VALIANT COMMUNICATIONS

NEXCON TELECOMUNICACIONES

VCL-2143

MouseTrap™ IP Network Intrusion Detector

Introduction:

Valiant's MouseTrap™ is an essential security tool that sits behind the firewall equipment emulating a "decoy server" / a "honeypot" in a secure environment to detect firewall breaches and unauthorized intrusions. Valiant's MouseTrap™ forms an essential part of the digital forensics kit that may be installed in secure critical infrastructure such as in Sub-Stations, Smart Grid Distribution Systems, Airport and Railway IT Networks, as well as Financial Infrastructure such as Banks and Payment Processing Gateways to "alert" the network administrator of unauthorized intrusions or a firewall breach.

Valiant's MouseTrap™ finger-prints the complete credentials of the hostile entity (or entities) who have entered the protected network by maintaining a complete log of its (their) credentials such as IP address, Domain and location of the intruder. Each log entry is time-stamped with the exact time and date of each such incident when the unlawful intrusion occurred.

Access to MouseTrap™ is password protected with advanced security features that can be customized to meet and exceed the security requirements of even the most demanding network administrator. The MouseTrap™ can optionally be managed centrally from a RADIUS Server to provide enhanced levels of access security and centralized password management and control. All MouseTrap™ logs are stored in the non-volatile memory of the device that can store up to ten million logs that are over-written on a FIFO basis.

Application:

- Utilities: Electric generation, transmission and distribution
- Smart Grid Distribution Systems, SCADA multi-drop networks
- Oil & Gas production, pipelines
- Railway and Airport Infrastructure
- Financial Infrastructure Banks, Payment Processing Gateways
- Law Enforcement.

Universality of Purpose and Ease of Use:

- Seamless scalability
- Infrastructure neutral
- Transparent to network and applications
- Easy installation and management

Interfaces:

- Total Number of System Interfaces: 2
  - 1 x 10/100 RJ45 MouseTrap™ network interface
- Auto MDI/X (straight or crossover Ethernet cable correction)
- USB serial port for local access and configuration.
-

Security Features:

Unlawful Entry and Intrusion Detection

- SNMP trap generation as well as an external (dry contact) alarm output which may be wired to a user preferred audio or visual alarm annunciator device.
- Sounds and sends an alert when the IP address or IP Domain from the user programmed Black List.
- Non-volatile Access Log with capability to "fingerprint" all access attempts and keep a log of the IP addresses and Domain for forensic analysis by the network administrator.
- **Filters:** Port (Soft) Based, IP Address based and IP Domain based
- **White List option:** Sounds the alarm / sends an alert when the IP address / IP domain is outside the user programmed white list
- **White List and Black List options:** Sounds the alarm / sends an alert when the IP address / IP domain is in the user programmed black list
- Resistance to Denial of Service (DoS) Attack

Outbound Traffic Monitoring:

Ability to scan outbound traffic and to alert the network administrator if an unauthorized data transmission taking place from any of the IEDs such as RTUs, PMUs, Bay Control Units, Servers etc. which may be considered as a potential security threat. This feature is useful in detecting "moles" or "malicious firmware" in any of the IEDs that may be unlawfully transmitting data to any destination (i.e. IP address) which has not been authorized by the network administrator. Useful tool in enhancing cyber-security of Sub-Stations, SCADA, Oil and Gas and Financial Infrastructure such as banks etc.

Mousetrap™ complements Valiant's Firewall Security solutions for enhancing firewall resilience and network security:

VCL-2143, MouseTrap™ may be used in conjunction with VCL-2142, VCL-2142E and VCL-2778, Gigabit Ethernet Failover Switch to provide 1:1 Firewall Redundancy and Automatic Failover in the event of the detection of a "Firewall" breach by switching to the redundant "Firewall" equipment.

Valiant's VCL-2142 and VCL-2142E are integrated firewall solutions with extremely advanced features that may be installed to secure critical infrastructure such as Sub-Stations, Smart Grid Distribution Systems, Airport and Railway IT Networks as well as Financial Infrastructure such as Banks and Payment Processing Gateways. This solution supports Deep Packet Inspection, Per-frame/packet authentication, Resistance to Denial of Service (DoS) Attack.

VCL-2778, is a Failover Gigabit Ethernet Switch which provides 1+1 Automatic Ethernet Failover Protection between an "active" and "standby" equipment, such as firewalls and routers that are connected to the network through an Ethernet Interface.

Power:

Power: 15V DC to 60V DC.

- Power consumption: 9W at maximum load
- 100~240VAC, 50/60Hz (external adapter)
- 85VDC ~ 250VDC (external adapter)

Security, Monitoring and Access Control:

- Password Strength Monitor
- Device Management and Alarm Monitoring
- Command Line Interface - Telnet, SSH with clear text disable
- SNMPv2 Alarms
- Alarm condition detection/reporting (traps/SNMP alarm table)
- Alarm Relay for connecting External Audio / Visual Alarms
- Syslog, Audit Log,
- Secure Boot
- Encrypted Firmware Updates
- Password Protection with password strength monitor
- RADIUS Password Authentication
- SSH (Secure Access Control) with encrypted Password Protection

LED Indicators:

- System Status LED and Power LED

Environmental:

- Operational:
  - Temperature -20C to +60C (-4F to 140F),
  - Humidity up to 95% R.H. (Non-condensing at 60C)
  - Cold start: temperature -10C
  - Maximum Operational Humidity 95% R.H. (Non-condensing)

Regulatory:

- Emissions: As per CISPR 22 / EN55022 Class A
- FCC: Part 15 Subpart A
- Immunity: EN55024, EN61000
- RoHS
- CE

VCL-MouseTrap User Interface

Compliance/ Regulatory:

- Meets CE requirements
- Complies with FCC Part 68 and EMC FCC Part 15 and CISPR 22 Class A
- Operation ETS 300 019 Class 3.2
- Operation ETS 300 019 Class 3.2
- Transportation ETS 300 019 Class 2.3

Physical and MTBF:

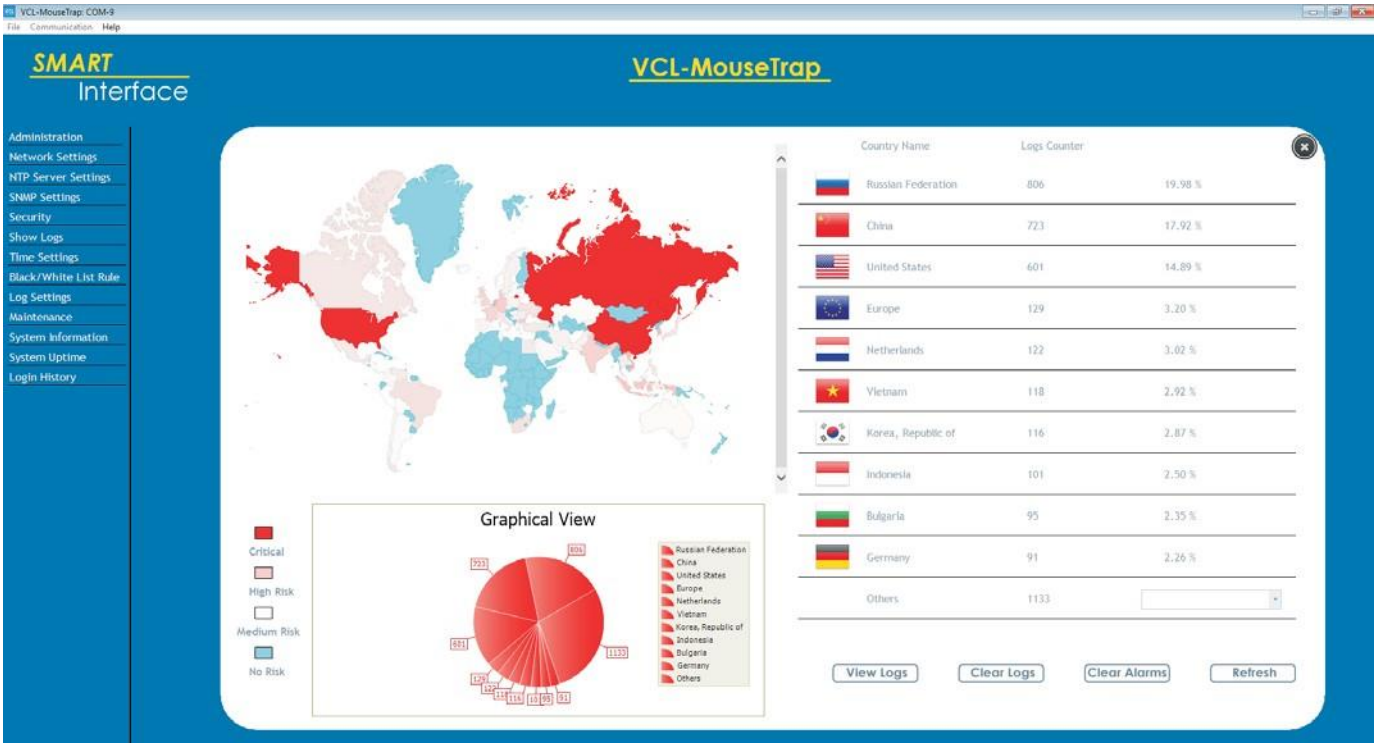
DIN-Rail Industrial (IP50) Chassis.
Optional, 1U, Ruggedized Industrial 19-Inch Chassis.
Height x Depth x Width: 40 mm x 170mm x 168 mm
Weight: <1 Kg
MTBF: ≥ 280,000 hours

Ordering Information (Base Unit):

Part No.:	Description
VCL-2143	MouseTrap™ IP Network Intrusion Detector DIN Rail Mounting Version *Add Power Supply
VCL-2144	SMS alert option DIN Rail Mounting Version *Add Power Supply

*Add Power Supply Options:

DC024	1 x 24V (9~32) DC Power Supply Input
DC048	1 x 48V (18~60) DC Power Supply Input
DC110	1 x 110V (80~150) DC Power Supply Input (with external adaptor)
DC220	1 x 220V (180~290) DC Power Supply Input (with external adaptor)
AC120	1 x 120V (90~260) AC Power Supply Input (with external adaptor)



NEXCON Telecomunicaciones
Calle Cidro 2 Planta 2 Oficina 1
28044-Madrid
Tfn: +34-915098994
mail@nexcon.es