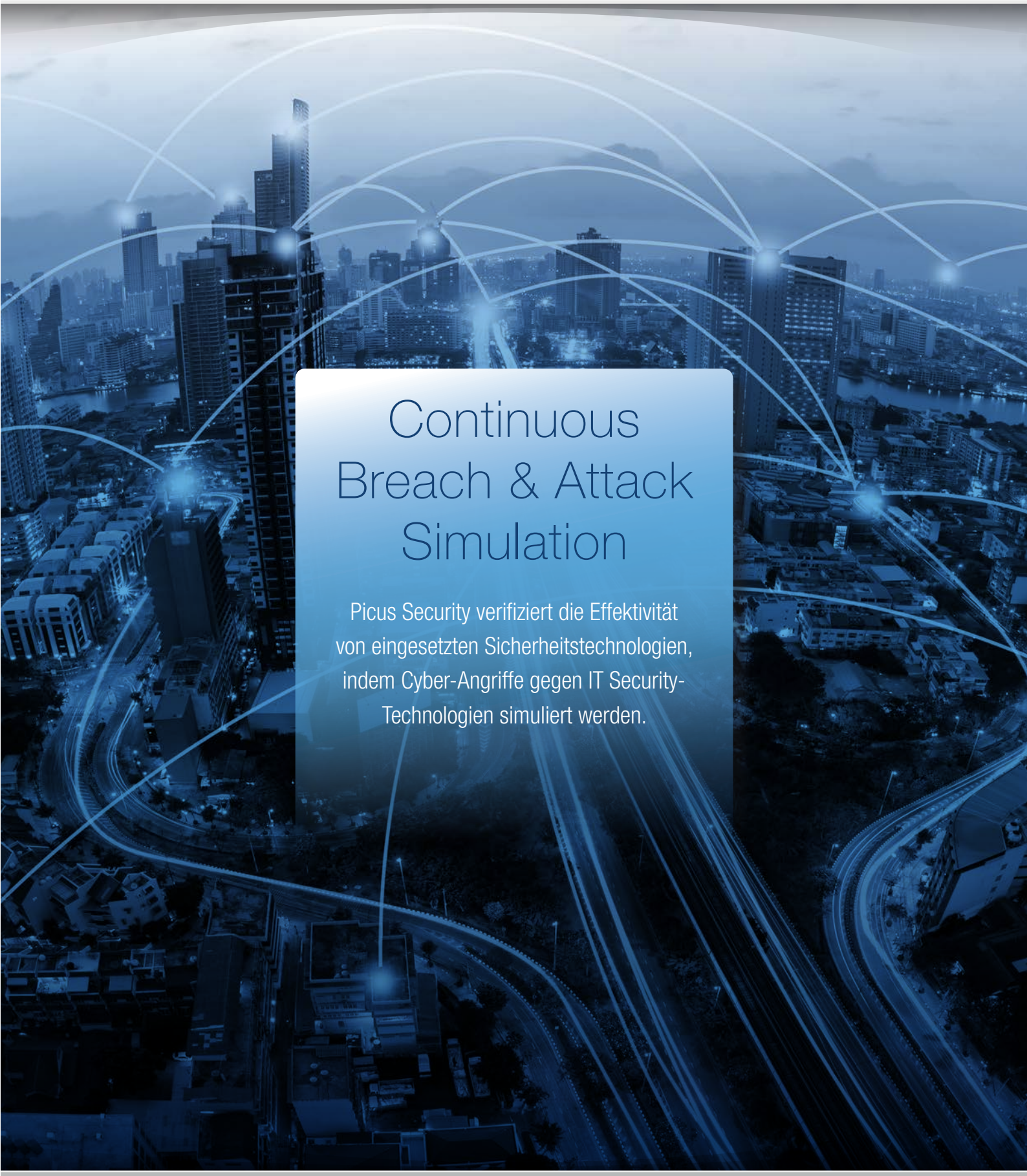
bitbone

PICUS SECURITY



Continuous Breach & Attack Simulation

Picus Security verifiziert die Effektivität von eingesetzten Sicherheitstechnologien, indem Cyber-Angriffe gegen IT Security-Technologien simuliert werden.

Produkt- & Funktionsüberblick

Picus Security verifiziert die Effektivität der implementierten Sicherheitstechnologien, durch Auswertung der Reaktion auf simulierte Cyber-Angriffe.

Grundlage dafür ist eine von Picus Security bereitgestellte und ständig aktualisierte Datenbank mit echten „Cyber-Threat Samples“ für den Missbrauch von Schwachstellen und Exploits, für Malware-Angriffe, für den Angriff auf Web-Anwendungen sowie den Abfluss von Daten.

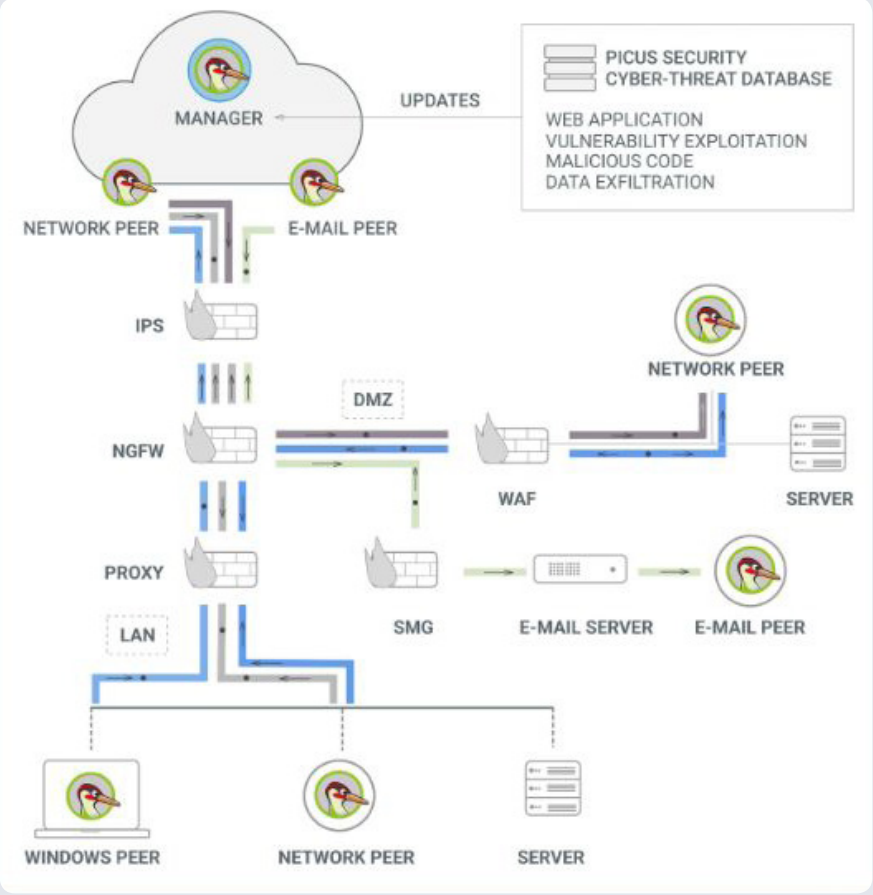
Dazu werden in einem Unternehmensnetzwerk Cyber-Angriffe zwischen 2 beliebig definierten Endpunkten simuliert, die von den jeweiligen Verteidigungsinstanzen am Gateway, am EndPoint sowie E-Mail-GW als echte Angriffe bewertet werden sollten.

Die Strecke zwischen den zwei definierten Endpunkten wird als sog. Vektor bezeichnet, z.B. Angreifer > Client-LAN, Angreifer > Mail-GW, Angreifer > EndPoint.

Welche Bedrohungsszenarien werden bei den durchgeführten Cyber-Angriffen simuliert:

- Angriffe durch bekannte ActiveX Steuerelemente, Java Applets, Ransomware, (Angriffs-)Scripte, Spyware, Trojaner, Viren, Würmer
- Angriffe auf Web-Anwendungen durch Command Injection, Cross-Site Scripting, Denial of Service, Directory Traversal Attack, Local File Inclusion, SQL Injection, XML Injection
- Angriffe durch die Ausnutzung von Schwachstellen wie Command-Execution-Exploits, DoS-Exploits, Lokale Exploits, sowie weitere Remote-Exploits

Die Simulation dieser Angriffe liefert bereits nach wenigen Stunden die ersten Resultate, die für die Optimierung des Sicherheitsniveau genutzt werden können.



Lizensierung

- Es wird, unabhängig der Unternehmensgröße oder der Anzahl der eingesetzten Endgeräte, nur die Anzahl der Vektoren, sowie die Nutzungsdauer des Service lizenziert.
- Ein Vektor wird als Strecke zwischen zwei definierten Punkten bezeichnet, innerhalb derer die Angriffssimulation durchgeführt wird.
- Picus ist als Subscription-Lizenzform mit einer Lizenz-Laufzeit von 12, 24 oder 36 Monaten erhältlich.

Herstellersupport

- Standardsupport 8x5 an Werktagen.
- Erweiterter 24x7x365 Support auf Anfrage.
- Ein dediziertes Technical Account Programm (TAM) ist gegen Aufpreis verfügbar.

Technologiepartnerschaften des Herstellers

- ArcSight
- CheckPoint
- Cisco
- F5 Networks
- Fortinet
- IBM QRadar
- LogRhythm
- McAfee
- Palo Alto
- Snort
- Splunk
- OpenSouce-Support für modSecurity und Snort

Welche Nutzen bietet die bitbone AG ihren Kunden?

- vertriebliches und technisches KNOW HOW
- technischer Standard-Support oder Wartungsvertrag (8x5)
- Unterstützung bei einer Evaluierung
- Neben klassischen Lizenzverkauf, verstehen wir uns als Ihr Picus-MSSP
- gute und enge Vernetzung zum Lieferanten und Hersteller

Alleinstellungsmerkmale des Herstellers

FORDERE DIE EIGENE IT-SICHERHEIT HERAUS!
Erlaube dem Security-Team die Sicherheitsinfrastruktur im Unternehmensnetzwerk mit echten Bedrohungen anzugreifen, bevor es Cyber-Kriminelle tun.

BESEITIGE IT-SICHERHEITS-LÜCKEN!
Identifiziere vorhandene Sicherheitslücken oder Konfigurationsschwächen und nutze die Remediation-Empfehlungen von Picus Security, um Schwachstellen schnell zu beseitigen.

MAXIMIERE DIE EFFEKTIVITÄT DER IT-SICHERHEIT!
Picus Security hilft Unternehmen, die Erkennungsrate von Cyber-Angriffen nachhaltig zu steigern und so die Effektivität der eingesetzten IT-Sicherheitstechnologien zu maximieren.

STEIGERE DIE REAKTIONSEFFEKTIVITÄT!
Durch die Verifikation der vorhandenen Angriffsfläche können IT-Sicherheitslücken schneller geschlossen werden.

STRESSTEST IN PRODUKTIONSUMGEBUNGEN
Picus Security führt Security-Effektivitätstests in Produktionsumgebungen durch, da diese im Vergleich zu Tests in statischen Laborumgebungen besser und realistischer Reaktionen auf Cyber-Angriffe darstellen.

Auswirkungen der Technologie auf Security, Compliance, TCO und Ressourcenoptimierung

COMPLIANCE
Regelmäßige Sicherheitschecks in Produktionsumgebungen sind stetige Anforderungen von Richtlinien wie z.B. ISO, BSI oder PCI-DSS. Diese können mit Picus automatisch und kontinuierlich durchgeführt werden.

STEIGERUNG DES IT-SICHERHEITSNIVEAUS
Durch die Überprüfung der eingesetzten IT-Sicherheitstechnologien mit Picus Security können unentdeckte Sicherheitslücken und fehlerhafte Konfigurationen erkannt und zügig beseitigt werden, bevor potentielle Angreifer diese ausnutzen können.

OPTIMIERUNG VON RESSOURCEN
Durch den Einsatz von Picus Security können IT-Abteilungen bestimmte Assessment-Tätigkeiten automatisieren und damit den Einsatz der oft knappen Ressourcen optimieren.

REDUZIERUNG VON GESAMTKOSTEN (TCO)
Durch den Einsatz von Picus Security können bestehende IT-Sicherheits-technologien effektiver genutzt werden. Des Weiteren ermöglicht die gesamt-heitliche und herstellerneutrale Verifikation von Security-Lösungen eine klare TCO-Kostenbetrachtung, sowie die Identifikation für weitere gezielte Investitionen.

Nutzen einer Partnerschaft mit dem Hersteller

- **Einstieg in den Zukunftsmarkt „Breach and Attack Simulation (BAS)“**, da Unternehmen die Effektivität der eingesetzten Security-Technologien permantent und in Echtzeit aufgrund der immer komplexer werdenden Cyberbedrohungen überprüfen müssen.
- Die **Umsatz- und Wachstsumspotentiale mit Neukunden** liegen im Assessment bestehender IT-Sicherheitslösungen. Unabhängig davon, von wem die obigen Technologien erworben wurden, können Partner mittels Picus Security Neukunden akquirieren.
- Die **Umsatz- und Wachstsumspotentiale mit Bestandskunden** lie-gen im Assessment bestehender IT-Sicherheitslösungen. Dadurch, dass Bestandskunden obige Technologien einsetzen, sind die Chancen auf Cross-Selling-Umsatz mit Picus Security sehr attraktiv.
- Nach dem Abschluss eines Assessments können weitere **Dienstleistungen,** wie z.B. „Security GAP-Analysen“, als Optimierungsmaßnahmen angeboten werden.

Einsatzszenarien der Technologie

Picus überprüft die Effektivität von Security Technologien (Gateway, EndPoint oder E-Mail) durch die Simulation von verschiedenen Angriffen durch Malware & Exploits

Es ist eine Tatsache, dass Unternehmen hohe Investments in Security Technologien tätigen und dabei oft die Konfiguration dieser bei den Standardeinstellungen belassen. Durch eine Angriffssimulation können aktuell vorhandene Schwachstellen sowie eine fehlerhafte oder unzureichende Konfiguration der eingesetzten Technologie erkannt und somit deren Sicherheitsniveau optimiert werden (Security Improvement).

SECURITY-EFFIZIENZ-ÜBERPRÜFUNG VON:
- DLP-Technologien
- E-Mail-Systemen
- EndPoint-Security-Technologien
- IPS-Technologien
- FW / NGFW-Technologien
- Content-Filter / Proxy-Technologien
- Malware Sandbox-Technologien
- WAF-Technologien

Für bestimme Hersteller-Produkte wie z.B. CheckPoint NGFW, Cisco Firepower, F5 Networks BIG-IP, Fortinet (AV, IPS & WAF), McAfee vNSP, ModSecurity (Open Source), Palo Alto Networks NGFW, Snort (Open Source) bietet Picus Remediation- und/oder Konfigurations-Empfehlungen. Neben der herstellerunabhängigen Verifikation der eingesetzten IT-Sicherheitslösungen kann Picus Security auch zur Überprüfung definierter, organisatorischer IT-Security-Prozesse und etablierter Methodiken genutzt werden, um auch hier optimierungspotential zu erkennen.

Kontakt

Sie haben Fragen oder möchten bestellen?
Wenden Sie sich bitte an:

Sebastian Scheuring
Vorstand

T: +49 931 250 993-10
E: info@bitbone.de

Über Picus Security

Nach der Investition in bekannte Sicherheitslösungen denken viele Unternehmen, dass sie vor Cyber-Angriffen sicher sind. Warum lesen wir dann weiter über neue Angriffe, die jede Woche gelingen? Verbessern Sie die Effizienz Ihres vorhandenen Sicherheits-Stapels mit Picus und seien Sie auf die neuen Bedrohungen vorbereitet.

Seien Sie immer vorbereitet vor neuen Bedrohungen, identifizieren Sie Ihre schwachen und starken Sicherheitsmaßnahmen in Echtzeit und beheben Sie Auffälligkeiten in Minutenschnelle.

Mit neuen Bedrohungsmustern in Produktions-umgebungen misst Picus kontinuierlich die Effektivität von Sicherheitsabwehrmechanismen und lokalisiert starke und schwache Punkte der Verteidigungsschichten. Indem sie Sanierungsalternativen auflisten, verbes-sert Picus Ihre Sicherheit und hilft Ihnen, Ihre Sicherheitsinvestitionen optimal zu nutzen.

Über die bitbone AG

Die bitbone AG bietet in zwei Geschäftsbereichen ein breites Spektrum an IT-Lösungen und -Leistungen: Wir sind Dienstleister mit Fokus auf Infrastruktur- und Security-Lösungen, verstehen uns aber auch als Ihr MSSP.

Als Dienstleister versorgen wir deutschlandweit Unternehmen und Organisationen mit IT-Lösungen, damit die Mitarbeiter alle Informationen zur Verfügung haben, die sie für eine effiziente Arbeit benötigen. Darüber hinaus sind wir Ihr kompetenter Ansprechpartner für Standardtechnologien, die IT-Infrastrukturen rundum und optimal mit Informationsmanagementsystemen vereinbar machen.

Dazu zählen Servertechnologien, Softwareverteilung, Monitoring, Plattformen, Virtualisierung und Cloud-Lösungen. Neben Open-Source Lösungen ist unser Security Bereich ein 2. Standbein in unserem Unternehmen.

Neben klassischen Themen wie Endpoint-, Firewall-, AS, EMM, Verschlüsselung und Backup, bieten wir auch Services im Bereich Auditing, Schwachstellenscanning und einer Breach & Attack Simulation an.

Unser Ziel ist es, die für Sie qualitativ und wirtschaftlich optimale Lösung zu finden. Dafür setzt jeder unserer engagierten Mitarbeiter zuverlässig sein Können ein. Langjährige Erfahrungen aus zahlreichen Projekten, der Mut zu neuen Technologien und ein funktionierendes Teamwork sind die Grundvoraussetzungen für unseren Erfolg.

www.bitbone.de

bitbone AG
Prymstraße 3
97070 Würzburg

T: +49 931 250 993 -10
F: +49 931 250 993 -199
E: info@bitbone.de