Smart solutions for smart networks

Version 4.1

VCL-2143 MouseTrap™ Honeypot

Network Intrusion Detector

VISUALIZE AND SEE A CYBER-ATTACK IN REAL-TIME

LOCATE THE-ATTACKER IN REAL-TIME WITH DETAILED FORENSIC ANALYSIS

IDENTITY YOUR NETWORK VULNERABILITY IN LESS THAN 60 SECONDS

Introduction

VCL Network-MouseTrap™ is an essential network security tool that sits behind the firewall in a secure environment to detect firewall breaches and unauthorized intrusions in that network. **VCL Network- MouseTrap™** is an advanced “honeypot” / “decoy server” that can be programmed by the user to emulate various types of IEDs such as Protection Relays, RTUs or Payment Gateways etc. and 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 hostile intrusions and firewall breaches.

VCL Network-MouseTrap™ provides various alerts in real time - including audio visual alerts - when it detects a network security breach.

The **VCL-2143 Network-MouseTrap™** finger-prints the complete credentials of the hostile entity (or entities) who have entered the protected network by maintaining a complete log of their credentials such as IP address, domain and the originating location details of the intruder. Each log entry is time-stamped with the exact time and date of each such incident when an unlawful intrusion occurs.

CXR Networks

Application

The VCL-2143, Network MouseTrαp™ may be used 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.

May be used to secure:

* Utilities: Power generation, power transmission and power distribution systems
* Smart Grid: Power Distribution Systems
* Oil & Gas pipelines and production facilities
* Remote nodes in a SCADA networks
* Railway and Airport Infrastructure
* Financial Infrastructure such as Banks and Payment Processing Gateways
* IT Networks of Law Enforcement Agencies.

Universality of Purpose and Ease of Use:

* Seamless scalability
* Infrastructure neutral
* Transparent to networks and network applications
* Easy installation and management.

Interfaces

* Total Number of System Interfaces: 2
* 1 x 10/100 RJ45 Network-MouseTrαp™ “Decoy-Server / Honey- Pot” Network Interface
* 1 x 10/100 RJ45 Network-MouseTrαp™ Secured Network Management Interface
* Dry-Contact Relay Alarm Output.
* RS232 / RS485 Output that may be wired to a VCL-2702, Network Kill-Switch to disconnect the WAN from the LAN in the event of a detection of a Firewall breach.
* Application Note #1: The RS232 or Dry Contact Alarm Relay Output may be wired to a VCL-2778 (1G) / VCL-5078 (10G) Network Failover-Switch to switch the network to a Standby (Redundant) Firewall event of a detection of the Primary Firewall breach.
* Application Note #2: The RS232 or Dry Contact Alarm Relay Output may be wired to a VCL-2702 (1G) / VCL-5072 (10G) Network Kill-Switch-Switch to isolate the critical assets in the event of the detection of a network intrusion breach.
* Out-of-band security alerts
* USB serial port for local access and configuration

Security Features and Highlights

* Emulations: May be programmed by the user to emulate various types of targets such as a Protection Relay, RTU or Payment Gateway etc. to lure an unsuspecting intruder.
* White-List option: Sends an alert when the IP address or IP Domain are accessed by any entity not in the user programmed White List.
* Black-List option: Sends an alert when the IP address or IP Domain are accessed by any entity originating from the user programmed Black List.
* User Programmed Filters: Port (Soft) Based, IP Address based and IP Domain based
* SNMP trap generation for transmitting security alerts over a secured IP network.
* Dry contact alarm output.

CXR Networks

* Out-of-Band Security Alerts transmitted over a serial RS232 / RS485 interface. RS232 / RS485 Output that may be wired to a VCL-2702 (1G) / VCL-5072 (10G) Network Kill-Switch to disconnect and isolate the WAN from the LAN in the event of a detection of a "Firewall" breach.
* Alternately, the RS232 / Dry Contact Alarm Relay Output from VCL- 2143, Network MouseTrαp may be wired to VCL-2778 (1G) or VCL- 5078 (10G), Network Failover-Switch to switch the network to a Standby (Redundant) Firewall event of the detection of a breach of the "Primary Firewall".
* Integrated audio and visual alarms with alarm acknowledgment button.
* 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
* Resistance to Denial of Service (DoS) Attacks.

User Cases

Network MouseTrαp™ complements the other CXR's Network Security solutions to enhance network resilience and network security:

* VCL-2143, Network MouseTrαp™ may be used in conjunction with either VCL-2778 (1G) or VCL-5078 (10G), Ethernet Failover Switches to provide "1:1 Firewall Redundancy" and automatic failover in the event of detection of a "Firewall" breach by switching to the redundant (standby) "Firewall".
* VCL-2778 (1G) and VCL-5078 (10G) Failover Switches may be used to provide 1:1 Protection between "active" and "standby" networks or equipment (such as firewalls and routers) that are connected to the network through an Ethernet Interface.
* VCL-2778 is a 1G Ethernet Failover Switch that may be used to provide 1:1 Failover Protection on 1G Ethernet links.
* VCL-5078 is a 10G Ethernet Failover Switch that may be used to provide 1:1 Failover Protection on 1G or 10G Optical Ethernet links.
* VCL-2143, Network MouseTrαp™ may be used in conjunction with either VCL-2702 (1G) or VCL-5072 (10G), Ethernet Kill-Switches isolate and protect critical assets in the event of detection of a network intrusion.
* VCL-2702 is a 1G Ethernet Kill-Switch that may be used to protect and isolate critical assets or networks connected on 1G Ethernet links.
* VCL-5072 is a 10G Ethernet Kill-Switch that may be to protect and isolate critical assets or networks connected on 10G Optical links.

Security, Monitoring and Access Control

* Password protection with password strength monitor
* Device Management and Alarm Monitoring
* Command Line Interface - SSH (Secure Access Control) with encrypted Password Protection, Telnet (with clear text disable option)
* SNMPv2 and SNMPv3 Traps and NMS for secure, real time remote monitoring
* Alarm condition detection/reporting (SNMP traps/SNMP alarm table)
* Integrated Audio and Visual Alarms with Alarm Acknowledgement Button
* Dry Contact Alarm Relay for connecting External Audio / Visual Alarms
* Syslog, Audit Log
* Secure Boot
* Encrypted Firmware Updates
* Optional Integrated NMS (Network Management Software). Provides access to all cyber-security products through a single NMS

CXR Networks

Led Indicators

* System Status LED and Power LED
* Intrusion Detection Alarm LED

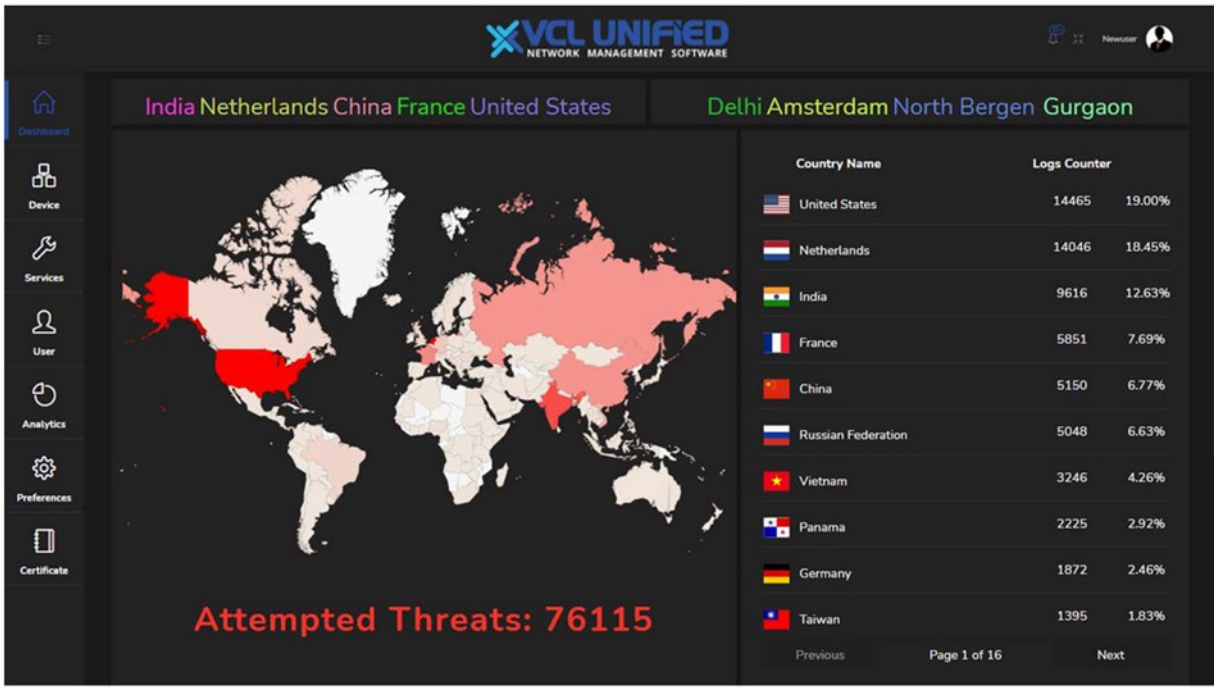
Environmental (Operational)

* 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 32 / EN55032 Class A
* FCC: Part 15 Subpart A
* Immunity: EN55024, EN61000
* RoHS, CE

VCL-Mouse Trαp User Interface



Power

* Power: 15V DC to 60V DC.
* Power consumption: 9W at maximum load
* 100~240V AC, 50/60Hz (external adapter)
* 85V DC ~ 250V DC (external adapter)
* 1+1 redundant (AC and/or DC) power supply option is available for 19-Inch Rack Mount version

Compliance

* Meets CE requirements
* Complies with FCC Part 68 and EMC FCC Part 15 and CISPR 32 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 Rack Mount Chassis.
* Height x Depth x Width: 42 mm x 175mm x 168 mm
* Weight: <1 Kg
* MTBF: ≥ 280,000 hours

Ordering information

Reference	Description
VCL-2143 DIN-DC012060	VCL-MouseTrap, Network Intrusion Detector. DIN RAIL Mount, 1 * 10/100 RJ45 (F) MouseTrap network interface, 1 * 15~60V DC (48V DC nominal) Power Supply Input, Management: USB serial port for local access, Installation Kit: System Core Cables, Mounting Hardware.

CXR Networks
CXR
T +33 (0) 237 62 87 90
www.cxr.com
Rue de l'Ornette 28410 Abondant France
contact @ cxr.com