SureLog

International Edition //2017

NEXT-GENERATION SIEM

SURELOG: INGRATED SIEM AND LOG MANAGEMENT

- ANET Company Overview
- What is SureLog?
- Benefits
- Advantages
- SureLog Demo
- Q & A

ANET COMPANY PROFILE

- Founded 2008
- +280 International Customers
- Energy, Finance, Education, Government, Manufacturing, Retail, Transportation, Tourism, Healthcare
- 10 + Partners World-Wide

WHY SURELOG

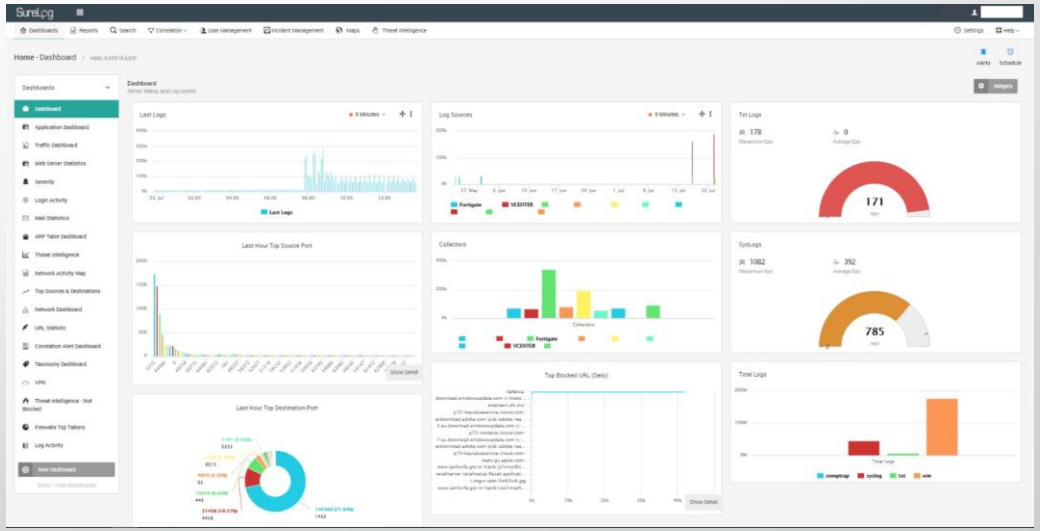
- *With SureLog, You can quickly investigate alerts or possible breaches to analyze your threat landscape with minimal security resources.*
- Audit reporting to meet compliance requirements such as PCI DSS, HIPAA, FFIEC, and others
- "Log monitoring and security intelligence allows you to see logical network changes that could be a symptom of an attack,"
- Easy to use interface

HOW SURELOG HELPS

- Detect advanced security threats
- Investigate suspicious activity
- Monitor for unauthorized access
- Meet compliance objectives
- If your information gets into the wrong hands, it can lead to identity theft and other similar issues.
- Reduction of capital and operational cost
- Early detection of security incidents
- Provide comprehensive and efficient reporting
- Deliver crucial operational efficiency

INTEGRATED NEXT-GENERATION SIEM AND LOG MANAGEMENT

- Multi-Functional Security Management Platform
- Integrated Security and Log Management Platform
- Real-time security management across thousands of devices, including applications as diverse as satellite, cryptography and security devices.
- Granular control over any type of event definition, with the ability to collect,
- Normalizes and integrates data from any device, application or service.



INTEGRATED NEXT-GENERATION SIEM AND LOG MANAGEMENT

SureLog delivers:

- Next-generation SIEM,
- Log management
- Intelligent security search
- Simple, easy to-install
- Cost-effective solution
- Providing immediate value

for security and compliance to organizations of any size.

INTEGRATED NEXT-GENERATION SIEM AND LOG MANAGEMENT

Highly flexible architecture and support for high volume data throughput rates.

- Superior correlation engine
- Definition of complex combinations of events
- Easy creation and customization of correlation rules
- Graphical, drag-and-drop rule creator
- Sophisticated threat intelligence management

INTEGRATED NEXT-GENERATION SIEM AND LOG MANAGEMENT

Supports 155 brands, 350 devices, log categorization into 1513 groups
Event Taxonomy comprises more than 200 fields

Security Information and Event Management

Advanced Correlation Engine

Security Operations Center

Log Management

Log Forensics

Threat Intelligence

INTEGRATED NEXT-GENERATION SIEM AND LOG MANAGEMENT

Sophisticated threat intelligence management allows SureLog to dynamically collect black lists and update its database.

Security Reporting

Real-Time Alerts

Event Correlation & Analysis

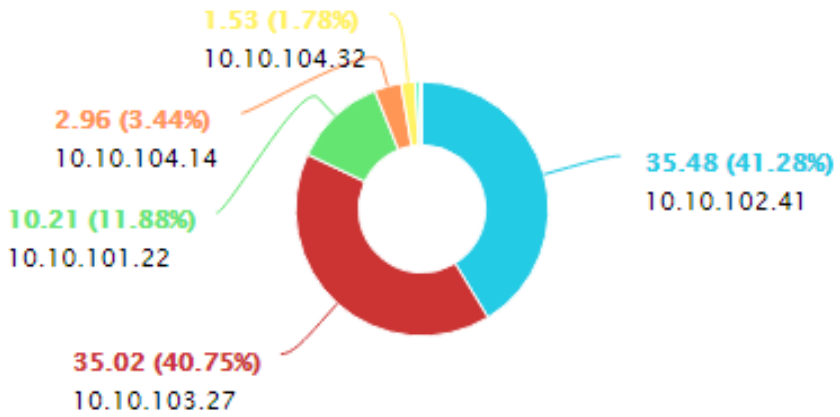
Compliance Management

Rich Taxonomy

Protecting Against Insider Attacks

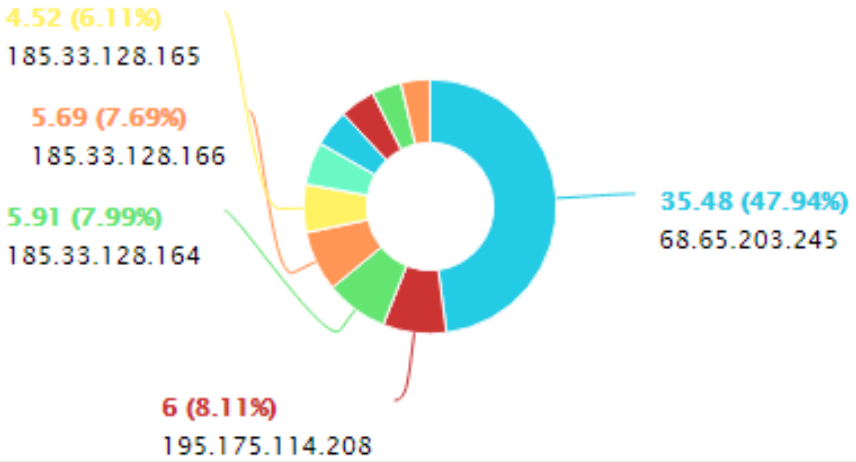
Last Hour Top SENT Source

Firewall Events (SENT) Top:10

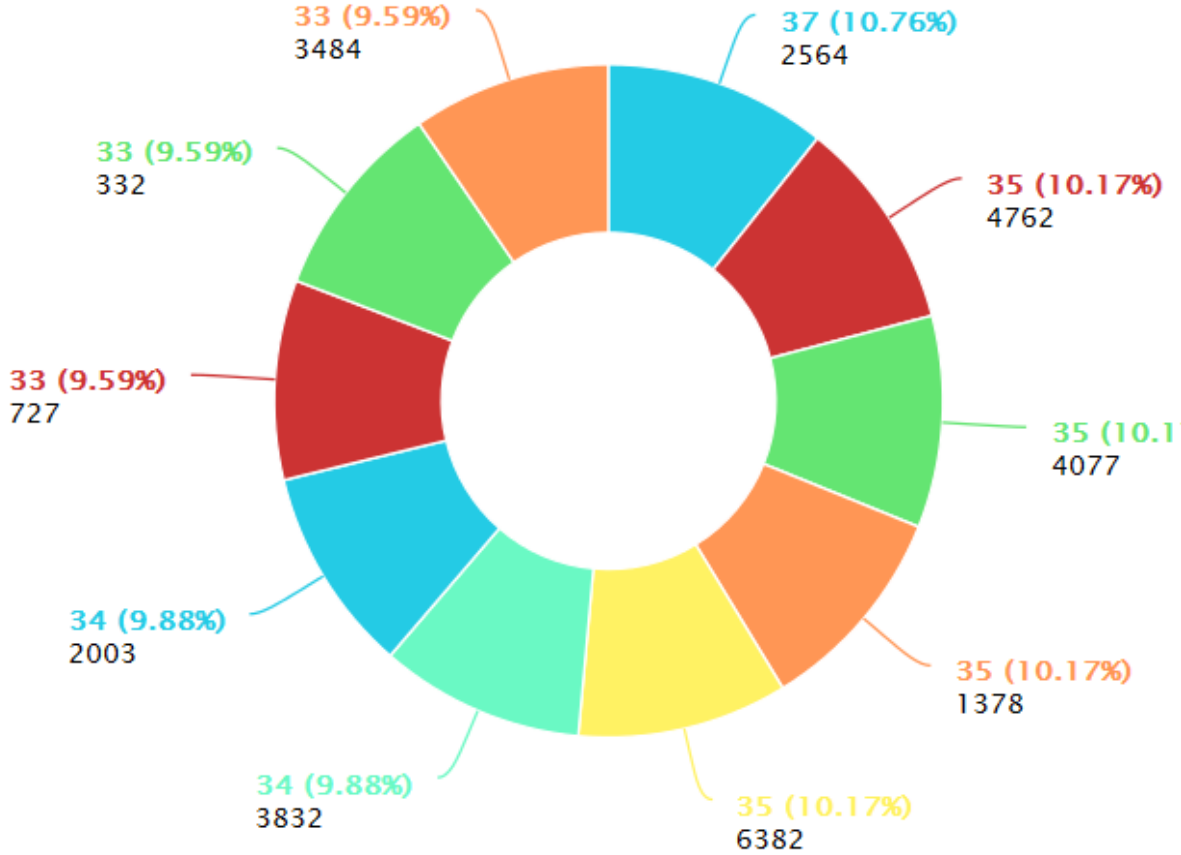


Last Hour Top SENT Destination

Firewall Events (SENT) Top:10



SourcePort Statistics



SourcePort	count
2564	37
4762	35
4077	35
1378	35

SURELOG ADVANTAGES

Unified Security Intelligence Platform

SIEM, Log Management with Host and Network Forensics

- SureLog is a web based, agent-less, SIEM, log analysis and reporting software.
- Monitors, collects, analyzes, and archives logs and monitoring parameters from enterprise-wide network perimeter security devices, Routers, Switches, SNMP Devices, VM, DHCP servers, Linux or Windows Systems.

SURELOG ADVANTAGES

CORRELATION ENGINE

- Leverages predefined rules to identify attack patterns and malicious behavior
- Automates analysis so that attacks can be quickly identified and breaches can be quickly contained

CORRELATION ENGINE ADVANTAGES

- SureLog is fast
- Can trace multiple logs with different types within a defined time frame
- SureLog can correlate different logs
- SureLog can trace a log being created with desired parameters or not
- SureLog can audit privileged user activity
- SureLog can correlate privileged user behavior with specific network activity
- Correlation rule editor is simple to use
- SureLog supports multiple filtering options
- Compression-based correlation feature

SURELOG ADVANTAGES

SIMPLE CORRELATION RULES

- User Authentication
- Attacks on theNetwork
- VirusDetection/Removal
- Web Server
- Monitored Log Sources
- User Activity Reports
- Access Reports
- Malware
- Email activity
- Web Content
- User Account activity

SURELOG ADVANTAGES

ADVANCED CORRELATION RULES

- Attack followed by account change
- Scan followed by an attack
- Detects An Unusual Condition Where A Source Has Authentication Failures At A Host But That Is Not Followed By A Successful Authentication At The Same Host Within 2 Hours
- Pattern matching: "files accessed by a starting process within 20 minutes" pattern is matched within 1 hour with the same process name and same files on another machine
- If there is an access from the internal network with the same user name while the VPN connection is open to a file accessed by the same VPN user

SIMPLE CORRELATION RULE CREATION

Add Rule

LOG

Observed Rule

Create Rule

Threshold Rule

Create Rule

BEHAVIORAL

Trend Monitor Rule

Create Rule

Statistics Rule

Create Rule

MONITORING

Value Changed Rule

Create Rule

Never Seen Before Rule

Create Rule

LIST

Add List Rule

Create Rule

EXPERT

Expert Rule

Create Rule

Home - Correlation

Reports | Alerts | Schedule

Reports

- Correlation
  - Firewalls
  - General Applications
  - WEB Server
  - Network Monitor
  - Operating Systems
  - Others
  - Cisco
  - Windows
  - Performance Monitoring
  - Threat Intelligence
- Expert

Show All Rules

CorrelationWizard and Template Rules

Add Rule

Rule Name | Rule Type | Passive | Filter

1 2 3 Next Last

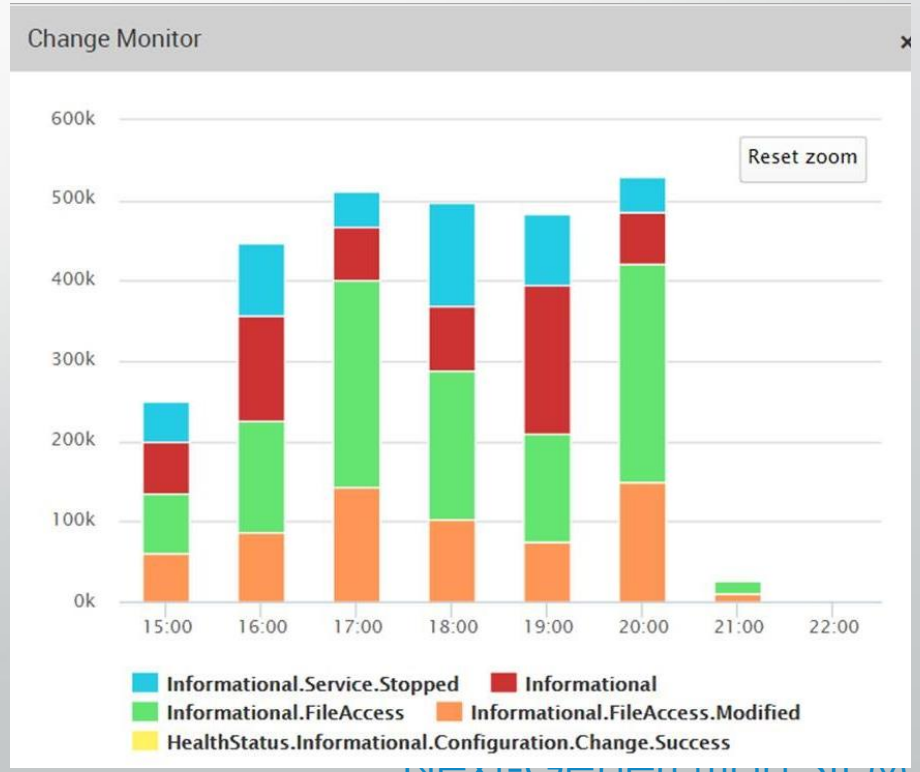
	Rule Type	Rule Name	Rule Description	Rule Category	Rule	Edit
☐	Wizard	Repeat Attack-Firewalls	Alert on 15 or more Fire...	Firewalls	Show Rule	Copy Rule Edit Delete
☐	Wizard	Check whether there are 5 ...	Check whether there ar...	Firewalls	Show Rule	Copy Rule Edit Delete
☐	Wizard	Suspicious Post from Untr...	Files with executable ex...	WEB Server > Security	Show Rule	Copy Rule Edit Delete
☐	Wizard	test		Others	Show Rule	Copy Rule Edit Delete
☐	Wizard	Warn once, if more than 10...	Warn once, if more than...	Others	Show Rule	Copy Rule Edit Delete
☐	Wizard	Warn, if reconnaissance att...	Warn, if reconnaissance...	Others	Show Rule	Copy Rule Edit Delete
☐	Wizard	Inform the source IP which...	Inform the source IP wh...	Others	Show Rule	Copy Rule Edit Delete
☐	Wizard	Logon attempts in not bus...	Logon attempts in not b...	Others	Show Rule	Copy Rule Edit Delete

ALL SURELOG ADVANTAGES

TAXONOMY

Mapping of information from heterogeneous sources to a common classification. A taxonomy aids in pattern recognition and also improves the scope and stability of correlation rules

- Compromised->RemoteControlApp->Response
- HealthStatus->Informational->HighAvailability->- LinkStatus->Down
- IPTrafficAudit->IP Too many fragments
- PSpoofAccess->ICMP CODE Redirect for the Host
- FileTransferTrafficAudit->Authentication Failed
- NamingTrafficAudit
- Session->Start
- ICMP Destination Network is Administratively Prohibited



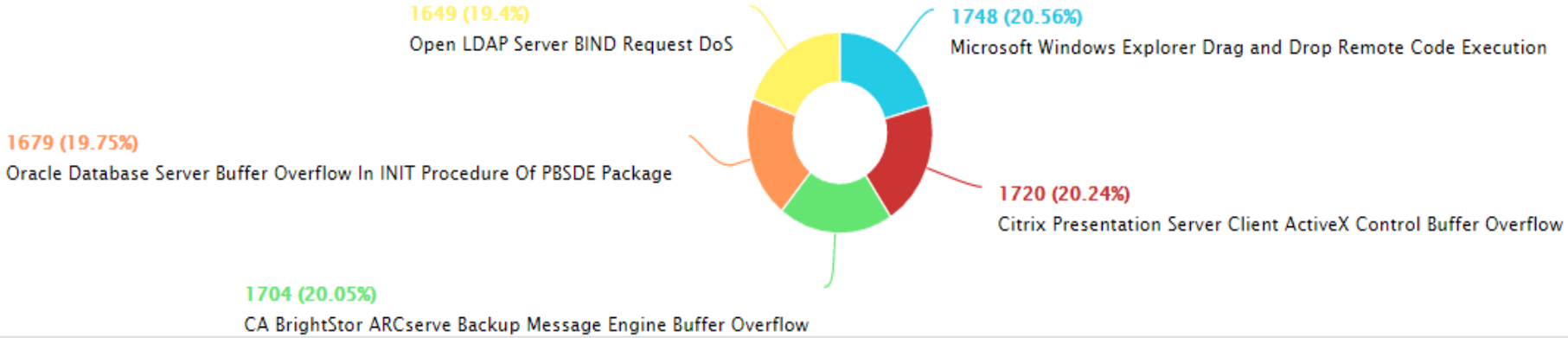
Deep Security Intrusion Prevention

Intrusion Prevention

Widgets

Top 10 Resons For Detected IPS Events

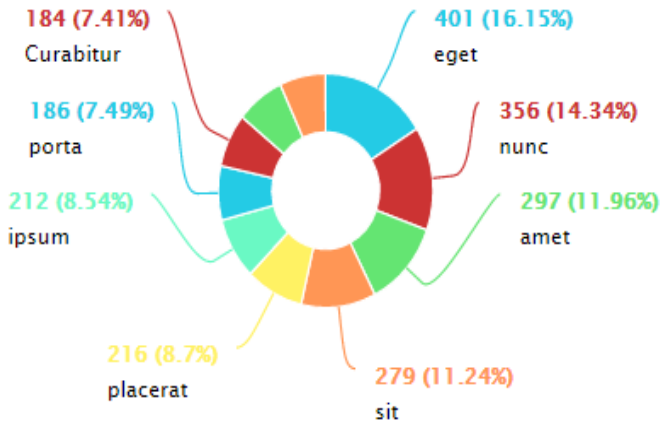
Intrusion Prevention (Name) Top:10



Show D

Top Hosts For Prevented IPS Events

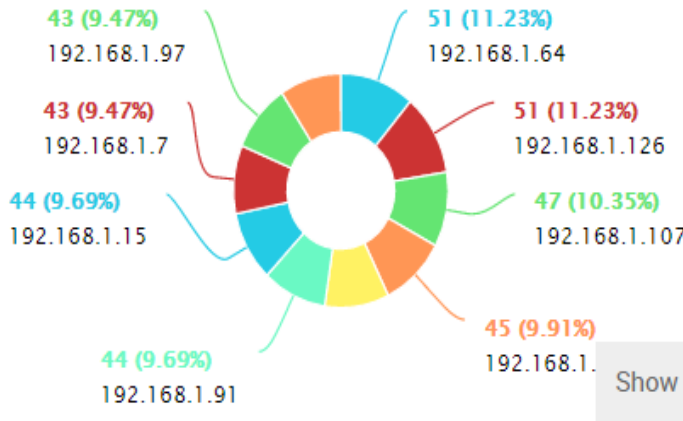
Intrusion Prevention (SrcName) Top:10



Show Detail

Top 10 Source IPs For Detected IPS Events

Intrusion Prevention (SourceMachine) Top:10

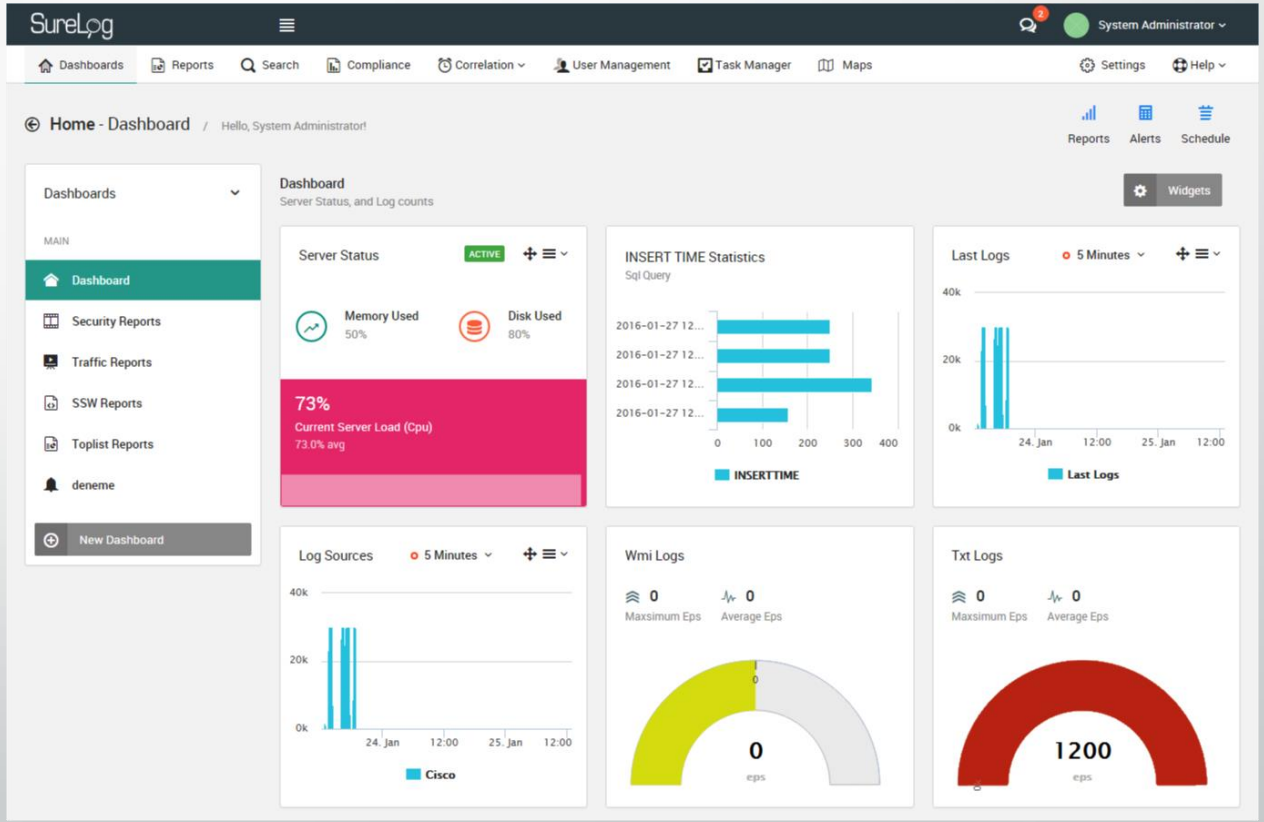


Show D

SURELOG BENEFITS

SureLog is the Fastest Integrated Log Management & SIEM software solution with strong correlation engine.

- Decision speed
- Continuous learning
- Real-time alerting and historical forensics



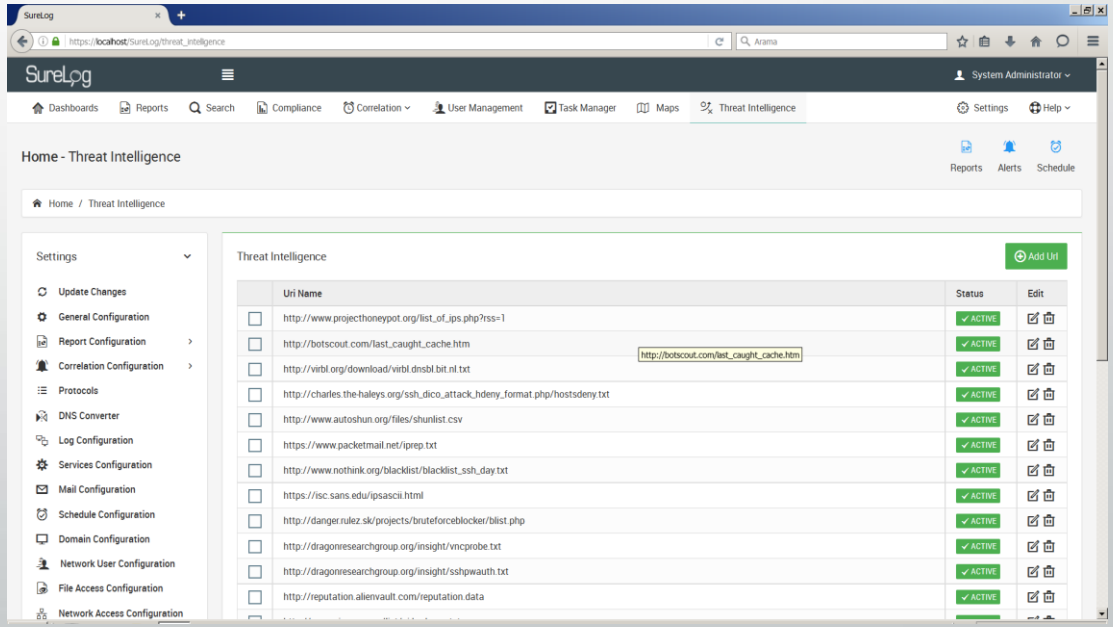
SURELOG BENEFITS

Customers who have used SURELOG have experienced:

- Improved productivity.
- Higher business operations uptime.
- Lower IT costs.
- Improved business performance.
- Ability to meet Service Level Agreements.
- By correlating customer service level commitments you will have better visibility to required response times.
- Monitor applications.
- Monitor ecosystem business services, not just devices.

SURELOG THREAT INTELLIGENCE BENEFITS

- SureLog aggregates more than 1 million threat information from numerous sources and applies automated confidence algorithms to produce intelligence and reputation data. A large library of openly available information lists, which is consolidated, classified and automatically analyzed to derive intelligence and reputation information with confidence
- Sources include:
  - Botnet Domains
  - Botnet URL's
  - Malware Domains
  - Malware URL's
  - Email Phishing
  - Phishing Domains
  - Phishing URL's



SURELOG BENEFITS

DEMO

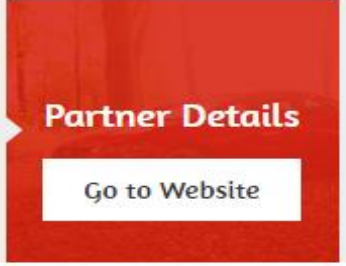
- Online One-to-One demo is available
- Registered on site demo is also provided

PRICING

- Based on EPS and log source

ESTEEMED CLIENTS

HONDA



BAYER

BRITISH AMERICAN TOBACCO

FOX

e·on

Roche

Pierre Fabre

LESAFFRE

INVEST AZ

Skipsteknisk

ENERJİSA

EVYAP

Santander

adidas

DAIKIN

HONDA

BAYER

BRITISH AMERICAN TOBACCO

FOX

ENERJİSA

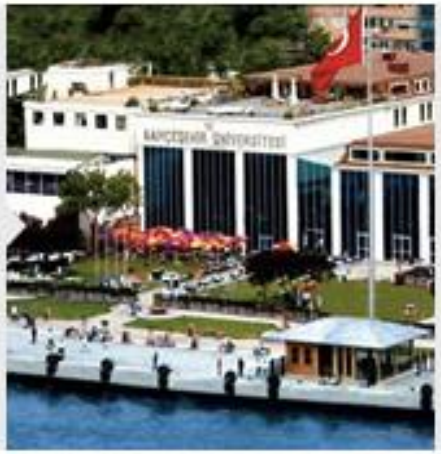
Roche

Pierre Fabre

LESAFFRE

INVEST AZ

Skipsteknisk



EVYAP

ISBI

KOROZO

mavi

NAMET

ПART

PEKİN & PEKİN

Palit

TURK TELE KOM

UN

Q & A

SureLog

SURELOG: NEXT-GENERATION SIEM

THANKYOU