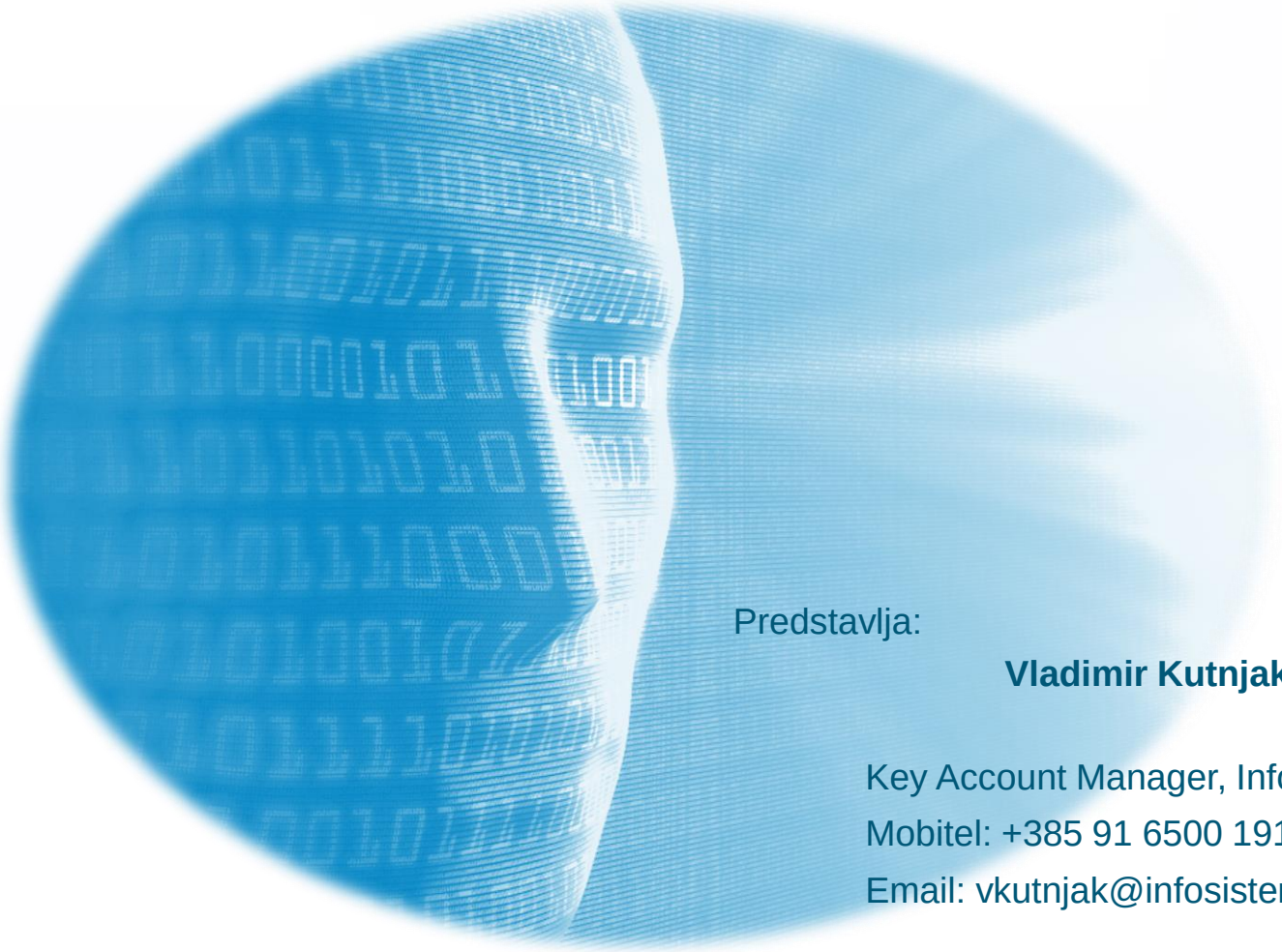
Get to Zero Incidents



Predstavlja:

Vladimir Kutnjak

Key Account Manager, Infosistem d.d.

Mobitel: +385 91 6500 191

Email: vkutnjak@infosistem.hr

Infosistem d.d.

- jedna od vodećih informatičkih tvrtki u Hrvatskoj
- 50+ godina iskustva
- 50+ visokoškolovanih stručnih djelatnika
- bogate reference
- certifikat ISO

Korisnici

te mnogi drugi.....

Partneri

UNISYS	Authorized Distributor
CISCO	Certified Premier Partner
hp	Preferred Partner
ORACLE PartnerNetwork CERTIFIED PARTNER	Certified Partner
Microsoft GOLD CERTIFIED Partner	Gold Certified Partner
EMC²	Reseller & Service Centre EMC Documentum Partner
imprivata	Authorized partner
PRINTRONIX	Silver Partner
CERTIFIED vmware PROFESSIONAL	Certified Partner
IBM	Advanced Business Partner
DELL	Registered Partner
PEARSON VUE AUTHORIZED TEST CENTER / PROMETRIC TEST CENTER	Authorized Test Center

STEALTH

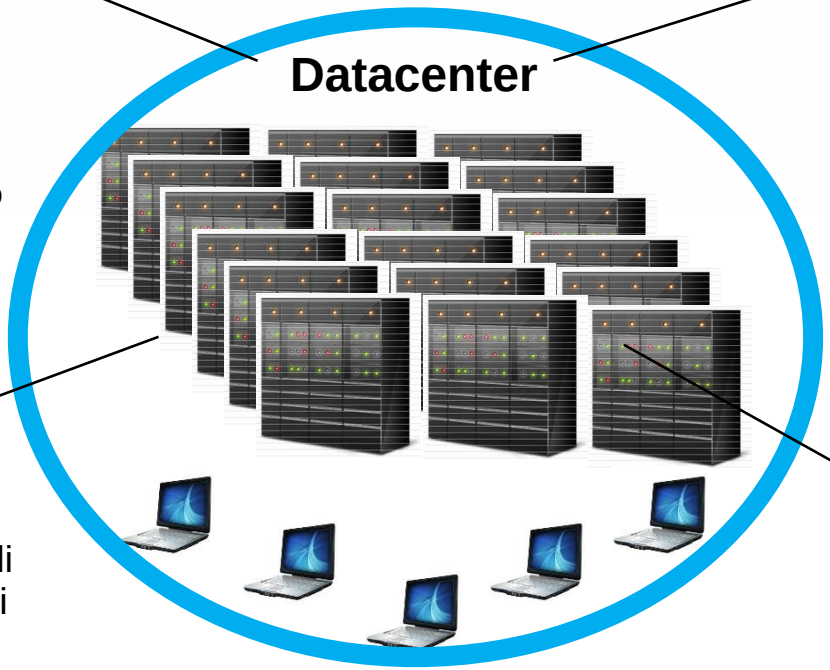
Software Defined Security by UNISYS

Stealth Security Portfolio

Stealth protects your most mission-critical environments – inside and outside your datacenter

Stealth (core)

Isporučuje fundamentalnu zaštitu za glavne podatkovne centre i IT imovinu kao što su serveri, stolna računalna, mobilna računala, kao i micro segmentaciju.



Stealth (mobile)

Pruža mogućnost sigurnog pristupa za mobilne uređaje i Stealth-om zaštićenu imovinu u podatkovnom centru

Stealth (cloud)

Proširuje Stealth zaštitu virtualnih strojeva na javnim ili privatnim oblacima; softverski orkestrirana i automatizirana plug-in implementacija

Stealth (compute)

Omogućuje sigurnu podjelu fizičke IT imovine - uključujući procesore, memorije, mreže i I/O - što rezultira vrlo sigurnim i prediktivnim IT enklavama

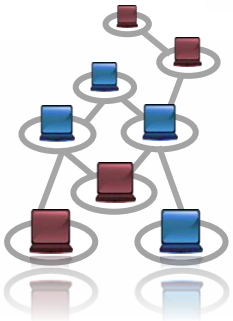
amazon web services™ Microsoft Azure

INFOSISTEM d.d. UNISYS

Stealth – Four Key Elements

Kriptografski protokoli

Kriptografski servis pruža FIPS 140-2 certificiranu AES-256 enkripciju

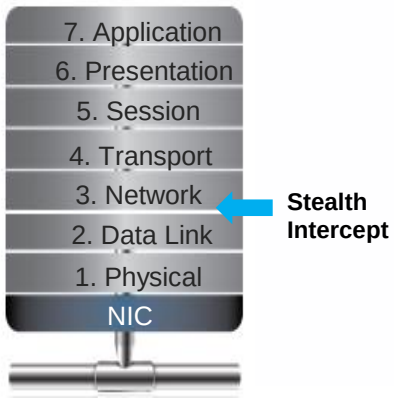


Virtualne interesne zajednice

Skriva korisnike, podatke i servere od svih koji nisu u zajednici (non-COI)

Algoritam rasipanja podataka i rekonstrukcija podataka

Štiti podatke od napada. Nisu potrebne nikakve promjene unutar aplikacija.

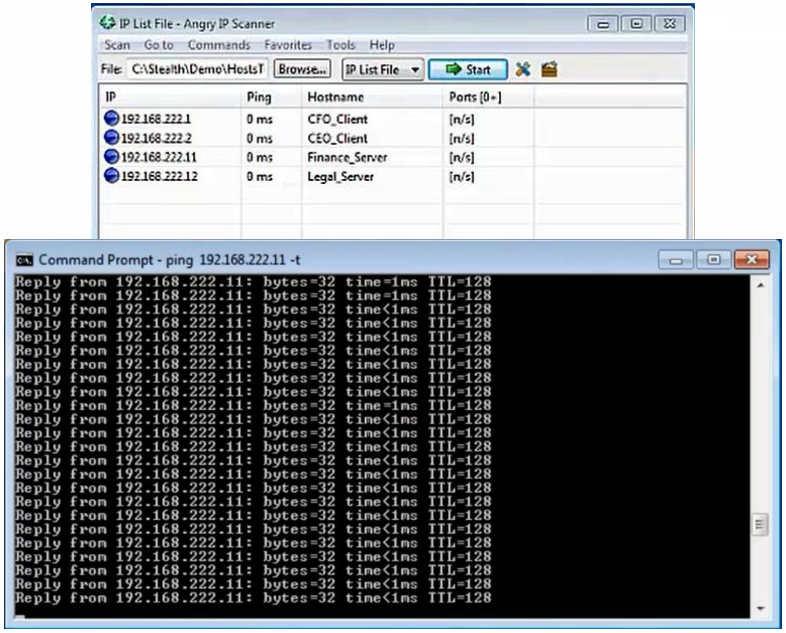


Nevidljiv aplikacijama

Stealthom formatirane poruke može protumačiti samo Stealth.

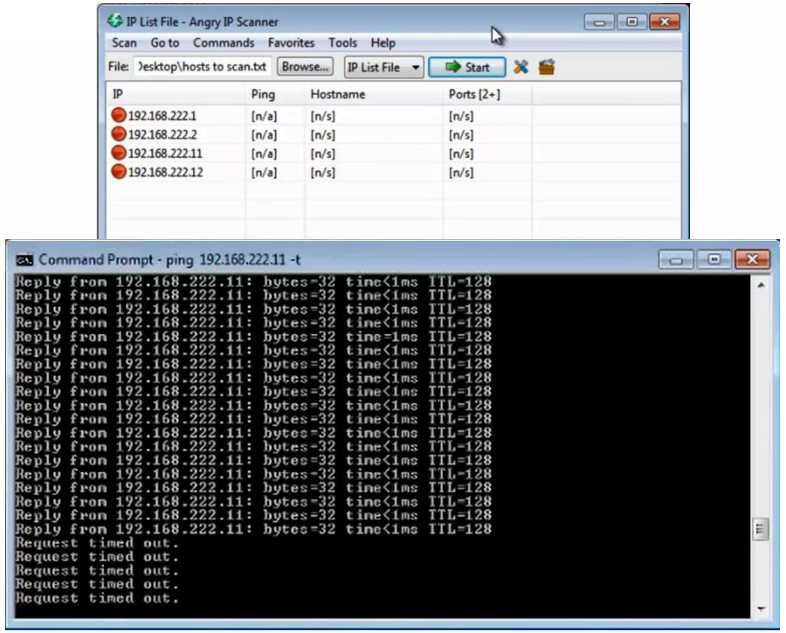
Stealth Ignores Communications from Unknown Sources (Hackers, Malicious Insiders)

Before Stealth



Nezaštićeni server je otvoren za „ping” – što hakerima osigurava polazišnu točku za proboj

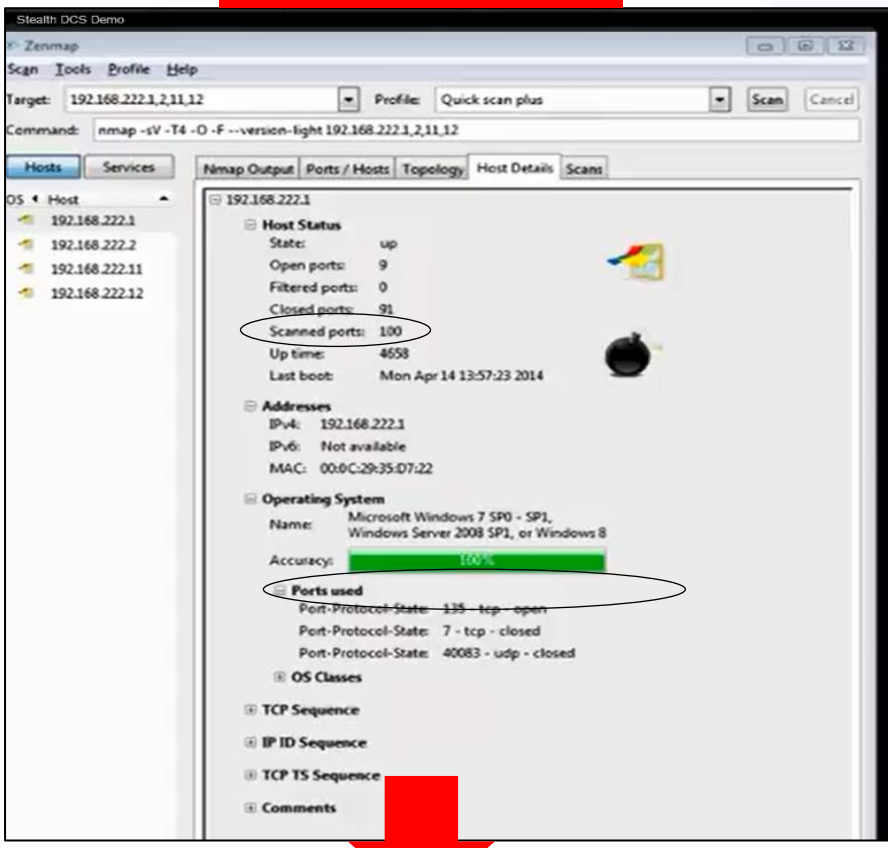
After Stealth



Stealthom zaštićeni server ne odgovara na „ping” – haker ga jednostavno ne može pronaći.

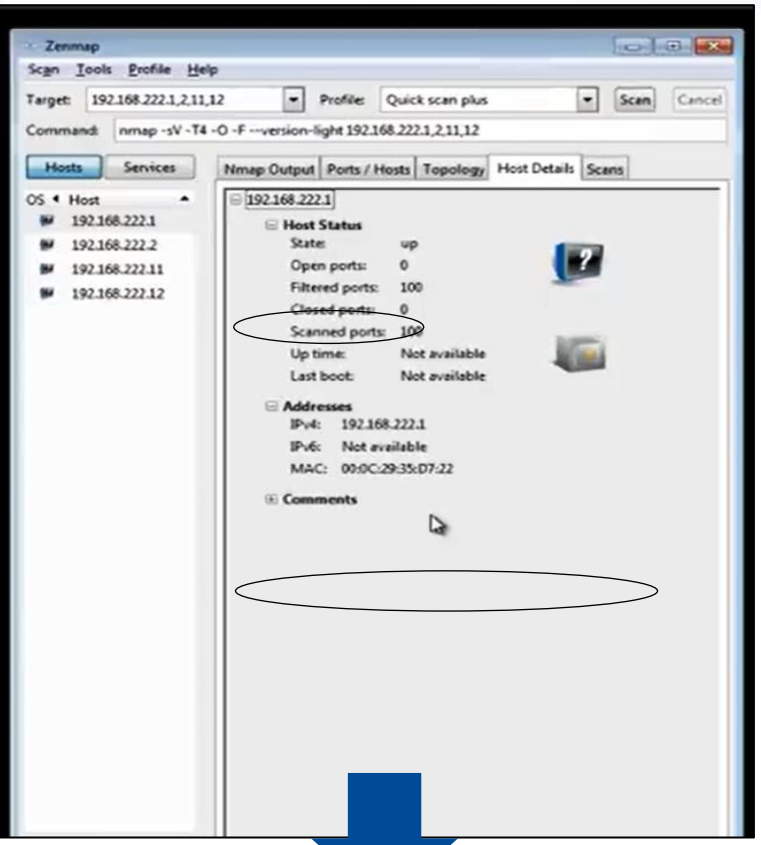
Stealth Protects Important System Information

Before Stealth



Informacije o portovima i operativnom sustavu su dostupne

After Stealth



Portovi su zatvoreni; ni jedna informacija o operativnom sustavu nije prikazana; informacije o hostu i pripadajućem IP-u su beskorisne jer će paketi biti ispušteni.

STEALTH

by UNISYS

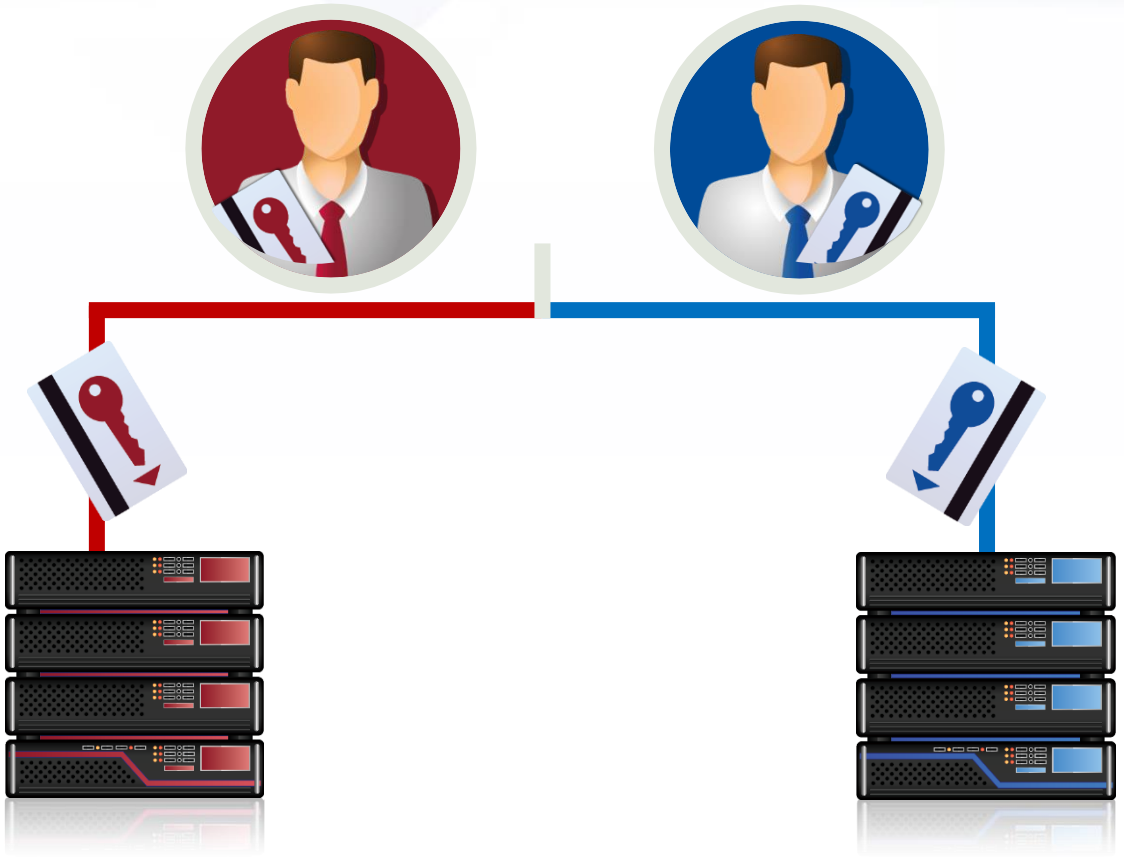
Kako Stealth Radi

Identity-Based Communities of Interest

Korisničke zajednice

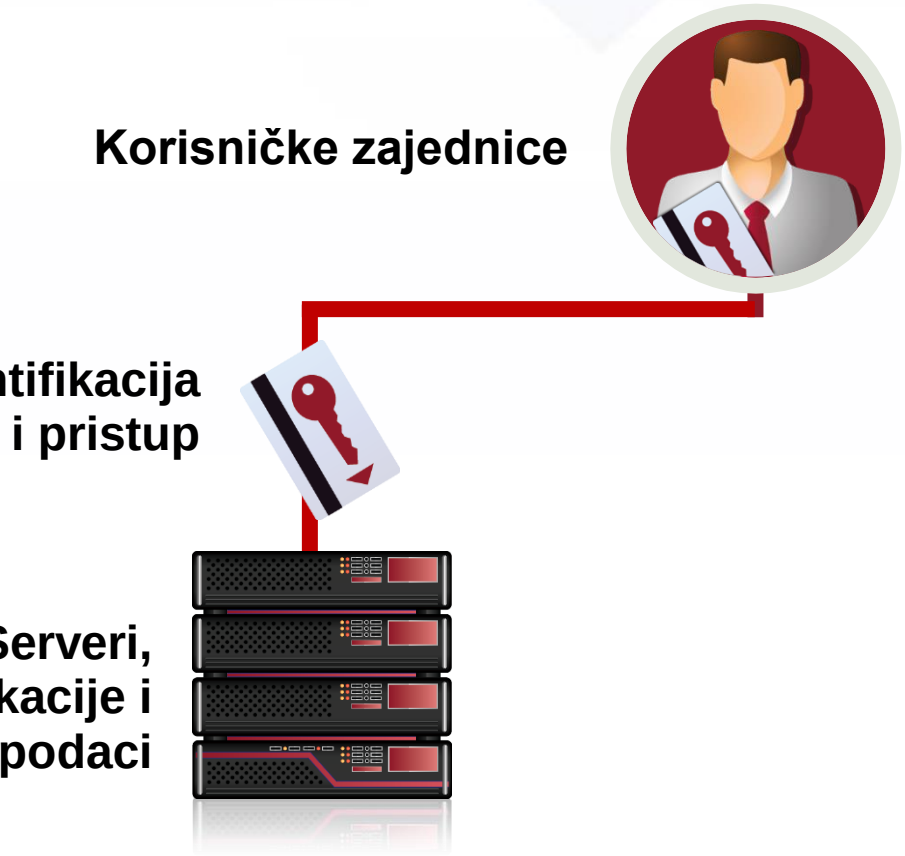
Ključevi, autentifikacija i pristup

Serveri/VM-ovi, aplikacije i podaci



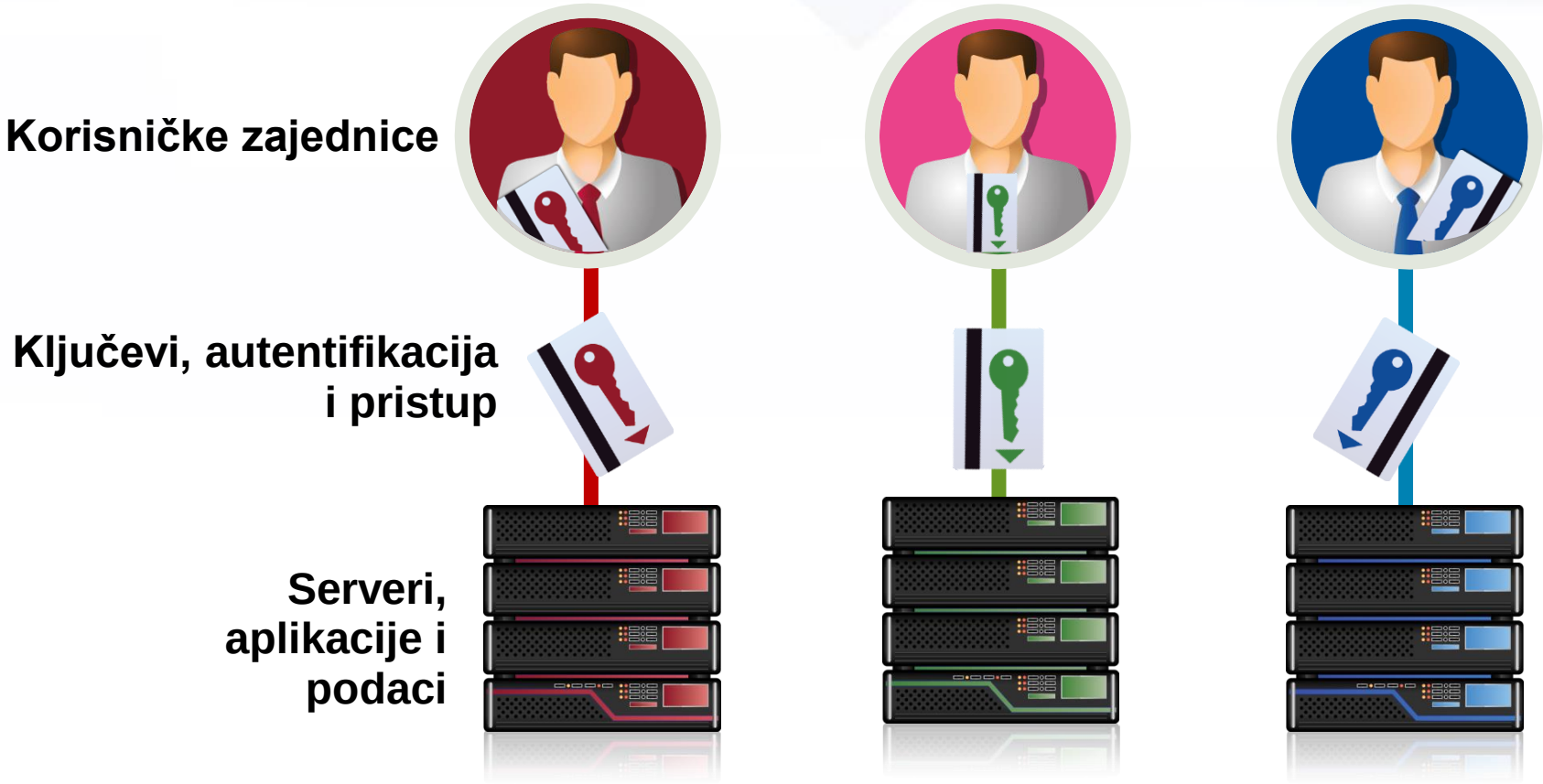
Svaka zajednica je zaključana, a korisnici dodjeljeni određenoj interesnoj zajednici vide samo njima autorizirane resurse unutar podatkovnog centra.

Identity-Based Communities of Interest



Crveni korisnik ne zna da postoji plava interesna zajednica, kao i njoj pripadajući resursi unutar podatkovnog centra.

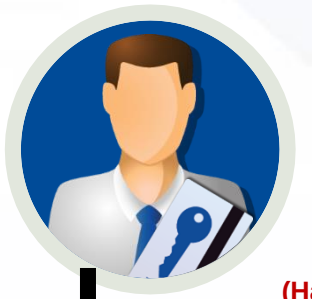
Identity-Based Communities of Interest



Plavi i crveni korisnik ne znaju da postoji zelena interesna zajednica, kao i njoj pripadajući resursi unutar podatkovnog centra

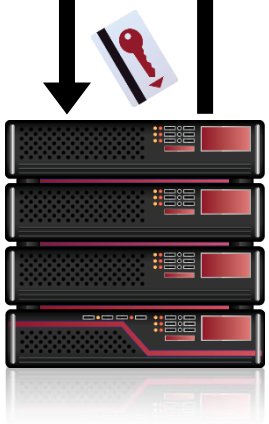
Stealth Data-in-Motion (DIM)

Tradicionalna neuspješna mrežna sigurnosna prijava

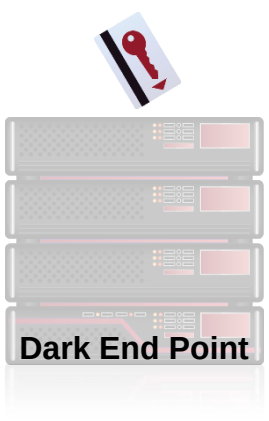


Potvrda (Hacker proba ponovo)

Nemaš autorizaciju



Stealth sigurnosna prijava



Stealth odbacuje podatkovne pakete u slučaju pokušaja neovlaštene autorizacije i ne šalje nikakav odgovor krajnjem korisniku.

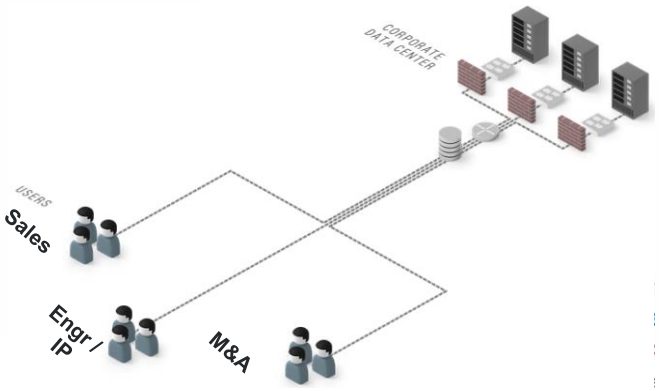
STEALTH

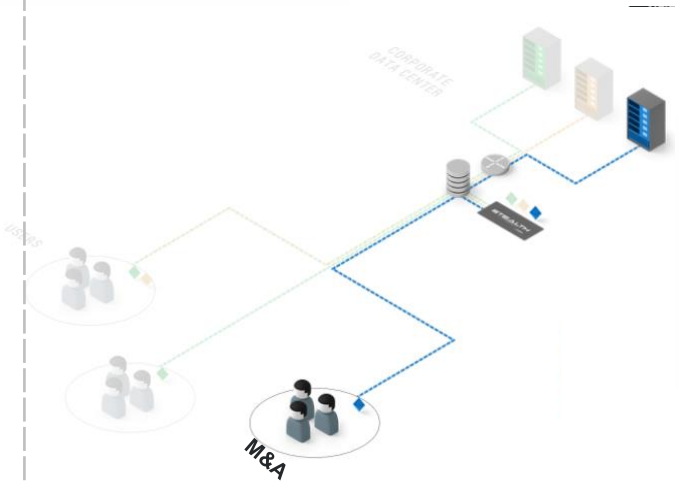
by UNISYS

Stealth Use Cases

Stealth (core): Mikrosegmentacija

Zaštita kritičnih sustava





Problem

- Tradicionalna sigurnosna rješenja za podatkovna sjedišta osiguravaju samo perimetar oko njega, a ne i ulazno-izlazni promet unutar podatkovnog centra.
- Pokušaji segmentiranja pomoću firewall-a često ostavljaju sigurnosne propuste zbog stalne potrebe za ručnim promjenama firewall pravila - hakeri / zlonamjerni korsnici iznutra iskoristiti će ove nedostatke.

Rješenje:
Stealth Micro-segmentacija

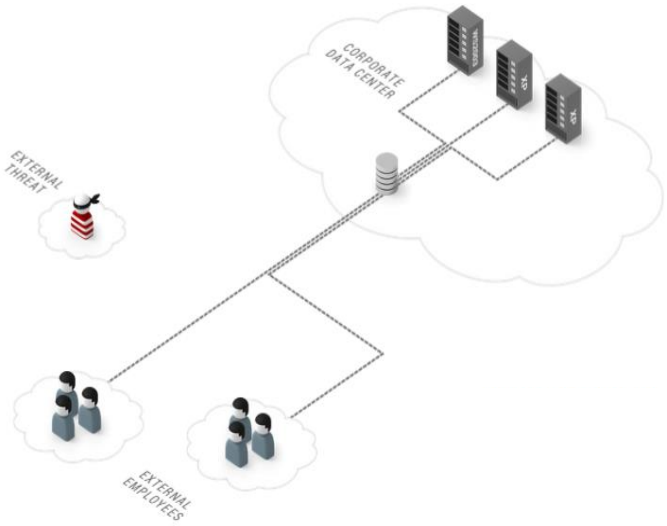
- Stealth razdvaja cijelo podatkovno sjedište u mikro segmente, manje zone koje je lakše zaštititi.
- Lateralna kretanja ograničena su na područje samo unutar dodijeljene zone.

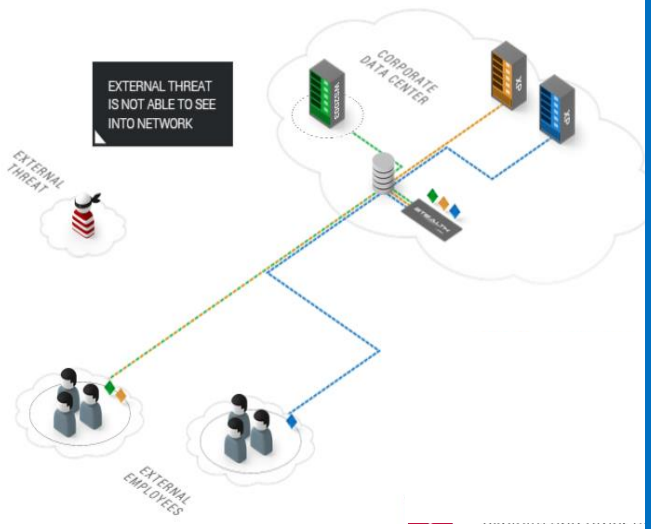
Stealth Highlights

- **Go dark**
  Učiniti krajnje točke nevidljivima svim hakerima / zlonamjernim insajderima
- **Segmentiranje data centra bazirano na korisničkim identitetima**
  Kontrola pristupa na bazi „need to know„ autorizacijskog pristupa
- **Osiguranje prolaznih podataka**
  Čuvanje podataka putem kriptiranja pristupnih točaka
- **Smanjenje troškova**
  Konsolidacija mreža, smanjenje broja vatrozidova kao i promjena pravila upravljanja istima.
- **Jednostavnije upravljanje sigurnošću**
  Brza prilagodba promjenama poslovnih potreba i regulatornim zahtjevima

Stealth (core): Mikrosegmentacija

Legacy System Protection





Problem

- Stari legacy sustavi kojima izlazi podrška od strane vendora, kao što su Microsoft Windows XP, Microsoft Windows Server 2003 i sl.
- Hakeri ciljaju ove ranjive sustave jer im je lakše pristupiti nakon što se na njima više ne ažuriraju sigurnosni segmenti putem tzv. „zakrpa”
- Prestanak podrške ovog tipa povećava mogućnosti sigurnosnih napada na sustav

Rješenje:

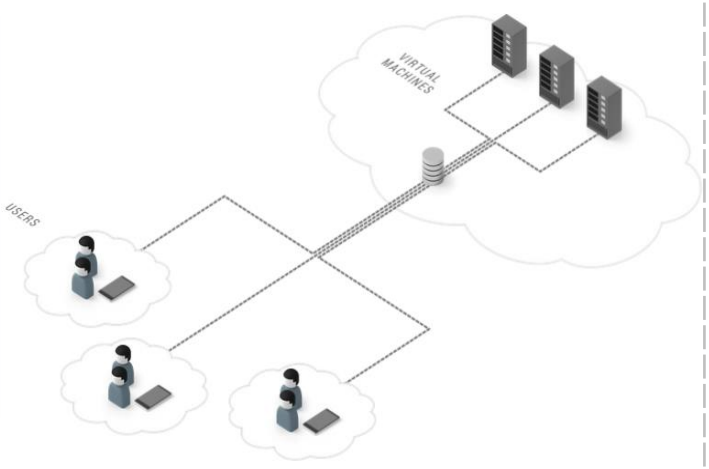
Stealth Legacy System Protection

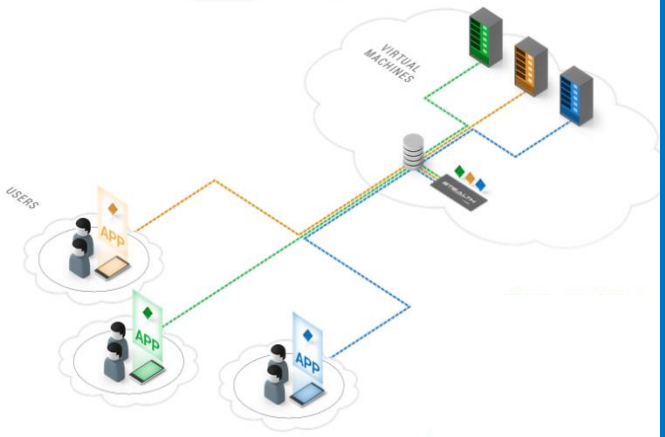
- Stealth sustavi štite i nepodržane operativne sustave na način da ih čine nevidljivima, maskiranima i nemogućim za identifikaciju od strane neautoriziranih korisnika.
- Stealth segmentira i izolira nepodržane operativne sustave od ostatka mreže.

Stealth Highlights

- **Go dark**
  Windows XP ili Windows Server 2003 krajnje točke postaju nevidljive neautoriziranim vanjskim i internim korisnicima
- **Zaštitite svoj datacentar**
  Izolacijom nepodržanih sustava od ostatka tvrtke
- **Ograničenje pristupa**
  Segmentiranje korisničkog pristupa / sistemskog pristupa na bazi „need to know” autorizacija
- **Postizanje regulatorne usklađenosti**
  Održavanje i poboljšavanje postojećih regulatornih zahtjeva ili industrijskih sigurnosnih zahtjeva

Stealth (mobile)





Problem

- Kontinuirano povećanje broja privatnih / BYOD mobilnih uređaja koji pristupaju korporativnoj mreži predstavlja dodatan rizik za korporativnu sigurnost
- Broj raznih zlonamjernih programa namijenjenih mobilnim uređajima nastavlja rasti, čime se značajno povećava rizični faktor za korporativnu sigurnost.

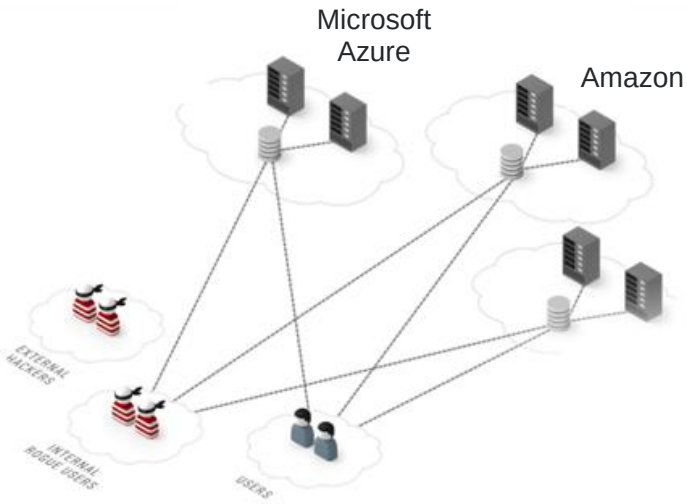
Rješenje:
Stealth (mobile)

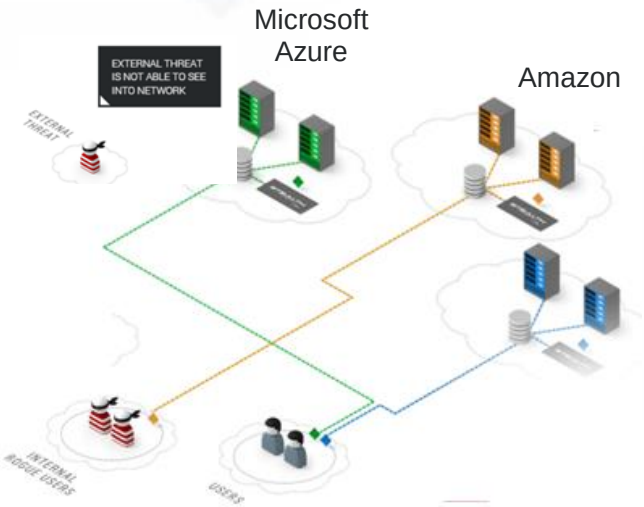
- Proširenje zaštite kritične imovine podatkovnih sjedišta u mobilnom okruženju – pružanjem pristupa podacima samo i isključivo autoriziranim korisnicima mobilnih uređaja
- Osiguranje cijelog procesa prijenosa podataka od mobilnih aplikacija do back-end procesnog okruženja.

Stealth Highlights

- Mobilna sigurnost je više od uređaja. Sveobuhvatna mobilna sigurnost počinje u podatkovnom sjedištu.
- **Budite neprimjetni – maskirajte krajnje točke**
  Učinite poslužitelje, laptope i mobilne aplikacije neuočljivima.
- **BYOD - sa pouzdanjem**
  Mobilni pristup korporativnim podacima baziran je na identitetu korisnika, a ne uređaja.
- **Osigurajte udaljeni pristup**
  Pružateljima telekomunikacijskih usluga, vanjskim suradnicima i poslovnim partnerima osigurajte mobilni pristup povjerljivim podacima bez straha od kompromitiranja.

Stealth (cloud)





Problem

- Sigurnost nastavlja biti barijera javnim sustavima „u oblaku" da uspješno postanu dio korporativnog sustava. Strah od mogućnosti uvida i pristupa osjetljivim podacima kroz Cloud zaustavlja napore u razvoju i testiranju takvih sustava
- Promet između Cloud-a i podatkovnog sjedišta obično je zaštićen enkripcijom samo do ruba Cloud-a.
- Promet između VM-a u javnom Cloud-u često nije kriptiran.

Rješenje:
Stealth (cloud)

- Stealth pomaže VM-a u Cloud-u da ostanu nevidljive vanjskim neautoriziranim korisnicima i smanjuje štete koja bi mogla nastati od strane internih neautoriziranih korisnika.
- Stealth kriptira prijenos podataka od podatkovnog sjedišta do VM-a u javnom Cloud-u, kao i međusobnu interakciju VM-a unutar javnog Cloud okruženja.

Stealth Highlights

- **Go dark – sakrijte krajnje točke**
  Maskirajte VM-a u javnom Cloud-u da budu nevidljive vanjskim neautoriziranim korisnicima
- **Zaštite kontrolu pristupa**
  Enkripcijski ključevi su kontrolirani od strane korporaciije i nisu dostupni pružateljima usluga u javnom Cloud-u.
- **Povećajte ekonomičnost**
  Stealth potiče korporacije da prebace veći obujam poslovnih opterećenja u javni Cloud, smanjujući Capex i Opex troškove podatkovnog sjedišta.
- **Pojednostavite upravljanje**
  Sa Stealth (cloud) sigurnosnim pravilima / procedurama omogućeno je obuhvaćanje više javnih Cloud okruženja.

STEALTH

Razvojni put i nagrade

by UNISYS

Stealth Extreme Scrutiny

Crypto-Module

Unisys Stealth

Award Winning

Network Risk Assessment
CWID 05
AF Comm Agency

IV&V
National Center for Counter-terrorism and Cybercrime SOCOM

Export License
Dept of Commerce

FIPS 140-2 Certification NIST

DIACAP MAC-1 Certification
JFCOM

JFCOM JIL
Testbed IO Range

SOCOM
R&D Prototype

DIACAP MAC-1 Certification
CWID 10

Commercial & Pub Sector

EAL4+ Certification NIAP

InterOp 2012
"Hot New Product"

2005 | 2006 | 2007 | 2008 | 2009 | 2010 | 2011 | 2012 | 2013 | 2014 | 2015

CWID 05
USAF

Combined Endeavour
EUCOM

CWID 08
DISA

CWID 09
DISA

JUICE 09
CECOM

CWID 10
SOCOM

GTRI
DJC2 PMO
SPAWAR

Private Lab
SSVT Validation:
Failed to compromise

"Large Integrator"
Tests and fails to break Stealth

Emerald Warrior '12
SIPRNet IATT

Independent Test Client-hired 3rd party: Failed to compromise

And again…
Different client, different tester: Failed to compromise

And again…

3rd party QSA and pen testing – PCI Compliance

DIACAP – DoD Information Assurance Certification and Accreditation Process
MAC – Mission Assurance Category (Level 1 is Highest)
DISA – Defense Systems Information Agency
EUCOM – European Command
SOCOM – Special Operations Command
JFCOM – JOINT Forces Command
JIL – Joint Intelligence Laboratory

CWID – Coalition Warrior Interoperability Demonstration
JUICE – Joint User Interoperability Communications Exercise
CECOM – Communications Electronics Command (US Army)
GTRI – Georgia Tech Research Institute
DJC2 – Deployable Joint Command and Control
NIST – National Institute of Standards and Technology
NIAP – National Information Assurance Partnership

Stealth Awards
Recognized for Cybersecurity Innovation

Frost & Sullivan 2015 New Product Innovation Award

Encrypted Network Security

NORTHERN VIRGINIA TECHNOLOGY COUNCIL
DESTINATION INNOVATION 2015 WINNER

TechAmerica Foundation
American Technology Awards
#AmericanTechAwards

Winner: *Cybersecurity Product of the Year 2014*

CRN

Tech 10 Security Products: Advanced Threat Protection (2014)

Hot Products from Interop (2012)

12TH ANNUAL AMERICAN BUSINESS AWARDS
THE STEVIES™

Winner: *Silver Stevie*

PEOPLE'S CHOICE STEVIE® AWARDS FOR FAVORITE NEW PRODUCTS

Winner: *Software Security*

NETWORKWORLD®

Click to view May 2014 Stealth product review

"Stealth is an interesting product that might just be a **great way to hide from hackers**."

- David Strom, editor-in-chief, *Network World*

INFOSISTEM d.d.

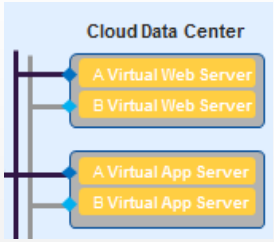
UNISYS

Stealth Value
Elevated Security, Simplified Management, Lower Costs

Zero Day Security Protection

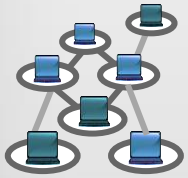
Stealth ne ovisi o digitalnom potpisu kako bi detektirao neautorizirane aktivnosti i prema to me je efikasan protiv zero'day malware napada.

Protects Cloud and Mobile



Stealth proširuje COI zaštitu na novu generaciju parametara zaštite imovine kao što su Cloud i mobilne tehnologije.

Značajno unaprijeđena upravljivost



Stealth implementira stvarni Software definirani sigurnosni model. Na taj način promjene su moguće jednostavnim promjenama u active directory podatcima.

Lowers Networking Costs

Stealth pomaže u potrebama izmjene parametara firewall uređaja koji se tipično kotiste za zaštitu mreže i sub domena unutar enterprise okruženja.

STEALTH by UNISYS

OneSign
Single Sign-On rješenje

„Ono nešto" što upotpunjuje sigurnosni sustav...

OneSign Single Sign-On

Imprivata, IT tvrtka koja nudi sigurnosna rješenja, pruža organizacijama na svjetskoj razini platformu kojom adresira i rješava pitanja sigurnosti kritičnih sustava, utječući na povećanje produktivnosti organizacija u pružanju usluga korisnicima i zadovoljstvu istima.

Rješenje je osobito namijenjeno organizacijama koje imaju korisnike koji rade u smjenama te se izmjenjuju na radnim mjestima (šalteri, blagajne, i slično).

Primarna zadaća:

- upravljanje sigurnošću, osobito u internim procedurama, osiguranjem jedinstvenog login-a za svakog korisnika za sve aplikacije koje korisnik upotrebljava u svakodnevnom radu
- Detaljan reporting za svakog korisnika (praćenje korištenja cijelog sustava u realnom vremenu, za svakog korisnika zasebno)

OneSign Single Sign-On

Znate li….

… da je oko 60% svih krađa podatka izvršeno internim probojem sigurnosti?

Glavna prednost rješenja je sigurnost u internim procedurama.

- Nema posuđivanja lozinki među korisnicima.
- Zna se tko, što i kada koristi (izvrstan izvještajni sustav).
- Ograničava se pristup pojedinim dijelovima sustava po korisniku (dodatno onemogućen uvid neovlaštenim osobama u podatke kojima ne bi trebali imati pristup.

Mogućnost povezivanja sa biometrijskim sustavom (dodatni stupanj sigurnosti u upravljanju sustavom i praćenje po svakom korisniku).

Hvala!

INFOSISTEM d.d.

Ivana Šibla 15, 10 020 Zagreb, Hrvatska
http://www.infosistem.hr

t +385 (0) 1 65 00 111
f +385 (0) 1 66 37 899
e infodesk@infosistem.hr