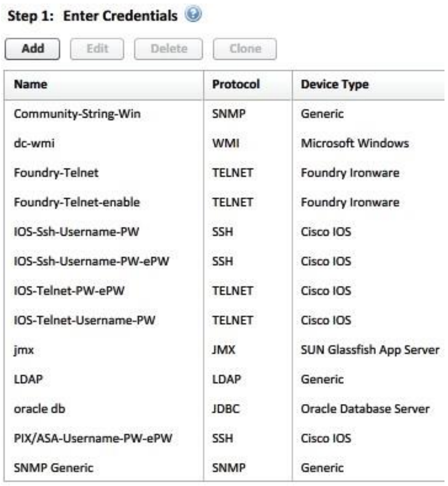
Collect, Parse, Correlate from anywhere

Supporting multi-vendor device sources and advanced parsing technology, the SIEM can collect, parse, correlate and store logs from virtually all your IT infrastructure sources. Our solution automatically interprets the device type and how to process the event logs as they are received.



- *Network activity logs* from Firewalls, Routers, Switches, VPN Gateways, Wireless LAN, Web/Mail Security Gateways, and Network IPS
- *Network resource utilization* and anomaly detection from network flow data
- *Server operating system* security logs from Windows, Unix, Linux and virtual machines
- Network infrastructure *application logs* from domain controllers, authentication servers, DNS and DHCP servers, and vulnerability management servers
- *User application logs* from web, application, and database servers

The SIEM intelligently categorizes the source of the log into different device groups such as Firewalls, Routers / Switchers, Wireless LAN Controllers, Printers, etc. It also groups into various server categories such as Windows, Unix, VMWare, and storage devices.



Step 1: Enter Credentials

Name	Protocol	Device Type
Community-String-Win	SNMP	Generic
dc-wmi	WMI	Microsoft Windows
Foundry-Telnet	TELNET	Foundry Ironware
Foundry-Telnet-enable	TELNET	Foundry Ironware
IOS-Ssh-Username-PW	SSH	Cisco IOS
IOS-Ssh-Username-PW-ePW	SSH	Cisco IOS
IOS-Telnet-PW-ePW	TELNET	Cisco IOS
IOS-Telnet-Username-PW	TELNET	Cisco IOS
jmx	JMX	SUN Glassfish App Server
LDAP	LDAP	Generic
oracle db	JDBC	Oracle Database Server
PIX/ASA-Username-PW-ePW	SSH	Cisco IOS
SNMP Generic	SNMP	Generic

Automatic Discovery

Discovery of your network infrastructure and its resources is accomplished using intelligent scanning methods. The SIEM employs a smart scan, which iteratively learns only about the live devices in your network. Since only live devices are traversed, it is much faster than other traditional methods of network security and device discovery.

It also supports a range scan method where each machine in the range is first pinged and then an attempt is made to do full discovery using the given credentials. Once the capabilities of the devices are known, the security information which can be fetched from those devices are automatically determined.

Multi-Faceted Data Collection

Collection of logs from a variety of devices and applications is accomplished with virtually all agent-less and agent-based data collection methods, including:

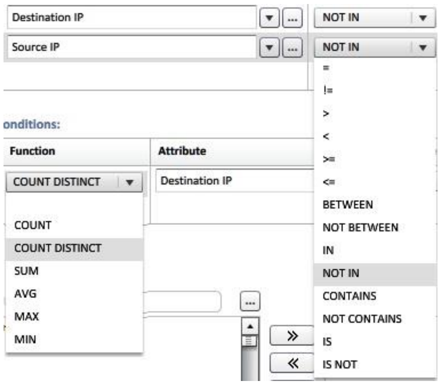
- SNMP
- Syslog
- Windows Management Instrumentation (WMI)
- Microsoft RPC
- Cisco SDEE
- Checkpoint LEA
- JDBC
- VMWare VI-SDK
- JMX
- Telnet
- SSH
- HTTPS
- IMAP / IMAP over SSL

Powerful Analytics for Real-time Correlation and Alerting

The SIEM can detect your network services and profile network traffic from network flows and firewall logs. An advanced analytics engine detects patterns in data over a rolling time window taking into account very complex patterns. This includes combined patterns of network, system, application and user activity. The built-in analytics engine can be easily extended using XML-based definitions.

We have more than 650 built-in rule classes covering hundreds of scenarios such as:

- Host scans, port scans, fixed-port host scans, denied scans, and other traffic anomalies
- Network device and server logon anomalies
- Network access anomalies from VPN, domain controller and wireless logons
- Web server and database access anomalies
- Rogue workstations, mobile devices, and WLAN APs etc. from DHCP logs
- Account lockouts, password scans, and unusual failed logon patterns
- Botnets, mail viruses, worms, DDOS, and other day zero malware from DNS, DHCP, web proxy logs, and flow



The analytics engine patterns are comprehensive and allow us to build complete Boolean operators and nested sub-pattern rules:

- Sub-patterns connected in the time dimension by operators such as AND, OR, FOLLOWED_BY, AND_NOT, NOT_FOLLOWED_BY
- Each sub-pattern can apply condition operators such as =, !=, BETWEEN, IN, NOT IN, IS, IS NOT, etc
- Each sub-pattern can filter and apply aggregation operators such as AVG, MAX, MIN, COUNT, and COUNT DISTINCT
- The thresholds can be static or statistically derived from automatically profiled data

Compliance Automation

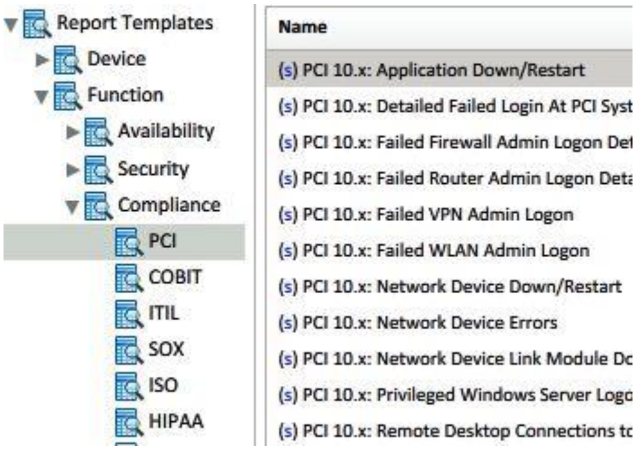
The SIEM offers full log aggregation, real-time event correlation, and online data retention with rules and reports mapped to compliance standards such as PCI, FFIEC, SOX, and HIPAA.

By incorporating an automated CMDB, statistical profiling, and true identity binding for complete access records, The SIEM helps automate your internal audit and control processes.

Standards and compliance are all about implementing policies, procedures, and technologies that reduce business risk, as well as being able to efficiently validate that controls are working according to stated policy expectations and mandated requisites. Beyond setting policy and procedures, many tools in an IT’s management portfolio must support compliance efforts.

The question then becomes finding the right technologies that best automate control verification and documentation, as well as those that streamline internal and external audit challenge/response processes. Compliance considerations for IT management tools should include the means to:

- Validate a broad set of policies across technologies
- Deliver on-demand results to auditor inquiries
- Readily obtain applicable data and documentation
- Normalize compliance-relevant data across disparate systems
- Diminish compliance liabilities and audit duration
- Meet auditing and data management standards
- Identify control gaps and prioritize incident response
- Adapt to existing security, governance and auditing processes
- Respond to complex and rapidly changing environments

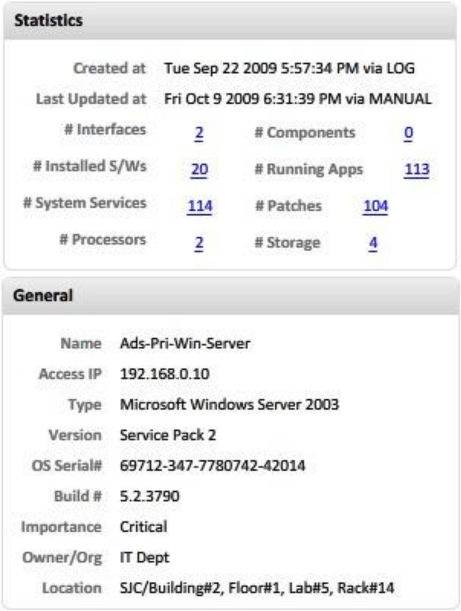


- Report Templates
  - Device
  - Function
    - Availability
    - Security
    - Compliance
      - PCI
      - COBIT
      - ITIL
      - SOX
      - ISO
      - HIPAA

Name
(s) PCI 10.x: Application Down/Restart
(s) PCI 10.x: Detailed Failed Login At PCI Syst
(s) PCI 10.x: Failed Firewall Admin Logon Det
(s) PCI 10.x: Failed Router Admin Logon Deta
(s) PCI 10.x: Failed VPN Admin Logon
(s) PCI 10.x: Failed WLAN Admin Logon
(s) PCI 10.x: Network Device Down/Restart
(s) PCI 10.x: Network Device Errors
(s) PCI 10.x: Network Device Link Module Dc
(s) PCI 10.x: Privileged Windows Server Logo
(s) PCI 10.x: Remote Desktop Connections tc

Compliance Support

The SIEM satisfies all of the compliance considerations shown here with built-in dashboards, analytics, and reports mapped to leading standards and compliance best practices.



Statistics

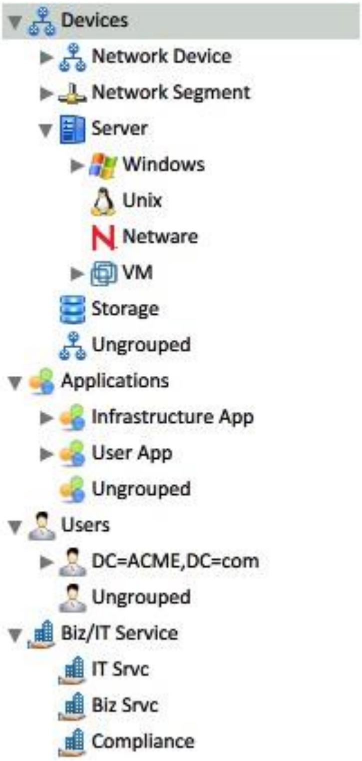
Created at	Tue Sep 22 2009 5:57:34 PM via LOG		
Last Updated at	Fri Oct 9 2009 6:31:39 PM via MANUAL		
# Interfaces	2	# Components	0
# Installed S/Ws	20	# Running Apps	113
# System Services	114	# Patches	104
# Processors	2	# Storage	4

General

Name	Ads-Pri-Win-Server
Access IP	192.168.0.10
Type	Microsoft Windows Server 2003
Version	Service Pack 2
OS Serial#	69712-347-7780742-42014
Build #	5.2.3790
Importance	Critical
Owner/Org	IT Dept
Location	SJC/Building#2, Floor#1, Lab#5, Rack#14

CMDB and Change Management

The fully automated and comprehensive CMDB is capable of discovering, intelligently grouping and maintaining a smart inventory of network assets, software, patches, users and directory objects. And we build all this directly from your infrastructure and trusted sources without requiring agents.



CMDB Features

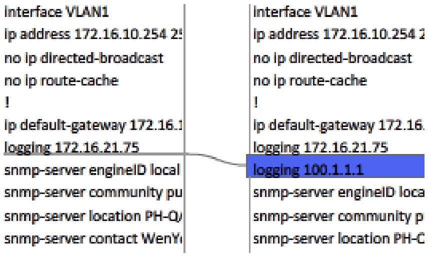
The SIEM discovers, records, monitors, and reports on all your network assets, both physical and virtual. Our solution allows organizations to quickly and easily:

- Track hardware and software assets
- Understand what software is installed and what is running
- Analyze system utilization by application and respective processes
- Associate asset allocation with users, groups and services
- Monitor network application use and resource consumption by user or group
- Track blacklist or whitelist applications
- Assess and integrate patch deployment and vulnerability issues
- Identify shelfware and license reduction opportunities
- Plan capacity and migration options for consolidation projects
- Prepare for audits

Change Management Features

As a part of Change Management, the following scenarios can be detected:

- Monitor network device configurations for startup configuration change and difference between startup and running configuration
- Monitor installed software differences for new software installations and existing software uninstalls
- Monitor active directory user/group membership changes
- Store versioned configuration in database
- Alert on configuration changes, tied together with admin IP and workstation
- Alert on unauthorized changes
- Report on configuration change history, optionally by business service



```
interface VLAN1
ip address 172.16.10.254 25
no ip directed-broadcast
no ip route-cache
!
ip default-gateway 172.16.1
logging 172.16.21.75
snmp-server engineID local
snmp-server community pu
snmp-server location PH-Q/
snmp-server contact WenY
```

```
interface VLAN1
ip address 172.16.10.254 2
no ip directed-broadcast
no ip route-cache
!
ip default-gateway 172.16.
logging 172.16.21.75
logging 100.1.1.1
snmp-server engineID loca
snmp-server community p
snmp-server location PH-C
```

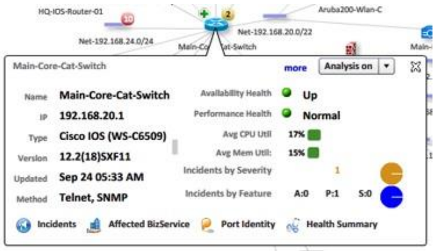
Running and Startup Configuration

Change Management also includes a discovery module capable of detecting the “start-up” and “running configuration” from network devices such as routers, firewalls and switches over a historical period. It intelligently detects the difference between the startup configuration and running configuration and differences between various startup configurations over a long period of time.

Whenever a change is detected, it creates a incident and notifies the administrator about the change. With this intelligence, the administrator can keep track of the changes done which are unauthorized configuration changes to their core network devices. The administrator can look at the configuration of any historical time interval, by selecting the revision of that configuration.

Configuration Diff

It is also possible to view the versioned configuration at any time, and is possible to search for specific keywords in the configuration. Using an intuitive UI, the administrator can also diff between any version of the running configuration. With this feature, it's very easy to detect changes and to pinpoint each specific change in the configuration.



Main-Core-Cat-Switch more Analysis on ▾ ☒

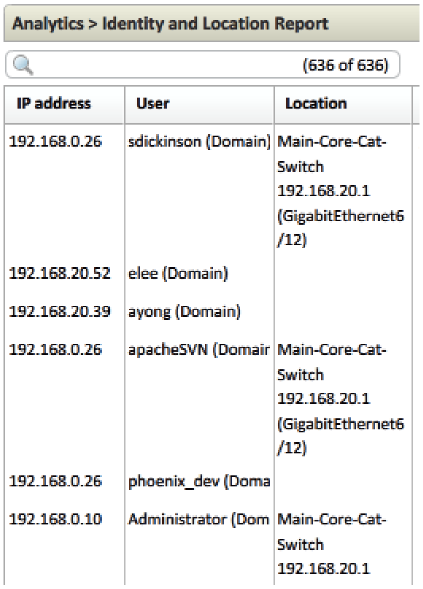
Name Main-Core-Cat-Switch
IP 192.168.20.1
Type Cisco IOS (WS-C6509)
Version 12.2(18)SXF11
Updated Sep 24 05:33 AM
Method Telnet, SNMP

Availability Health ● Up
Performance Health ● Normal
Avg CPU Util 17%
Avg Mem Util: 15%
Incidents by Severity 1
Incidents by Feature A:0 P:1 S:0

Incidents Affected BizService Port Identity Health Summary

Incident Notification Overlay

The system keeps track of the incidents occurring on your network using an advanced analytics engine in real-time. The user can write a rule to detect any simple or complex scenario and the system will create the correct alerts applicable to that scenario. The visualization engine automatically keeps track of these incidents and overlays them on the main graph nodes so that the user can get a rapid visual cue of network issues at any time. The tool has the option of showing all incidents – critical (red) incidents, warning (yellow), or informational (green) incidents. These topology incident overlays are automatically updated by the user interface. It's also possible to obtain full details on each incident, by just clicking on the incident count indicator button.



Analytics > Identity and Location Report

(636 of 636)

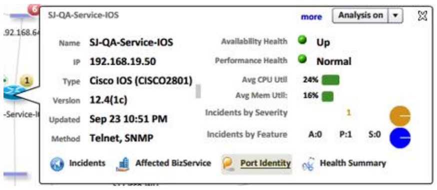
IP address	User	Location
192.168.0.26	sdickinson (Domain)	Main-Core-Cat-Switch 192.168.20.1 (GigabitEthernet6/12)
192.168.20.52	elee (Domain)	
192.168.20.39	ayong (Domain)	
192.168.0.26	apacheSVN (Domair	Main-Core-Cat-Switch 192.168.20.1 (GigabitEthernet6/12)
192.168.0.26	phoenix_dev (Doma	
192.168.0.10	Administrator (Dom	Main-Core-Cat-Switch 192.168.20.1

Identity Location Management

Using an innovative identity and location-to-event binding technology, the SIEM automatically associates IP addresses to machine names, MAC addresses, switch VLAN IDs, logged-on users and directory objects. Now complete who and where details are maintained as action records, irrespective of the use of shared credentials, including the network the user has connected to and by what method.

Know the User and Location – Not Just their IP Address

Using identity and location-to-event binding technology, the system intelligently associates IP addresses to machine names, MAC addresses, switch VLAN IDs, logged on user name, and directory identity. It automatically identifies a user's location in terms of nearest WLAN AP, controller, VPN gateway, Layer 2 switch port, and associates primary logins to secondary logins in order to identify the real user behind administrative accounts. With this information, any IP address can be automatically associated to a specific user, on a specific server/laptop, and connected to the network via a specific access method: AAA, VPN or switch.



SJ-QA-Service-IOS more Analysis on ▾ ☒

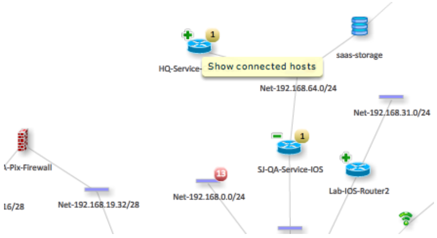
Name SJ-QA-Service-IOS
IP 192.168.19.50
Type Cisco IOS (CISCO2801)
Version 12.4(1c)
Updated Sep 23 10:51 PM
Method Telnet, SNMP

Availability Health ● Up
Performance Health ● Normal
Avg CPU Util 24%
Avg Mem Util: 16%
Incidents by Severity 1
Incidents by Feature A:0 P:1 S:0

Incidents Affected BizService Port Identity Health Summary

By binding user identity and location to events, full who and where details are maintained as an action record irrespective of the use of shared credentials. Now investigating operational issues, change anomalies, security breaches and violations, and reporting on internal user actions are no longer obstacles.

These actionable identity and location details are presented, used and always available in dashboards, topology maps, incidents, enterprise search, rules and reports. As changes in directory objects, new network devices and systems, or known or unknown users access your infrastructure, all the pertinent location and identity information is current and maintained for real-time and historic analysis.



Port Identity

The system keeps track of the MAC to VLAN ID mapping in switches and routers, so that it can map an IP address to a specific machine name, MAC/VLAN ID, and logged on user.

In this way, the SIEM provides the server (or host) connected to each port along with the corresponding IP address, user (VPN, Domain or AAA), location (switch or wireless controller), and the last and first seen time information.

Layer 2 Topology with Location

Now you can visualize your layer 2 topology for each switch or router along with VLAN ID and server information directly in the SIEM Topology View. Click on the '+' icon on any switch or router in the Topology view, and the latest layer 2 topology information for that device will be shown immediately.

The dynamic user identity and location mapping also helps to improve incident response time, investigations, planning, and operational changes. The identity and location information along with the historic event details can be exported into PDF or CSV formats and emailed to the applicable administrator.