Shanghai Guan An Information Technology Co., Ltd.

www.idss-cn.com

National Headquarters in Shanghai
Building 9, Shibei First Center, No. 3, Lane 1401, Jiangchang Road, Jing'an District, Shanghai, China

Production and Education Integration Base in Shanghai Lingang
Room 202 and Room 215, 2nd Floor, No. 800 Huanhu West 2nd Road, Nanhui New Town, Pudong New Area, Shanghai, China

National Headquarters in Beijing
21st Floor, Maotai Building, No. 29 North Third Ring Middle Road, Desheng Street, Xicheng District, Beijing

National Headquarters in Shenzhen
Room 3101, Office Building T1, Qianhai Financial Center, No.91 Guiwan 3rd Road, Qianhai Shenzhen-Hong Kong Cooperation Zone, Shenzhen, China

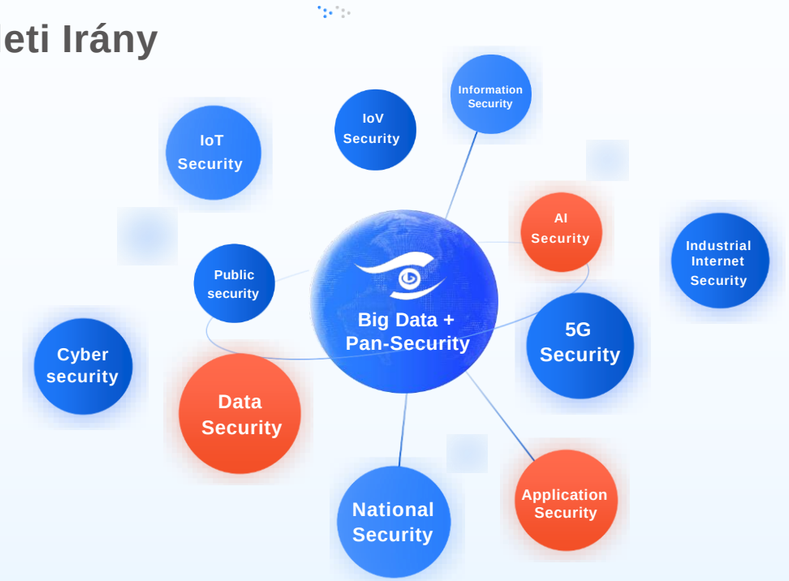
TARTALOM

A Cég Profilja

A Guan An Info. egy vállalat, amely big data és pánbiztonsági termékeket és szolgáltatásokat kínál. Az adatbiztonság, a kiberbiztonság, az 5G biztonság, a mesterséges intelligencia biztonsága, az ipari internet biztonsága és a közbiztonság fő területeire összpontosít, és átfogó információbiztonsági megoldásokat kínál távközlési szolgáltatók, kormányok, pénzügyi, villamosenergia-, közbiztonsági, egészségügyi és más iparági felhasználók számára.

A vállalatnak Sanghajban, Pekingben és Sencsenben van székhelye, valamint több laboratóriuma is. Ez az egyetlen olyan információbiztonsági képzőbázis Kínában, amelyet az Egyesült Nemzetek Képzési és Kutatóintézete (UNITAR) / Sanghaji Nemzetközi Képzőközpont (CIFAL) tanúsított, és tagja az UNIDO Sanghaji Nemzetközi Intelligens Gyártásfejlesztési Központ szakértői csoportjának. Az MIIT, az 5G Start-Up és a Shanghai High-tech Enterprises által tanúsított, a nagyszabású nemzeti események kiberbiztonsági védelmének műszaki támogató egységeként, a specializáció, a finomítás, a differenciálódás és az innováció kis óriásvállalataként ismert.

Üzleti Irány



Hozzáértés

A Guan An csapatának központi elemei több mint 20 éves szakmai tapasztalattal rendelkeznek az információbiztonság területén, és több mint 10 éves tapasztalattal a big data elemzésében. Számos aranyérmet nyertünk hazai és külföldi kiberbiztonsági technológiai versenyeken.

20+	15+	10+	8+	8+	200+	800+
Tapasztalat 20+ év	Szolgáltatás 15+ év	Big Data 10+ év	Adat Biztonság 8+ év	Laboratóriumok 8+	Szellemi tulajdon 200+	R&D munkatárs 800+

Kulcsfontosságú technológiák és képesítések

A vállalat szakmai képesítésekkel rendelkezik a kiberbiztonság és a big data területén a termékfejlesztés és a szolgáltatások terén, és számos nemzetközi és hazai szakmai rendszer- és technológiai tanúsítványt szerzett, mint például az ISO9000, ISO20000, ISO27001, ISO14001, ISO45001, CMMI-DEV, CCRC, CN ITSEC, CES SCN, CN CERT, és számos terméke IPv6 Ready Logo nemzetközi tanúsítványt is szerzett..

Társadalmi felelősségvállalás

A Guan An folyamatosan technológiai innovációkat hajt végre a „Kína Big Data+ támogatása” víziójával, a kiberbiztonsági személyzet képzésére összpontosítva, reagálva az „Egy Övezet, Egy Út” nemzeti kezdeményezésre, amelynek célja a nemzeti kiberbiztonság és a nemzetközi kiberbiztonság előmozdítása. Csere és együttműködés; aktív társadalmi felelősségvállalás, jótékonysági tevékenység előmozdítása, a szegénység enyhítésének elősegítése és a társadalom pozitív energiájának terjesztése.

Egyesült Nemzetek Szervezetének Képzési és Kutatóintézete (UNITAR) / Sanghaji Nemzetközi Képzőközpont (CIFAL) - Big Data Alkalmazások és Biztonsági Képzőbázis

Kiberbiztonsági készségek Versenyek

Népszerű tudományos képregény Guanzai története

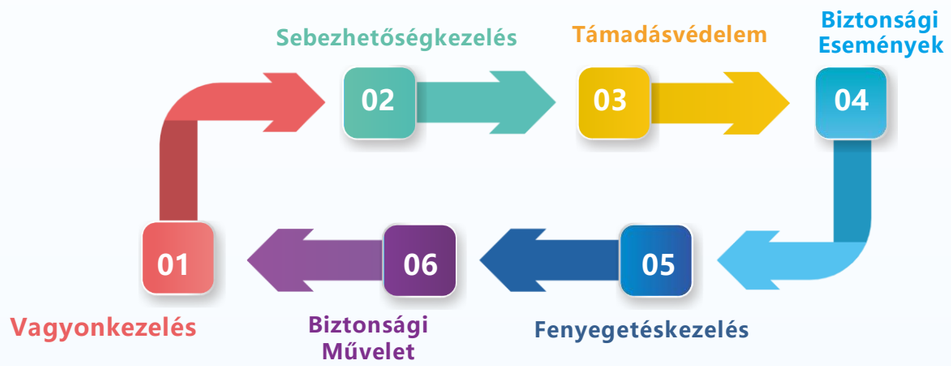
Kiberbiztonság az egyetemen

Szociális jóléti tevékenységek

GUANAN
Biztonsági Információ- é Eseménykezelő Rendszer

GUANAN Biztonsági Információ- és Eseménykezelő Rendszer hálózati forgalmat és napló adatokat gyűjt, valamint adatmodellezést, viselkedésazonosítást, korrelációs elemzést, mesterséges intelligenciát és egyéb módszereket alkalmaz a hatalmas mennyiségű, heterogén biztonsági adat elemzésére. Lehetővé teszi a SIEM elemzést az eszközök, sebezhetőségek, riasztások és események szempontjából, és nagyméretű képernyős megjelenítést generál az átfogó biztonsági helyzetről. Segít olyan vállalati hálózati biztonsági környezet kialakításában, amelyet a „jól szervezett adatirányítás, bőséges fenyegetéselemzési forgatókönyvek, tökéletes biztonsági figyelmeztető rendszer, hatékony reagálás a biztonsági eseményekre és rendezett biztonsági üzemeltetés” jellemez. A terméket széles körben használják távközlési szolgáltatóknál és állami tulajdonú vállalatoknál a pénzügyi, villamosenergia-ipari és más ágazatokban.

Érzékelési Lánc



Funkcionális Mátrix

GUANAN
Adatbázis-biztonsági Auditrendszer

GUANAN Adatbázis Biztonsági Audit Rendszer egy biztonsági audit termék, amely képes valós időben figyelni az adatbázis tevékenységeket. A rendszer segíti a vállalati üzemeltetési szakembereket az adatbázis műveletek megfigyelésében, elemzésében és nyomon követésében. A rendszer képes időben riasztani az illegális műveletekről, és csökkenti az adatbázis veszteségeit is. Az Adatbázis Biztonsági Audit Rendszer adatbázis-orientált felületnyelvet, intelligens protokollfelismerést, vizuális működési állapotot, interaktív és részletes kockázatkövetési képességet kínál. A rendszer egy új generációs adatbázis audit termék, amely tökéletesen teljesíti a vállalati elvárásokat megvalósítás, képzés és karbantartás nélkül.

Termékjellemzők

Átfogó Üzleti Audit

Minden adatbázistípust lefed, és lehetővé teszi a működési viselkedés pontos auditálását különféle környezetekben, biztosítva a teljes körű átláthatóságot az üzleti adatbázis-tevékenységekben.

Holisztikus Érzékeny Adatvédelem

Intelligensen azonosítja a bizalmas adatokat, testreszabott hozzáférési szabályzatokat alkalmaz a bizalmas információkhoz, és proaktívan csökkenti a szivárgás kockázatát a kontextus-érzékeny védelmi mechanizmusok révén.

Valós Idejű Kockázatriasztás

Hatékonyan figyeli és riasztást küld a kockázatos tevékenységekről, lehetővé téve az azonnali koordinációt a biztonságirányítási csapatokkal a proaktív fenyegetésre való reagálás érdekében.

Megfelelőségbiztosítás

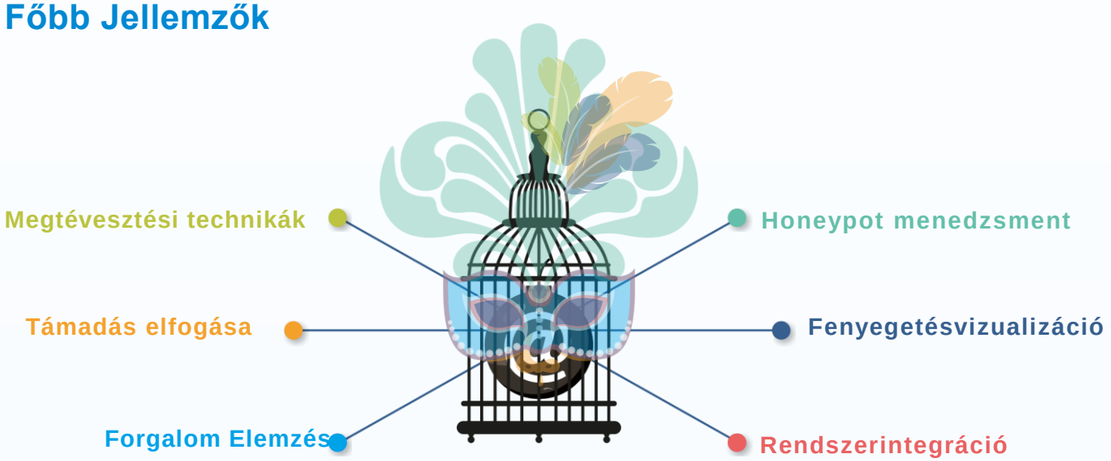
Biztosítja a szabályozásoknak való megfelelést, megkönnyítve a zökkenőmentes megfelelőségi auditokat és a szabályozások betartását a vállalatok számára.

Fő Előnyök

GUANAN
Elosztott Megtévesztő Rendszer

Mint hálózati biztonsági termék, a GUANAN Elosztott Megtévesztési Rendszer azzal a céllal készült, hogy javítsa a vállalati hálózati biztonsági képességeket. A rendszer megtévesztési technológiákra épül, és segíti az ügyfeleket a fenyegetések csapdába ejtésében és felismerésében. Előre telepített csalik segítségével eltereli a támadók figyelmét, és ráveszi őket, hogy ezeket a csalikat látogassák meg és támadják meg, ezáltal érzékeli és rögzíti a támadási viselkedést, majd visszakövetési és ellenintézkedési lehetőségeket biztosít, áttörést jelentve a hagyományos támadó-védő egyensúlytalansághoz képest.

Főbb Jellemzők



Alkalmazási Forgatókönyvek

A GUANAN elosztott megtévesztőrendszer intraneten történő telepítése képes észlelni az intranetes támadási viselkedéseket, beleértve a férgek terjedését, a zsarolóvírusok terjedését és a bányászszoftverek terjesztését, azonnal meghatározva a forrásokat a biztonsági kockázatok kiküszöbölése érdekében.

Intranet Behatolásészlelés

A támadók különféle taktikákat alkalmazva hatolnak be az intranetbe, belső programokat ugrószerverként használva felderítésre és támadásokra. A GUANAN elosztott megtévesztő rendszer csapdákat állít fel a rendellenes viselkedések azonosítására, javítja az intranet fenyegetéstudatosságát és átveszi az irányítást a biztonsági kezdeményezések felett.

Zsarolóvírusok és adatbányászat észlelése

Fenyegetésvédelmi együttműködés

A GUANAN elosztott megtévesztőrendszer, mint kulcsfontosságú intranet biztonsági hírszerzési forrás, szinkronizálja a rögzített eseményeket a SOC-val vagy más SIEM platformokkal, együttműködve más biztonsági rendszerekkel egy koherens védelmi mechanizmus létrehozása érdekében, megszilárdítva az intranet biztonságát.

GUANAN
Webalkalmazás Biztonsági Rendszer

A GUANAN Webalkalmazás Biztonsági Rendszer egy új WAAP alkalmazás, amely dinamikus védelmi technológiákra támaszkodik az automatizált gépi viselkedések elleni védelem érdekében. A passzív védekezés helyett proaktívan hajt végre dinamikus kód- vagy tartalom-elrejtést, titkosítást és token alapú hitelesítést. Képes elrejteni a sebezhetőségeket és a kódokat, valamint megvédi a rendszert az automatizált támadásoktól anélkül, hogy szabályokra, küszöbértékekre vagy aláírásokra támaszkodna. Lefedi a tipikus védelmi forgatókönyveket, beleértve a webes robotokat, eszköz-szkennelést, sebezhetőség-felderítést és adatbejárást. A támadások és fenyegetések észlelésével és feltárásával a rendszer a vállalati alkalmazásbiztonság őrzőjeként működik.

Főbb Előnyök

Alkalmazási Forgatókönyvek

Védelem Rosszindulatú robotok ellen

Proaktív védelmet implementál a kérelmek dinamikus, előre meghatározott mintákra való támaszkodás nélküli érvényesítésére, hatékonyan elfogja az automatizált webes feltérképező robotokat, és
védi az információkat a rosszindulatú webes adatgyűjtéstől a közösségi
médiában, az e-kereskedelemben, a közigazgatásban, a telekommunikációban, a térképszolgáltatásokban és az önkiszolgáló média platformokon.

Védelem Automatizált 0-NAPos sebezhetőség-észlelés ellen

Kihasználja az adatcsomagokat dinamikus obfuszkálási és legitimitási ellenőrzések végrehajtására, alapvetően az ismeretlen sebezhetőségek elleni védekezésre, és arra, hogy megakadályozza, hogy a támadók új sebezhetőségeket kihasználjanak az automatizált vizsgálatokhoz és támadásokhoz.

Védelem Webalkalmazás támadások ellen

Proaktív védelmi és szemantikai elemzési technikákat alkalmaz a kérések dinamikus validálására, valamint szintaktikai és lexikai elemzést végez, átfogó védelmet nyújtva a hagyományos webes alkalmazásokat fenyegető veszélyekkel, mint például az SQL-befecskendezés és a cross-site scripting (XSS).

Védelem API adatszivárgás ellen

Több motor védi az API-kat, felölelve az API kérési protokoll biztonságát, az API átviteli paraméterek biztonságát, az API alkalmazásbiztonságát és az API adatbiztonságot.
Ez a teljes életciklusra kiterjedő lefedettség kiküszöböli az API rosszindulatú támadásai és az érzékeny információk szivárgása által okozott biztonsági problémákat.

GUANAN
Végponti Felderítési és Reagálási Rendszer

A GUANAN Végponti Felderítési és Reagálási Rendszer több felhőplatformot és szerverarchitektúrát támogat, valamint könnyen telepíthető. A termék szoftver formájában kerül forgalomba, egyszerű konfigurációval és kezeléssel, valamint nagy pontosságú megfigyelési képességgel. A rendszer lehetőséget biztosít a vállalati üzemeltetési és biztonsági menedzsment szakemberek számára nagyszámú szerver biztonságos kezelésére, csökkentve az üzemeltetési költségeket, és jelentősen javítva a vállalat biztonsági védelmi képességeit még alacsonyabb biztonsági szakértelem mellett is.

Főbb Jellemzők

Eszközleltár
Pontos üzleti szintű eszközazonosítást és dinamikus áttekintést kínál. Az A/S architektúrának köszönhetően több mint 10 típusú hoszt és több mint 800 üzleti alkalmazás leltározását és felismerését támogatja, így átfogó betekintést nyújt az informatikai eszközökbe.

Kockázatészlelés
Ez a funkció lehetővé teszi a felhasználók számára a belső kockázatok pontos azonosítását, segítve a biztonsági csapatokat a problémák gyors felkutatásában és a megoldások kidolgozásában. Részletes eszköz- és kockázati információkat nyújt a mélyreható elemzéshez és reagáláshoz, biztosítva a proaktív fenyegetéscsökkentést.

Behatolásérzékelés
Többszörös észlelési képességeket biztosít a behatolási események valós idejű és pontos érzékeléséhez, a veszélyeztetett gazdagépek azonosításához és a hatékony válaszintézkedések megtételéhez – biztosítva a fenyegetések gyors elszigetelését és a hálózat ellenálló képességét.

Megfelelőségi alapérték
Betartja Kína információbiztonsági szintű védelmi (ISLP) követelményeit és a CIS (Center for Internet Security) referenciaértékeit, támogatva az operációs rendszerek, webalkalmazások, adatbázisok és egyéb üzleti környezetek több verzióját a szabályozási összhang biztosítása érdekében.

Forgatókönyvek

Gazdagép biztonsági védelme
Többféle válaszmechanizmust kínál – beleértve az automatikus blokkolást, a manuális elkülönítést, a fekete-/fehérlistákat és az egyéni munkafolyamatokat –, hogy a felhasználók hatékonyan, a központi helyen tudják megoldani a behatolási incidenseket, biztosítva a gyors fenyegetéselhárítást.

Speciális sebezhetőség-észlelés
Ügynökalapú folyamatos monitorozás és elemzés révén azonosítja a rendszer/alkalmazás sebezhetőségeit, az exp/poc-okat és az újonnan felmerülő fenyegetéseket, valamint kereszthivatkozásokat végez egy átfogó sebezhetőségi adatbázissal a pontos és hatékony észlelés érdekében.

ISLP megfelelőségi audit
Biztonsági alapkövetelményeket hoz létre a gazdarendszerek számára, testreszabott megfelelőségi ellenőrzéseket végezve különböző környezetekben. Szabványosított technikai keretrendszert biztosít a nem megfelelő konfigurációk azonosításához, a biztonsági intézkedések fokozásához és a kockázatok mérsékléséhez a szabályozási követelményekkel összhangban.

GUANAN
Sebezhetőségi Szkennelési Rendszer

Mint Kína vezető, átfogó, pontos és könnyen elérhető vállalati szintű sebezhetőség-kezelő rendszere, a GUANAN Sebezhetőség-ellenőrző Rendszer segít a hálózatban található mindenféle sebezhetőségi kockázat felderítésében, professzionális és hatékony biztonsági elemzést és javítási javaslatokat nyújt, valamint a biztonsági irányítási folyamatnak megfelelően ellenőrzi a javítások hatékonyságát, ezzel minimalizálva a támadási felületet és a lehetséges veszteségeket.

Főbb Jellemzők

Szolgáltatásfelderítés
Azonosítja az aktív hálózati eszközökön futó szolgáltatásokat és azok részleteit, biztosítva a működési infrastruktúra láthatóságát.

Eszközfeltárás
Észleli a hálózaton lévő aktív eszközöket, így átfogó betekintést nyújt a csatlakoztatott erőforrásokba.

Sebezhetőségi felmérés
Aktív eszközöket vizsgál a sebezhetőségek azonosítása és értékelése érdekében, betekintést nyújtva a kockázatok enyhítésébe és a javítások priorizálásába.

Eszközleltár
Aktív eszközöket vizsgál a konfigurációk – beleértve az operációs rendszert, a hardvert, a szolgáltatásokat és a telepített szoftvereket – meghatározásához a részletes eszközkezelés érdekében.

Főbb Előnyök

Nagy teljesítmény és stabilitás
A többmagos feldolgozás és a többszálú architektúra kihasználásával akár 100 000 tranzakciót is képes kezelni másodpercenként. Az elosztott telepítés és a párhuzamos feldolgozás biztosítja a jövőbiztos skálázhatóságot a változó igényekhez igazítva..

Hatalmas tárhely és lekérdezési hatékonyság
Helytakarékos tömörítést használ a tárolási költségek csökkentése érdekében, miközben lehetővé teszi a másodpercnél rövidebb idő alatti lekérdezési válaszokat billiónyi strukturált/strukturálatlan adat esetén – a gyors adatkeresés révén növelve a működési hatékonyságot.

Átfogó adatvizualizáció
Az intuitív irányítópultok valós idejű biztonsági áttekintést nyújtanak, míg egy automatizált jelentéskészítő rendszer testreszabott, iparági szabványoknak megfelelő jelentéseket generál – mind a holisztikus biztonsági monitorozási, mind az operatív elemzési igényeket kielégítve.

Speciális intelligens elemzés
A big data és a gépi tanulás felhasználásával integrálja, korrelálja és előrejelzi a többdimenziós, több forrásból származó adatokból származó információkat, így pontos fenyegetésészleléssel és nyomozati támogatással ruházza fel a biztonsági csapatokat.

Moduláris skálázhatóság és kompatibilitás
Dinamikus moduláris architektúrára épül, zökkenőmentes bővítést biztosít, és saját protokollelemzésen keresztül integrálható a mainstream safety equipment rendszerekkel. származó rendszerek integrációját a testreszabott munkafolyamatok egyszerűen.

GUANAN
Következő Generációs Tűzfalrendszer

A GUANAN Következő Generációs Tűzfalrendszer különféle hitelesítési módszereket tartalmaz, és lehetővé teszi az alkalmazásokon, tartalmakon és eszközökön alapuló, többdimenziós és részletes vezérlést, amely védelmet nyújt a hálózati fenyegetésekkel szemben, beleértve a DoS/DDoS támadásokat, a jelszótörési kísérleteket, a gyenge jelszavakat, a sebezhetőségek kihasználását, a vírusokat és a trójai programokat, ezáltal biztosítva a belső hálózati erőforrások jogos és biztonságos elérését. Költséghatékony, hatékony és integrált biztonsági védelmi élményt nyújt a különböző iparágak ügyfeleinek, és erőteljesen támogatja a vállalatokat a háromdimenziós hálózati biztonsági védelem kiépítésében.

Funkcionális specifikációk

Alapvető Hálózati Funkciók

· Transzparens, útválasztási és hibrid módok, valamint linkaggregáció támogatása;
· Forrás NAT, cél NAT, port NAT és statikus NAT elősegítése;
· VLAN és VRF engedélyezése;
· WLAN és 3G vezeték nélküli hozzáférés integrálása;
· Statikus útválasztás, szabályzatalapú útválasztás, internetszolgáltatói útválasztás és forrás interfész útválasztás biztosítása;
· Dinamikus OSPF, RIP és OSPFv3 útválasztási protokollok beépítése;
· Útválasztás-észlelési funkció telepítése;
· IPv6 statikus útválasztás, útválasztó-hirdetés és alagútkonverzió támogatása.

Tűzfal Képességei

· Nyolc elemből álló integrációs stratégia kidolgozása felhasználók alapján;
· alkalmazások, forrás/cél interfészek, IP-címek, szolgáltatások és idő;
· Erőforrás-kezelés megkönnyítése címek, szolgáltatások, ütemtervek, alkalmazások és felhasználók számára;
· Szabályzatprioritások módosításának engedélyezése;
· IPv6 biztonsági szabályzatok beépítése.

Biztonsági Védelem

· IP-MAC kötést, ARPspoofing védelmet és ARP Flood támadás elleni védelmet kínál;
· IPv4 anomáliacsomag-támadások, például Ping of Death, Land-Base, Tear Drop, TCP Flag Winnuke, Smurf, Jolt2 elleni védelem;
· Portszkennelés és IP-szkennelés elleni védelem;
· SYN Flood, UDP Flood, ICMP Flood, DNS Flood támadások elleni védelem interfészek és IP-címek alapján;
· IPv6 anomáliacsomag-támadások, például Winnuke, Land-Base, TCP Flag, Fraggle, IP Spoof stb. elleni védelem.

VPN Jellemzők

·Különböző IPSecVPN protokollok és telepítési módszerek támogatása;
·Házirend- és útvonalalapú IPSecVPN biztosítása;
·CA központok és X.509 tanúsítványformátumok integrálása;
·VPN Track felajánlása;
·SSL VPN alagút mód támogatása;
·GRE VPN beépítése;
·Biztonsági védelem és sávszélesség-kezelés biztosítása VPN alagutak alatt.

Forgalomirányítás

· Többszintű, beágyazott sávszélesség-kezelés megvalósítása csatornák, interfészek, felhasználók és alkalmazások alapján;
· Sávszélesség-prioritáskezelés jóváhagyása;
· Maximális sávszélesség-korlátok, minimális sávszélesség-garanciák és rugalmas sávszélesség érvényesítése;
· IP-címenkénti sebességkorlátozás felajánlása;
· Kizárási szabályzatok támogatása.

Behatolásészlelés és -megelőzés

· Automatikus protokollfelismerés;
· Több mint 3000 előre definiált támadási aláírást tartalmaz;
· Automatikus és manuális frissítéseket kínál az aláírás-adatbázishoz;
· Védelem a férgek, trójai programok, adathalászat és egyebek ellen.

Felhasználókezelés

· Helyi tűzfalon keresztüli felhasználóhitelesítés támogatása;
· Szabványos Radius, LDAP és harmadik féltől származó felhasználóhitelesítés integrálása;
· Portálon keresztüli felhasználóhitelesítés biztosítása;
· Online felhasználófigyelés és időtúllépés-kezelés engedélyezése;
· Központosított felhasználói szabályzatkezelés megkönnyítése.

Vírusvédelem

· Vírusszűrés HTTP, FTP, SMTP, POP3 és IMAP protokollokon keresztül;
· Bizonyos fájltípusok blokkolása;
· Tömörített fájlok vizsgálata akár 20 szint mélységig;
· Manuális és automatikus vírusadatbázis-frissítések támogatása;
· Kártékony URL-szűrés beépítése.

Vizualizáció

· Valós idejű eszközállapot-statisztikák megjelenítése a CPU, a memória és az interfész forgalmáról;
· Felhasználói és alkalmazásforgalmi statisztikák vizualizálása kördiagramokkal, oszlopdiagramokkal és trendvonalakkal;
· Felhasználók és alkalmazások valós idejű rangsorolása;
· Azonnali riasztások küldése a rendszereseményekről és a biztonsági kockázatokról.

Termékjellemzők

GUANAN
Behatolásmegelőző Rendszer

Ez egy új generációs behatolásmegelőző biztonsági termék. Az egyre kihívást jelentő hálózati környezetben, ahol egyre több rejtett fenyegetés és összetett forrás érinti a rendszereket, a GUANAN Behatolásmegelőző Rendszer a hálózat 2-től 7-ig terjedő rétegeinek alapos elemzését és észlelését végzi egy teljesen új, felhasználóközpontú nézőpontból. Képes megvédeni a hagyományos ARP és DDoS támadások, valamint a vírusok, férgek, trójai programok, túlcsordulásos támadások és más rosszindulatú viselkedések ellen, amelyek a hálózati forgalomban rejtőznek. A rendszer támogatja a jellemzőelemzést és a kockázatértékelést sandbox technológiával kombinálva, így átfogó védelmet nyújt ismert és ismeretlen fenyegetésekkel szemben. A GUANAN Behatolásmegelőző Rendszer teljes körű biztonsági védelmet biztosít a hálózati rétegtől az alkalmazási rétegig mind a felhasználók hálózatán, mind a szervereken, és megfelel a Többszintű Védelmi Rendszer (MLPS) 2.0 követelményeinek.

Főbb Jellemzők

Átfogó behatolásmegelőzés

Proaktív vírusvédelem

Fejlett állandó fenyegetés (APT) elleni védelem

Hatékony és pontos észlelési képességek

Nagy teljesítményű fenyegetéscsökkentés

Virtualizált skálázhatóság

Robusztus védelmi architektúra

Átfogó naplóellenőrzés

Felhasználóbarát kezelés

Korszerű biztonsági szakértelem és szolgáltatás

Főbb Előnyök

Szakképzett biztonsági védelem

Teljes spektrumú védelmet kínál a behatolások, rosszindulatú programok és DoS/DDoS támadások ellen integrált megelőzési mechanizmusokon keresztül.

Átfogó naplóellenőrzés

Többdimenziós statisztikai jelentéseket generál különféle naplóforrásokból, lehetővé téve a mélyreható megfelelőségi elemzést és az incidensek forenzikus vizsgálatát.

Nagy hatékonyságú precíziós érzékelés

A TCP csomagok újra-összeszerelését és a protokollállapot-elemzést használja ki a gyors és pontos fenyegetésazonosításhoz, minimális téves riasztással.

Nagy teljesítmény és megbízhatóság

Egységes észlelési technológiát, kettős aktív feladatátvételt és VRRP-t kínál a zökkenőmentes működés érdekében, biztosítva az alacsony késleltetésű feldolgozást és a nulla egyedi meghibásodási pontot.

Rugalmas hálózatépítés és telepítés

Támogatja a megkerülő, útválasztási és transzparens módokat a virtualizált telepítés mellett, így könnyedén alkalmazkodik a hibrid IT környezetekhez.

GUANAN
Biztonsági Szolgáltatások

A biztonsági szolgáltatások célja, hogy speciális technológiákon, folyamatokon és szakértelmen keresztül rendszerszintű védelmet nyújtsanak, lehetővé téve a szervezetek számára a kockázatok kezelését, a kritikus eszközök védelmét és a stabil működés fenntartását. A GUANAN adathalász e-mail gyakorlatokat kínál, amelyek a valós támadási helyzetek szimulálásával növelik a felismerési és védekezési képességet, ezáltal csökkentve az alkalmazottak rosszindulatú e-mailekkel való érintkezéséből eredő adatvédelmi incidensek kockázatát. Emellett a behatolási tesztelési szolgáltatásunk proaktív, hackereket utánzó módszereket alkalmaz a sebezhetőségek – például SQL injekció, cross-site scripting (XSS) és konfigurációs hibák – azonosítására a célrendszerekben. Mindkét szolgáltatás gyakorlati megoldásokat nyújt: az adathalász gyakorlatok erősítik az alkalmazottak tudatosságát és éberségét, míg a behatolási tesztelés technikai javítási stratégiákat és konkrét intézkedéseket biztosít a biztonsági hiányosságok megszüntetésére. Együttesen megerősítik a kibertámadások elleni védelmet, elősegítik a szervezeti biztonságtudatosságot, és összhangban állnak a kockázatcsökkentés legjobb gyakorlataival.

Adathalász e-mail gyakorlat

Terv kidolgozása és ütemezése

Állítson be egyértelmű határidőket és mérföldköveket.
Tervezzen realisztikus adathalász e-mail sablonokat (tárgysorok, tartalom, mellékletek).
Dolgozzon ki egy incidensre adott választervet a lehetséges kockázatokra.

Résztvevők és szerepkörök meghatározása

Határozza meg a résztvevők körét (pl. meghatározott csapatok/osztályok).
Osszon ki szerepköröket: feladók (szimulációk lebonyolításához), célpontok (címzettek) és megfigyelők (az eredmények nyomon követéséhez).

Gyakorlat utáni elemzés

Elemezze az adatokat az alkalmazottak tudatosságának felméréséhez (pl. kattintási arányok, válaszidők, észlelési arányok).
Gyakorlati hasznos információkat generálhat jelentések vagy irányítópultok segítségével, amelyekkel tájékoztatást nyújthat a képzések fejlesztéséről és a biztonsági stratégiáról.

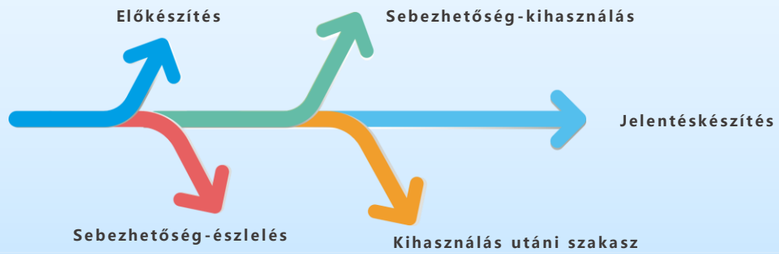
Viselkedésfigyelés és naplózás

Kövesse nyomon az e-mail kézbesítési állapotát (beérkezési idő, megnyitási arány).
Rögzítse a felhasználói interakciókat: linkkattintások, mellékletek letöltései, űrlapbeküldések vagy jelentett gyanús tevékenységek.

E-mailek létrehozása és küldése

Készítsen hitelesnek tűnő adathalász e-maileket meggyőző témákkal, rosszindulatú linkekkel vagy hamis mellékletekkel.
Terjessze az e-maileket a célközönséghez ellenőrzött csatornákon keresztül.

Behatolásvizsgálat



Contact Information

David Zeng
Director of international Business Development
strategic planning Department

+86 135 2061 7806
+44 751 5548 957
zenghao3094@idss-cn.com
www.idss-cn.com
Building 9, Shibei First Center, No. 3, Lane 1401, Jiangchang Road, Jing'an District, Shanghai, China

Please scan the QR code to add me as a friend