honeyBox® industrial

2-Port-Version

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.

Additional monitoring of your DMZs

Scenario: You use IPS in your DMZs to protect your systems, but once an attacker has taken over one of the DMZ systems, the IPS can no longer detect and prevent the attack from spreading within the DMZ. **Implementation:** You install a honeypot appliance and patch its sensor interfaces into the individual DMZ systems. As soon as the virtual honeypots are attacked, you can initiate countermeasures. **Result:** substantial improvement in the security and availability of your DMZ systems

Attack Detection and Alarm

- reliable detection of attackers in the network
- low costs each networksegment
- 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

Scope of tasks

In industrial networks, security appliances developed for office fields, can often not be implemented. Even Patching or installing of anti-virus 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 requirement 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

FUNCT□ONS

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
- USB stick (recovery of hard-ware appliance)

Integration

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

Support

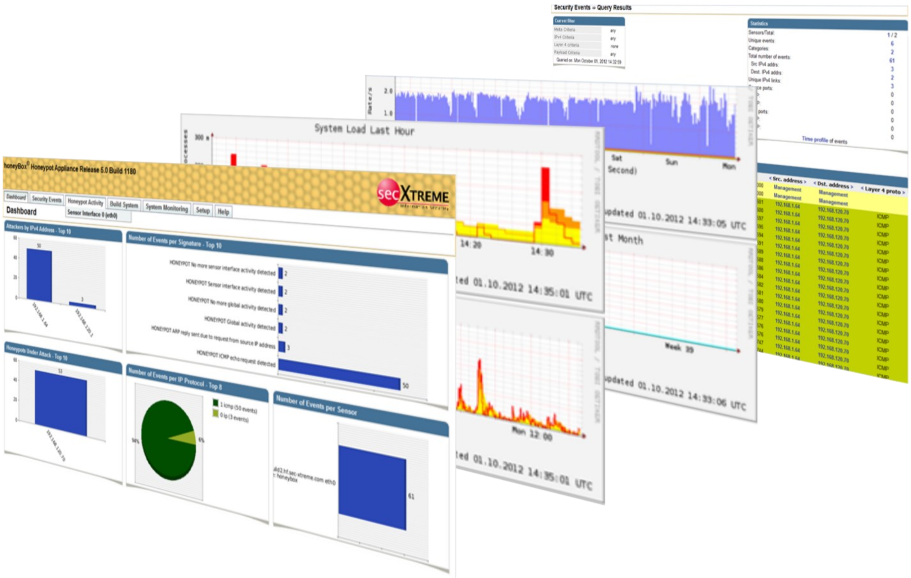
- 5x8 telephone and e-mail service

Hardware exchange

- 2 years garantee
- Keep your hard disk option

Functions and Characteristics

Security alerts of honeyBox® industrial 2 Port are centrally recollected and centrally evaluated with a secure HTTPS connection in the browser. A data-evaluation based on different qualities is possib-le. This makes directed drill-down possible. Furthermore alerts can be forwarded to partnersystems like syslog. Security occurences could be integrated by the digital exits of the sys-tem even in plant-visualisation.



Security Events » Query Results
Statistics
System Load Last Hour
honeyBox® Honeypot Appliance Release 5.0 Build 1180
secXTREME
Dashboard
Attackers by IPv4 Address - Top 10
Number of Events per Signature - Top 10
Honeypots Under Attack - Top 10
Number of Events per IP Protocol - Top 8
Number of Events per Sensor

Hardware	
CPU	Intel Atom D525, 1,8 GHz, 2 Core, Hyperthreading
Main Memory	1 GB DDR2
Network	2 x 10/100/1000 Copper
USB	4 x USB 2.0
Storage	64 GB 1,8 Zoll S-ATA MLC SSD
RS232	3 x DB9
Digital Outputs	4 (max 60 mA)
Power Supply	DC 10-30 Volt
Power Consumption (typ.)	min. 17 Watt, typ. 45 Watt
Operating Temperatur	-20 bis +55 Degree Celsius
Certifications	CE, FCC, RoHS

Awards for the honeyBox® appliance family

INNOVATIONSPREIS-IT
BEST OF 2014
initiative mittelstand
IT-SECURITY

IT-BESTENLISTE 2011
TOP 2011 IT-Lösung
ITBestenliste.de

secXTREME
Information Security

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.

All trademarks used are trademarks of the relevant proprietors; we reserve the right to make technical changes, errors excepted.

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
http://www.sec-xtreme.com