

VCL-2143

Version 4.1

NETWORK MOUSETRAP™ HONEYPOT

Introduction :

VCL Network- MouseTrap™ est un outil de sécurité réseau essentiel qui se trouve derrière le pare-feu dans un environnement sécurisé pour détecter les violations du pare-feu et les intrusions non autorisées dans ce réseau. VCL - MouseTrap™ est un outil avancé, programmable par l'utilisateur pour émuler différents types d'IED tels que des relais de protection, des RTU ou des passerelles de paiement, ...et constitue un élément essentiel qui peut être installé pour sécuriser les infrastructures critiques telles que les sous-stations, les systèmes de distribution de réseaux intelligents, les réseaux informatiques des aéroports et des chemins de fer ainsi que les infrastructures financières telles que les banques et les passerelles de traitement des paiements pour « alerter » l'administrateur du réseau des intrusions hostiles et des violations de pare-feu.



MouseTrap™ fournit diverses alertes en temps réel, notamment des alertes sonores et visuelles lorsqu'il détecte une brèche de sécurité réseau enfreinte.

MouseTrap™ conserve un journal complet des informations d'identification telles que l'adresse IP, le domaine et les détails de l'emplacement d'origine de l'intrus. Chaque entrée du journal est horodatée avec l'heure et la date exactes de chacun de ces incidents lorsqu'une intrusion illégale se produit.

Visualisez et constatez une cyberattaque en temps réel

Application:

- Le **VCL-2143, Network MouseTrap™** peut être utilisé pour sécuriser les infrastructures tels que les sous-stations, les systèmes de distribution intelligents, les réseaux informatiques aéroportuaires et ferroviaires ainsi que les infrastructures financières telles que les banques et les passerelles de traitement des paiements.

Peut être utilisé à sécuriser:

- Utilitaires : Pouvoir génération, pouvoir transmission et pouvoir distribution systèmes
- Intelligent Grille: Pouvoir Distribution Systèmes
- Huile & Gaz pipelines et production installations
- Télécommande nœuds dans un SCADA réseaux
- Chemin de fer et Aéroport Infrastructure
- Financier Infrastructure tel comme Banques et Paiement Passerelles de traitement
- IT Réseaux de Loi Mise en vigueur d'agences.

Universel et Facile d'utilisation:

- Sans besoin d'évolution
- Transparent en matière d'infrastructure
- Transparent aux réseau et réseau d'application

Installation et gestion aisées

Introduction :

Total Nombre de Système Interfaces : 2

- 1 X 10/100 RJ45 Réseau - Interface réseau
- 1 réseau RJ45 10/100 - Interface de management sécurisée
- Contact sec Sortie Relais Alarme.
- Sortie RS232 / RS485 pouvant être câblée à un VCL-2702, Network Kill-Switch pour déconnecter le WAN du LAN en cas de détection d'une brèche du Pare-feu.
 - **Note d'application n°1 :** La sortie de relais d'alarme RS232 ou à contact sec peut être câblée à un VCL-2778 (1G) / VCL-5078 (10G) pour faire passer le réseau en veille (redondant). Evènement sur Pare-feu ou détection sur Pare-feu primaire.
 - **Note d'application n°2 :** La sortie de relais d'alarme RS232 ou à contact sec peut être câblée à un VCL-2702 (1G) / VCL-5072 (10G) pour isoler les actifs critiques en cas de détection d'un violation d'intrusion dans le réseau.
- Alertes de sécurité hors bande
- Port série USB pour accès à la configuration localement.

Localisez l'attaquant en temps réel grâce à une analyse détaillée

Sécurité Caractéristiques et Points forts:

Émulations : peuvent être programmées par l'utilisateur pour émuler différents types de cibles telles qu'un relais de protection, une RTU ou une passerelle de paiement ,...

- **Liste blanche option:** Envoi d'une alerte quand l'adresse IP ou le domaine IP sont accédés par une entité non déclarée dans la liste blanche.
- **Liste noire option:** Envoi d'une alerte quand l'adresse IP ou le domaine IP sont accédés par une entité programmée par l'utilisateur dans la liste noire.
- **Filtres programmables d'utilisateurs :** Basé sur l'adresse IP, sur le domaine IP.
- Génération d'interruptions SNMP pour transmettre des alertes de sécurité sur un réseau IP sécurisé.
- Sortie d'alarme sur contact sec.
- Transmissions des alarmes hors-bande via un port série RS232 / Interface RS485 . RS232 / RS485 Sortie filaire pouvant être connectée à un VCL-2702 (1G) / VCL-5072 (10G)
- Alternativement, le port RS232 / le Contact sec depuis un VCL-2143, MouseTrap peut être filaire à VCL-2778 (1G) ou VCL- 5078 (10G), en cas de détection de faille « Firewall ».
- Alarmes sonores et visuelles intégrées avec bouton d'acquiescement d'alarme.
- Journal d'accès non volatile avec la capacité de « empreinte digitale » de toutes les tentatives d'accès et de conserver un journal des adresses IP et du domaine pour une analyse médico-légale par l'administrateur réseau.
- Résistance aux attaques par déni de service (DoS).

Identifier la vulnérabilité de votre réseau en moins que 60 secondes

Cas d'emploi:

MouseTrap™ complète les autres solutions de sécurité réseau de Valiant pour améliorer la résilience et la sécurité du réseau :

- VCL-2143, MouseTrap™ peut être utilisé en conjonction soit avec VCL-2778 (1G) ou VCL-5078 (10G), "1:1 Pare-feu Redondance" et automatique basculement en cas de détection d'une faille « Firewall » par passage sur le réseau redondant "Pare-feu".
- VCL-2778 (1G) et VCL-5078 (10G) sont connectés au réseau à travers d'une interface Ethernet.
- VCL-2778 est un commutateur de basculement Ethernet 1G qui peut être utilisé pour fournir 1:1 Basculement protection sur 1G Ethernet liens.
- VCL-5078 est un commutateur de basculement Ethernet 10G qui peut être utilisé pour fournir 1:1 Basculement protection sur 1G ou 10G Optique Ethernet liens.
- VCL-2143, Réseau MouseTrap™ peut être utilisé en conjonction avec VCL-2702 (1G) ou VCL-5072 (10G), en isolant et protégeant en cas de détection d'un réseau intrusion.
- VCL-2702 est un Switch Ethernet 1G qui peut être utilisé pour protéger et isoler les actifs ou les réseaux critiques connectés sur des liaisons Ethernet 1G.
- VCL-5072 est un switch 10G Ethernet Antidémarrage utiliser pour protéger et isoler les réseaux critiques connectés sur liens optiques 10G.

Sécurité, Surveillance et Contrôle d'accès:

- Mot de passe avec protection renforcée
- Surveillance management des entités et alarmes
- Interface en ligne de commande - SSH (Secure Access Control) avec protection par mot de passe crypté, Telnet (avec option de désactivation du texte clair)
- SNMPv2 et SNMPv3 Traps et NMS pour une connexion à distance sécurisée et surveillance en temps réel
- Détection/rapport de conditions d'alarme (traps SNMP/tableau d'alarmes SNMP)
- Alarmes sonores et visuelles avec acquittement des alarmes audio/visuelles externes
- Syslog, Enregistrement audit
- Boot sécurisé
- Mises à jour logicielles cryptées
- NMS intégré en option (logiciel de gestion de réseau). Fournir un accès à tous les produits de cybersécurité via un seul NMS.

Indicateurs leds:

- Led Statut Système et Led Power
- Led Détection d'intrusion

Environnement (opérationnel) :

- Température -20 °C à +60 °C (-4 °F à 140 °F),
- Humidité max. 95% RH (Sans condensation à 60 °C)
- Démarrage: température - 10 °C
- Maximum Opérationnel Humidité 95% RH (Sans condensation)

Certifications:

- Émissions : Conforme CISPR 32 / EN55032 Classe UN
- FCC : Partie 15 Sous-partie A
- Immunité: EN55024, EN61000
- RoHS, CE

VCL – MouseTrap : Interface Utilisateur :



Alimentation:

Alimentation: 15VDC à 60VDC.

- Consommation: 9W max
- 100 ~ 240VAC, 50/60Hz (adaptateur externe)
- 85VDC ~ 250VDC (adaptateur externe)
- Option alimentation redondante 1+1 (AC et/ou DC) disponible pour version à montage en rack 19 pouces

Conformité:

Conforme aux exigences CE

- Conforme FCC Partie 68 et CEM FCC Partie 15 et CISPR 32 Classe UN
- Opération ETS 300 019 Classe 3.2
- Opération ETS 300 019 Classe 3.2
- Transport ETS 300 019 Classe 2.3

Caractéristiques physiques et MTBF :

Rail DIN Industriel (IP50) Châssis.

- Facultatif, 1U, Châssis Industriel, montage en rack de 19 pouces .
- H * P * L: 42 mm X 175mm X 168 mm
- Poids: <1 Kg
- MTBF : ≥ 280 000 heures

Informations commerciales (Unit de base):

Partie Non.:	Description
VCL-2143- DIN-DC012060	VCL- MouseTrap, Détecteur d'Intrusion Réseau. Version rail-DIN - 1 * 10/100 RJ45 (F) interface Ethernet - 1 * 15 ~ 60 VDC (48VDC nominal) - 1 * port USB/Série pour management local - Kit Installation: Câbles, Kit de montage, Documentation, Utilisateur Manuel

*Options :

VCL-EMOD 0444-AC220	Alimentation externe rail DIN (externe), Convertisseur AC/DC, DRL30-24-1 - 1 * Entrée AC [90 ~ 240VAC, 50-60 Hz] - 1 * Sortie DC [24VDC ~ 1,25 A, 30W]
VCL-EMOD 0444-DC220	Alimentation externe rail DIN (externe), Convertisseur DC/DC, DRL30-24-1 - 1 X Entrée DC [110 ~ 250VDC] - 1 * Sortie DC [24VDC ~ 1,25 A, 30W]

Technique Caractéristiques sont sujets à changements sans avis.
Révision 4.1



CXR
T 02 37 62 87 90
www.cxr.com

17, Rue de l'Ornette 28410 Abondant France
contact @ cxr.com

Smart Solutions for Smart Networks

Information contained in this document is not contractual. CXR improves its products continuously. Specifications may change without notice.