honeyBox® industrial

1-Port-Version

Attack Detection and Alarm

- reliable detection of attackers in the network
- low costs each network segment
- no effect on the high availability of the network
- centralized analysis of security - warnings
- hardware suitable for industrial fields
- low operating expenses needed
- simple integration into the network
- no pattern-updates necessary

OPERATIONAL SCENARIOS

Monitoring your LAN for attackers

Scenario: Your LAN is not monitored end-to-end, yet attacks on your internal systems could cause serious damage.
Implementation: As a solution dedicated to the detection of internal attacks, Honeypot Appliances can provide you with rapid protection without any need to change the network structure.
Result: The ability to detect and to record attacks keeps you constantly updated as to whether any attackers are at work in your network. You can then initiate any measures necessary to block and analyze the attack.

Infected software smuggled in by careless system technicians

Scenario: You permit service technicians access to networks of industrial plants. In case their infected computers could distribute malware on control systems and substantially disrupt your production.
Implemention: You install one honeyBox industrial in each of your LAN with remote access. This enables you to recognize immediately if any computer from service staff is infected and could probably damage your plants.
Result: You are able to recognize infected systems easily and fast and prevent the spread of malware.

Scope of tasks

In Industrial networks, security appliances developed for office fields, can often not be implemented. Even Patching of installing of antivirus is impossible.
The problem is, that especially those networks in industrial fields do require a high level of security and protection. As follows, any damages could produce problems in production fields and in areas of infrastructures even cost lives.

To deal with those requests of security , beside using firewalls, a different solution is needed for recognizing attacks and infections with malware fast and easily.

solution

secXtreme has developed the honeyBox® industrial, covering the requirements at low cost.

By choosing suitable functions individually, a high level of advantage in security, time for realization, investment and costs is reached.

secXTREME Information Security

Functions and Characteristics

FUNCTIONS

Honeypot
- Up to 250 virtual honeypots for each interface
- 40+ honeypot-templates
- 19+ special-services

Security
- Hardened Debian Linux
- SSHv2
- HTTPS (local CA)
- File system integrity checks
- Security baselining
- Local firewall
- Digitally signed software

Management
- Web GUI monitoring
- SSHv2
- Setup using KVM, SSHv2
- Backup/restore/recovery
- System-monitoring
- Watchdog
- Alert-System (e-mail, pager, syslog, database, logfiles)

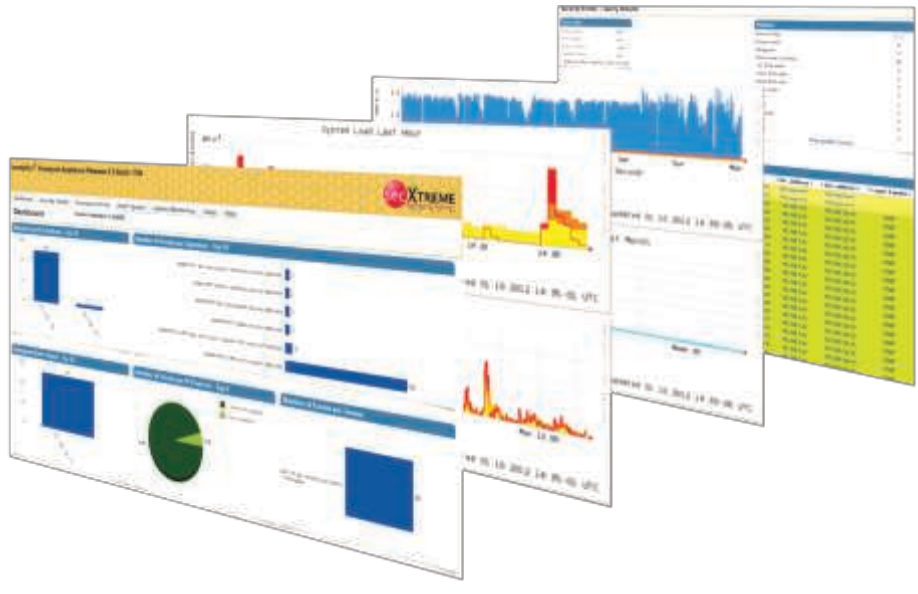
Installation
- Preinstalled

Integration
- Secure updates over the internet
- NTPv3 time synchronisation
- E-mail
- Syslog (CSV and CEF)

Support
- 5x8 telephone and e-mail service

Hardware exchange
- 2 years garantee
- Keep your hard disk option

Security alerts of honeyBox® industrial 1 Port are centrally recollected and centrally evaluated with a secure HTTPS connection in the browser. A data-evaluation based on different qualities is possible. This makes directed drill-down possible. Furthermore alerts can be forwarded to partnersystems like syslog. Security occurences could be integrated by digital exits of the system even in plant-visualisation.



Hardware	
CPU	AMD Geode LX-800 (500 MHz)
Main memory	512 MB DDR SDRAM
Network	1 x ethernet channel(10/100)
USB	2 x USB 2.0
Storage	4 GB CompactFlash-socket
RS232	2 x DB9
Power supply	DC 12-24 Volt, max 15 % toleranz
Power consumption(typ.)	7 Watt typ.
Operating temperatur	0 bis +50 degree
Humidity	5 % - 95 % non condesing
Dimensions	48mm x 123mm x 135 mm
Certifications	CE, FCC, RoHS

Awards for the honeyBox® appliance family

About secXtreme GmbH: secXtreme GmbH is a company that is specialised in information security. This includes audits, penetration testing, security analyses and training courses. In addition to these areas, secXtreme develops special solutions for the security environment. secXtreme is a member of the German CERT-Verbund and supports customers with incident management and forensic analysis.

secXtreme GmbH
Kiefernstraße 38
D-85649 Brunnthal-Hofolding

Tel. +49(0)89-18 90 80 68-0
Fax.+49(0)89-18 90 80 68-77
E-Mail: info@sec-xtreme.com