# honeyBox® industrial

## 2-Port-Version

## Angriffserkennung und Alarmierung

EINSATZSZENARIEN

**Überwachung auf Angreifer**

**Situation:** Sie betreiben industrielle Netzwerke, die Ziele von Attacken sein können. Sie haben bisher keine Erkennungsmechanismen im Einsatz.
**Umsetzung:** Mit dem Einsatz der honeyBox® industrial in den gefährdeten Netzwerksegmenten erhalten Sie in kurzer Zeit eine Lösung, die speziell zum Erkennen auch bisher unbekannter Angriffe geeignet ist. Die Lösung benötigt keine Änderungen an Ihrem Netzwerk und beeinträchtigt die Verfügbarkeit des Netzwerks nicht.
**Ergebnis:** Über die Erkennung und Aufzeichnung von Angriffen erhalten Sie jederzeit einen aktuellen Informationsstand aus Ihren industriellen Netzwerken. Sie können bei Angriffen rasch Maßnahmen einleiten, um den Angriff einzudämmen.

**Schadsoftware durch Servicetechniker**

**Situation:** Für den Service der Anlagen ermöglichen Sie Dienstleistern einen Zugang in diese Netze. Infizierte Computer der Dienstleister können Ihre Steuerungssysteme ebenfalls infizieren und Ihre Produktion erheblich stören.
**Umsetzung:** Sie installieren in Netzen mit Remote-Zugang jeweils eine honeyBox ® industrial und erkennen infizierte Rechner von Servicemitarbeitern sofort, wenn diese versuchen, Ihre Anlagen zu infizieren.
**Ergebnis:** Sie sind in der Lage, infizierte Systeme schnell zu erkennen und die Ausbreitung von Schadsoftware zu verhindern.


- zuverlässige Erkennung von Angriffen
- sehr geringe Kosten je Netzsegment
- keine Beeinträchtigung der Verfügbarkeit
- zentrale Auswertung der Sicherheitsmeldungen
- industrietaugliche Hardware
- sehr geringer Betriebsaufwand
- einfache Integration in das Netzwerk

**Aufgabenstellung**

In industriellen Netzwerken können die im Office-Umfeld vorhandenen Sicherheitsmechanismen oft nicht implementiert werden. Zeitnahes Patchen der Systeme ist ebenso oft nicht möglich wie die Installation von Anti-Virensoftware.

Trotzdem haben diese Netzwerke einen hohen Sicherheitsbedarf. So können Störungen zu massiven Problemen in der Produktion führen und gerade im Bereich kritischer Infrastrukturen (Energie, Verkehr) auch Leib und Leben gefährden.

Um den Anforderungen an die Sicherheit gerecht zu werden, ist neben der klassischen Firewall ein anderer Ansatz notwendig, um Angriffe und Infektionen mit Schadsoftware zügig zu erkennen.

**Lösung**

secXtreme hat für diese Aufgabe die honeyBox® industrial entwickelt, die diese Anforderungen kostengünstig abdeckt.

Durch geeignete Auswahl der Funktionen auf der Appliance wird ein sehr hoher Nutzen bezüglich Sicherheit, Realisierungszeit, Investition und Betriebskosten erreicht.

secXTREME Information Security

# Funktionen und Eigenschaften

## FUNKTIONEN

**Honeypot**
- bis zu 250 virtuelle Honeypots je Interface
- 40+ Honeypot-Templates
- 19+ spezielle-Services

**Sicherheit**
- gehärtetes Debian Linux
- SSHv2
- HTTPS (lokale CA)
- Filesystem-Integrity-Checks
- Security-Baselining
- lokale Firewall
- signierte Software-Pakete

**Management**
- Monitoring und Alarm Management Web-GUI
- SSHv2
- Setup über serielle Schnitt-stelle und SSHv2
- Backup/Restore/Recovery
- System-Monitoring
- Watchdog
- Alert-System (E-Mail, Pager, Syslog, Datenbank, Logfiles)

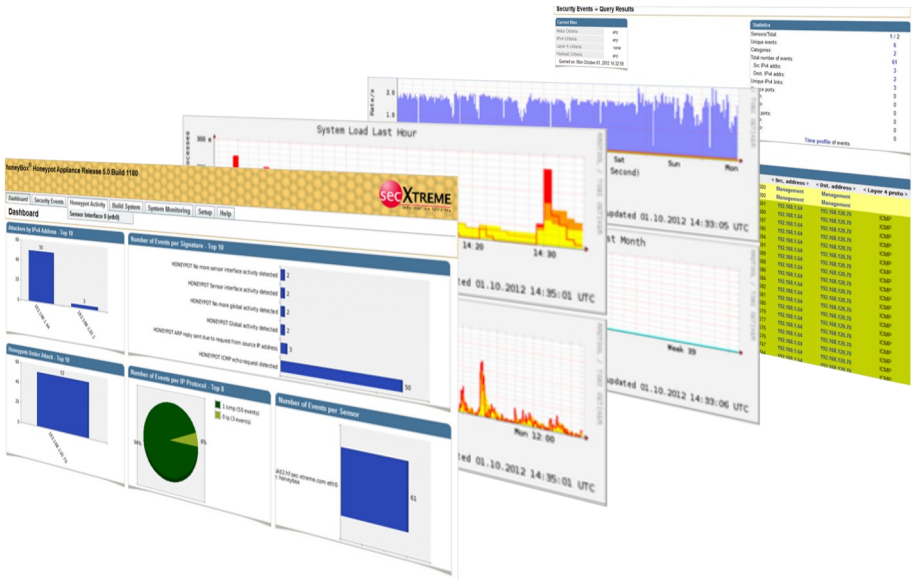
**Installation**
- vorinstalliert
- Recovery über Konfigurations-backup auf USB-Stick

**Integration**
- sicheres Updates über Internet
- NTPv3 Zeitsynchronisation
- E-Mail und Pager
- Syslog (CSV und CEF)

**Support**
- 5x8 per Telefon und E-Mail
- Deutsch und Englisch

**Hardwaretausch**
- 2 Jahre Gewährleistung (Bring-in-Service)
- Keep Your Hard Disk-Option

Die Sicherheitsmeldungen der honeyBox® industrial 2 Port werden zentral gesammelt und über eine sichere HTTPS-Verbindung im Browser ausgewertet. Die Auswertung nach verschiedenen Kriterien ist möglich. Damit steht die Möglichkeit für einen gezielten Drill-down zur Verfügung. Zudem können die Meldungen an Drittsysteme (z. B. per syslog) weitergeleitet werden. Sicherheitsvorfälle können über die digitalen Ausgänge des Systems auch in die Anlagen-visualisierung integriert werden.




| Hardware | |
|---|---|
| CPU | Intel Atom D525, 1,8 GHz, 2 Kerne, Hyperthreading |
| Arbeitsspeicher | 1 GB DDR2 |
| Netzwerk | 2 x 10/100/1000 Kupfer |
| USB | 4 x USB 2.0 |
| Speichermedium | 64 GB 1,8 Zoll S-ATA MLC SSD |
| RS232 | 3 x DB9 |
| Digitale Ausgänge | 4 (max 60 mA) |
| Spannungsversorgung | DC 10-30 Volt |
| Leistungsaufnahme | min. 17 Watt, typ. 45 Watt |
| Betriebstemperatur | -20 bis +55 Grad Celsius |
| Zertifizierungen | CE, FCC, RoHS |

Auszeichnungen für die honeyBox® Appliance Familie




Über secXtreme: Die secXtreme GmbH hat sich auf die Sicherheit Ihrer Informationen spezialisiert. Dazu gehören die Bereiche Audit, Penetration Testing, Sicherheitsanalysen und Trainings. Neben diesen Bereichen entwickelt secXtreme Sonderlösungen im Sicherheitsumfeld. secXtreme ist Mitglied im Deutschen CERT-Verbund und unterstützt seine Kunden bei Incident-Management- und Forensik-Aufgaben.



secXTREME Information Security

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