

Security Solution Guide

NAAD Co. Version: 2025.06.01

Security Solution Guide



۶	معرفی مجموعه
۱۰	تونل ارتباط امن
۱۱	خانواده تونل ارتباط امن دماوند
۱۵	خانواده تونل ارتباط امن دنا
۱۷	تونل ارتباط امن سه‌سند
۱۹	تونل ارتباط امن سه‌سند همراه
۲۲	خدمات امنیت
۲۴	خدمات تیم قرمز
۳۰	خدمات تیم آبی
۴۲	امنیت سیستم‌های کنترل صنعتی و فناوری‌های عملیاتی
۵۰	اعتبارات
۵۱	گواهی‌نامه‌ها
۵۳	مشتریان ما
۵۵	PT
۵۷	نمایشگاه‌ها

Table of Content

فهرست

Company Introduction

معرفی مجموعه



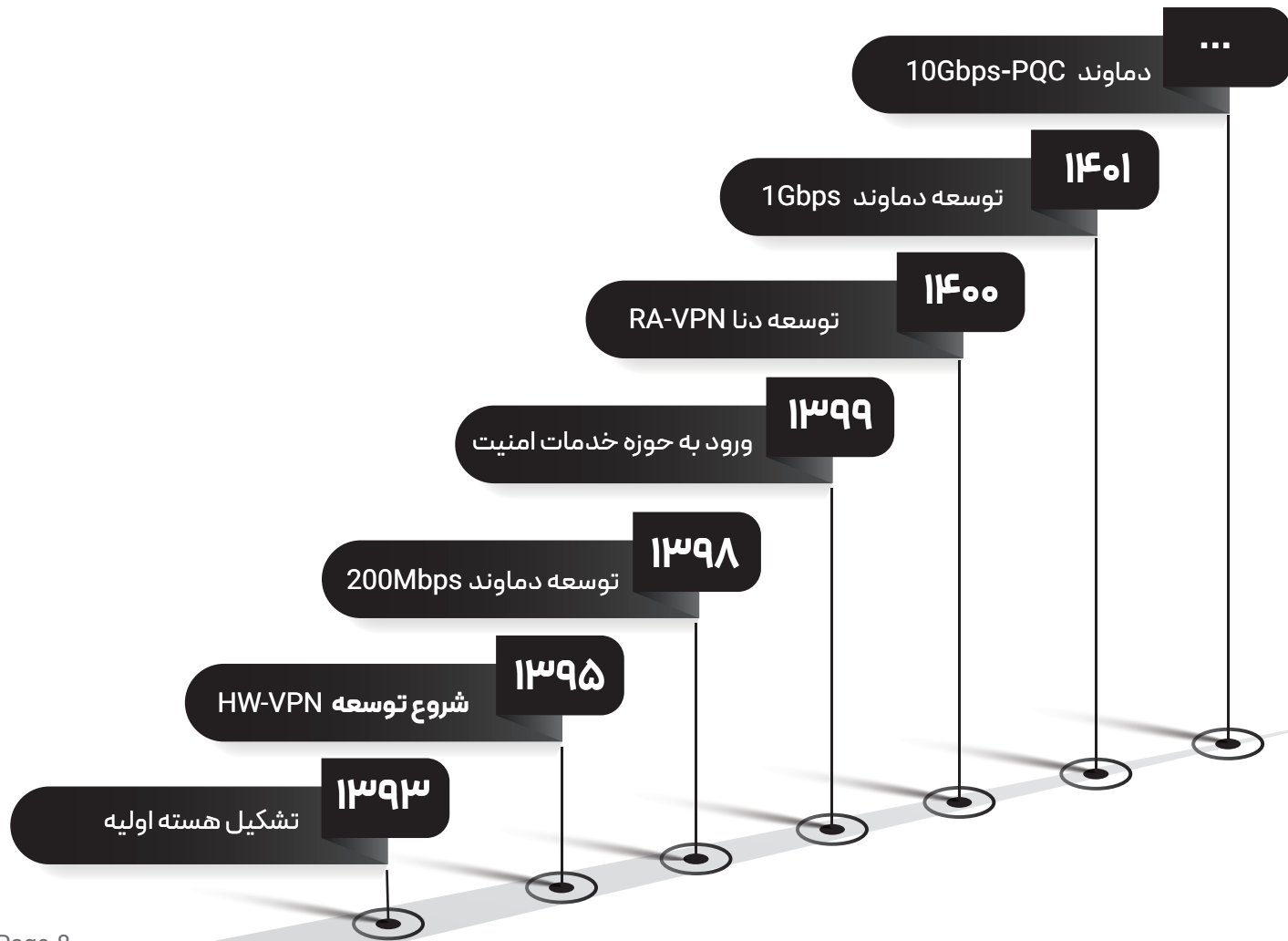
شرکت دانش بنیان **نواوران امن اندیش شریف** تحت برند **نآد** فعالیت خود را از سال ۱۳۹۳ به همت جمعی از اعضای هیات علمی و فارغ التحصیلان دانشگاه صنعتی شریف و با هدف امن سازی زیرساخت های حیاتی کشور آغاز کرد.

نآد چشم انداز خود را تقویت امنیت نقاط حساس و حیاتی کشور با رویکرد بومی و استفاده از دانش و مهارت متخصصان داخلی قرار داده است. رویکرد نآد پیاده سازی بومی و اصولی الگوریتم ها و الگوهای استاندارد بوده است. تیم تحقیق و توسعه شرکت نآد از جوانان نخبه و متخصص دانشگاه های صنعتی شریف، تهران، امیرکبیر و علم و صنعت تشکیل شده است.

نآد مسیر خود را از توسعه ماژول HSM^۱ آغاز کرد و در ادامه دانش انباشته بدست آمده را در دل خانواده محصول **تونل ارتباط امن سخت افزاری (Hardware VPN)** به کارگرفت. امنیت و پایداری این خانواده محصولات **حاصل یک دهه کار تحقیق و توسعه** مستمر می باشد. به کارگیری این محصول در زیرساخت های حساس و حیاتی کشور و کمک به ارتقا امنیت آن ها ، مایه افتخار و دلگرمی ماست.



در سال های اخیر به دلیل بروز چالش ها و حملات زیاد به زیرساخت های کشور و نیاز به ارتقاء دانش فنی سازمان های کلیدی کشور در حوزه امن سازی، در کنار توسعه تجهیزات زیرساختی ارائه خدمات امنیت (Securtiy Services) به این سازمان ها را نیز ماموریت خود قرار داده ایم. هدف ما کمک به تکمیل زنجیره امنیت در زیرساخت های حیاتی کشور است شامل تجهیزات امن و فرایندهای امن می باشد و خوشبختانه گام های موثری در این زمینه برداشته شد. دانش و خصوصاً تجربه انباشته این تیم، دارایی اصلی ما در انجام این ماموریت بوده است.



Hardware VPNs

تونل ارتباط امن سخت افزاری

- DAMAVAND Server-Side HVPNs (BareMetal)
- DENA Client-Side HVPNs (BareMetal)
- SAHAND Client-Side HOVPNs (Harden-OS)



DAMAVAND Hardware VPN Family

100Mbps | 1Gbps | 10Gbps^{coming soon}

Server-Side

ویژگی‌های کلیدی

- توسعه Bare-Metal و بدون سیستم عامل
- سطح مقطع نفوذ پایین و مقاوم در برابر آسیب‌های Zero Day سیستم عامل‌های متداول
- توسعه Data Plain بر بستر FPGA و مقاوم در برابر حملات مبتنی بر حافظه (Memory Attack)
- پشتیبانی از الگوریتم‌های رمز استاندارد مانند AES, RSA و ECDSA
- به کارگیری زیرساخت کلید عمومی (KPI)
- دارای قابلیت تولید اعداد تصادفی واقعی (TRNG)
- پشتیبانی از Tamper-Proof و مقاوم در برابر حملات فیزیکی



کارت تونل ارتباط امن دماوند 1Gbps

Security Solution Guide

DAMAVAND Family Technical Specification*

Type	100 Mbps	1 Gbps	10 Gbps coming soon
Architecture	Bare-metal	Bare-metal	Bare-metal
Packet per second (PPS)	16 Kpps	256 Kpps	512 Kpps
Simultaneous Tunnel Instances	15	60	60
NAT Traversal	Yes	Yes	Yes
Tamper-Proof	Yes	Yes	Yes
LAN Interface	1XGigEth - RJ45	RJ45	+SFP
WAN Interface	1XGigEth - RJ45	1XGigEth - SFP/RJ45	+SFP
Certificates	Yes	Yes	Yes
Side Channel Security	Yes	Yes	Yes
Cryptographic Algorithms	RSA 2048/4096 ECDSA (P-256) AES-256-GCM ECDH		
Custom Algorithms/ECC Curves	To be negotiated		
Audit Log	Yes	Yes	Yes

*For more information, see technical datasheet.



تونل ارتباط امن دماوند با Tamper-Proof



برد تونل ارتباط امن دماوند



Appliance نهایی دماوند جهت نصب روی رک شبکه^۱



تونل ارتباط امن دماوند- نصب شده روی
Appliance شرکت Nexcom

DENA Hardware VPN Family

Desktop | Portable coming soon

Client-Side

ویژگی‌های کلیدی

- توسعه Bare-Metal و بدون سیستم عامل
- سطح مقطع نفوذ پایین و مقاوم در برابر آسیب‌های Zero Day سیستم عامل‌های متداول
- توسعه Data Plain بر بستر FPGA و مقاوم در برابر حملات مبتنی بر حافظه (Memory Attack)
- پشتیبانی از الگوریتم‌های رمز استاندارد مانند RSA, AES و ECDSA
- به کارگیری زیرساخت کلید عمومی (KPI)
- دارای قابلیت تولید اعداد تصادفی واقعی (TRNG)



تونل ارتباط امن انفرادی دنا

Security Solution Guide

DENA Family Technical Specification*

Type	DENA Desktop	DENA Portable coming soon
Architecture	Bare-metal	Bare-metal
Encrypted Traffic Throughput	12 Mbps	12 Mbps
Simultaneous Tunnel Instances	1	1
NAT Traversal	Yes	Yes
Cryptographic Algorithms	RSA 2048/4096 ECDSA (P-256) AES-256-GCM ECDH	
Basic Post-Quantum Security	Yes	Yes
Certificate-based Tunnel	Yes	Yes
LAN Interface	USB Type-C	WiFi and USB
WAN Interface	1* 10/100/1000 ETH	3G/4G
Side Channel Security	Yes	Yes
Custom Algorithms/ECC Curves	To be negotiated.	
Tamper Resistant	No	Yes

*For more information, see [technical datasheet](#).

SAHAND-Desktop Hardware VPN

Desktop

Client-Side

ویژگی های کلیدی

- Tiny linux امن سازی شده (Harden OS)
- کاهش سطح مقطع نفوذ
- عدم اتصال مستقیم کلاینت نهایی به اینترنت خارج از VPN
- پشتیبانی از الگوریتم های رمز استاندارد مانند RSA, AES و ECDSA
- به کارگیری زیرساخت کلید عمومی (KPI)
- پشتیبانی از شبکه 4G/3G و سیم کارت سازمانی در سمت WAN
- پشتیبانی از شبکه Wi-Fi در سمت LAN
- راه اندازی آسان (Plug & Play)



تونل ارتباط امن انفرادی سهند

Security Solution Guide

SAHAND-Desktop Technical Specification*

Type	SAHAND Desktop
Architecture	Tiny Linux
Encrypted Traffic Throughput	12 Mbps
Simultaneous Tunnel Instances	1
NAT Traversal	Yes
Cryptographic Algorithms	RSA 2048/4096 ECDSA (P-256) AES-256-GCM ECDH
Basic Post-Quantum Security	Yes
Certificate-based Tunnel	Yes
LAN Interface	1*10/100 Eth / Wi-Fi
WAN Interface	1*10/100 Eth / WIFI/USB-C
Side Channel Security	Yes
Custom Algorithms/ECC Curves	To be negotiated
Battery	-

*For more information, see [technical datasheet](#).

SAHAND-Portable Hardware VPN

Portable

Client-Side

ویژگی های کلیدی

- Tiny linux امن سازی شده (Harden OS)
- کاهش سطح مقطع نفوذ
- عدم اتصال مستقیم کلاینت نهایی به اینترنت خارج از NPV
- پشتیبانی از الگوریتم های رمز استاندارد مانند RSA, AES و ECDSA
- به کارگیری زیرساخت کلید عمومی (KPI)
- پشتیبانی از شبکه 3G/4G وسیم کارت سازمانی در سمت WAN
- پشتیبانی از شبکه Wi-Fi در سمت LAN
- کوچک و قابل حمل با باتری 7000mAh
- راه اندازی آسان (Plug & Play)



تونل ارتباط امن انفرادی دهند همراه

Security Solution Guide

SAHAND-Portable Technical Specification*

Type	SAHAND Portable
Architecture	Tiny Linux
Encrypted Traffic Throughput	5 Mbps
Simultaneous Tunnel Instances	1
NAT Traversal	Yes
Cryptographic Algorithms	RSA 2048/4096 ECDSA (P-256) AES-256-GCM ECDH
Basic Post-Quantum Security	Yes
Certificate-based Tunnel	Yes
LAN Interface	WiFi
WAN Interface	3G/4G
Side Channel Security	Yes
Custom Algorithms/ECC Curves	To be negotiated
Battery	7000mAh (last up to 8 hours)

*For more information, see [technical datasheet](#).

Security Services

خدمات امنيت



Red Team Services

خدمات تیم قرمز



Red Team Operations

عملیات تیم قرمز

شرح خدمت

- تیم قرمز ما با توسعه ابزارها و چارچوب‌های اختصاصی، شبیه‌سازی جامع حملات پیشرفته را بر اساس چرخه MITRE ATT&CK از شناسایی اولیه تا استخراج داده‌ها انجام می‌دهد.

کاربرد و ضرورت

- این خدمت مقاومت سازمان در برابر حملات هدفمند (Targeted Attack) را می‌سنجد و امکان اولویت‌بندی اصلاح کنترل‌ها را فراهم می‌کند.

مزیت رقابتی ما

- تجربه‌ی عملی تیم ما در بیش از 20 پروژه‌ی سازمانی بزرگ
- بهره‌گیری از تکنیک‌ها و ابزارهای کاملاً اختصاصی
- گزارش‌های چندلایه (فنی، مدیریتی)

Penetration Testing

تست نفوذ

شرح خدمت

- تیم ما با بهره‌گیری ابزارهایی مانند Nessus ، Burp Suite و استانداردهایی مانند OWASP ، فرآیند تست نفوذ را از اسکن خودکار تا بررسی دستی منطق کسب‌وکار در سامانه تحت وب ، برنامه موبایلی و شبکه اجرا می‌کند

کاربرد و ضرورت

- تست نفوذ ابزاری کلیدی برای سنجش مقاومت سامانه در برابر حملات واقعی است که می‌توان از طریق آن اطمینان مشتریان و ذی‌نفعان را با ارائه گواهی‌نامه‌های امنیتی تقویت نمود.

مزیت رقابتی ما

- تجربه عملی در بیش از ده‌ها پروژه در حوزه‌های مختلف (مالی و صنعتی و ...)
- گزارش‌های یکپارچه فنی و استراتژیک برای استفاده افراد فنی و غیرفنی
- «شبیه‌سازی باگ بانته»، مشارکت دو کارشناس کمکی با تخصیص 20٪ زمان و پاداش برای هر باگ کشف‌شده، جهت افزایش عمق بررسی و انگیزه تیم

Cyber Threat Intelligence

هوش تهدید

شرح خدمت

- تیم هوش تهدید ما با استفاده از پلتفرم‌های تجاری داده‌های بدافزارها، زیرساخت‌های تهدید و شاخص‌های نفوذ (IoCs) را جمع‌آوری و تحلیل می‌کند تا چشم‌اندازی کامل از حملات در حال وقوع و پیش‌بینی‌شده ارائه دهد.

کاربرد و ضرورت

- این خدمت با تشخیص زودهنگام حملات نوظهور و شناسایی بازیگران تهدید، امکان دفاع پیشگیرانه، مقابله با تهدیدات پیچیده و انطباق با الزامات امنیتی را فراهم می‌کند.

مزیت رقابتی ما

- دسترسی به پلتفرم‌های پیشرفته مانند IntelX و چندین مخزن تجاری و متن‌باز برای عمق بخشی به تحقیقات
- تیم تحلیلگر با توان کشف و تحلیل تهدیدات منطقه‌ای و بین‌المللی
- گزارش‌های ساختارمند و کاربردی برای مخاطبان فنی و غیرفنی جهت تصمیم‌گیری سریع و مؤثر

Breach and Attack Simulation

شبیه‌سازی حملات

شرح خدمت

-شبیه‌سازی حملات با ابزارهای BAS (مانند Caldera) برای سنجش اثربخشی قواعد تشخیص در مرکز عملیات امنیت (SOC) و بهبود پاسخ به حملات در SOC.

کاربرد و ضرورت

شبیه‌سازی حملات سایبری با ابزارهای BAS به سازمان‌ها کمک می‌کند اثربخشی سامانه‌های تشخیص تهدید و پاسخ به حوادث را در شرایط واقعی بسنجند. این کار نقاط ضعف در مرکز عملیات امنیت را شناسایی و استراتژی‌های دفاعی را بهبود می‌بخشد.

مزیت رقابتی ما

-استفاده از کتابخانه حملات مبتنی بر MITRE ATT&CK و گزارش مدیریتی
-ارائه گزارش مفصل فنی برای ارتقاء COS و گزارش مدیریتی

Blue Team Services

خدمات تیم آبی



NIST CSF (Organizational Assessment Based on the NIST CSF Standard)

ارزیابی سازمان بر اساس استاندارد

شرح خدمت

-ارزیابی جامع امنیتی سازمان با استفاده از چارچوب NIST CSF برای شناسایی نقاط قوت و ضعف در لایه استراتژیک، تدوین نقشه راه امنیتی، و همسوسازی با استانداردهای جهانی مانند IEC 62443 در OT و NIST 800-53 در IT.

کاربرد و ضرورت

-این خدمت به سازمان‌ها کمک می‌کند تا وضعیت امنیتی فعلی خود را درک کرده، ریسک‌های کلیدی را کاهش دهند و با الزامات نظارتی بین‌المللی هماهنگ شوند.

مزیت رقابتی ما

-ارائه گزارش مدیریتی از وضعیت امنیتی فعلی سازمان و ارائه وضعیت مطلوب سازمان در چشم انداز بلندمدت
-ارائه پروژه‌های میان‌مدت برای ارتقاء سطح امنیت کلی سازمان

Secure Network Architecture

بازطراحی امن معماری شبکه

شرح خدمت

-بازطراحی معماری شبکه با استفاده از الگوی Cisco SAFE ، بهینه‌سازی سلسه‌مراتب دسترسی، و پیاده سازی قابلیت‌های امنیتی مانند فایروال‌های نسل جدید (NGFWs) Next-Generation Firewalls)) برای کاهش سطح حمله و افزایش مقاومت در برابر نفوذ.

کاربرد و ضرورت

-سازمان‌ها با معماری‌های غیراصولی در معرض تهدیدات پیشرفته قرار می‌گیرند. این خدمت با طراحی معماری شبکه به صورت ماژولار و رعایت اصل دفاع در عمق موجب افزایش سطح امنیتی شبکه می‌شود و احتمال نشت داده‌ها را کاهش می‌دهد.

مزیت رقابتی ما

-تجربه موفق در بازطراحی شبکه برای سازمان‌های دولتی، بانکی و صنعتی با بیش از 15 پروژه ملی.
-استفاده از ابزارهای شبیه‌ساز (مانند GNS3) قبل از اجرا برای کاهش downtime و افزایش سرعت و کیفیت پیاده سازی
-ارائه مستندات فنی و نقشه‌های شبکه به زبان ساده برای تسهیل تصمیم‌گیری.

Security Audit

ارزیابی جامع امنیتی

شرح خدمت

- ارزیابی جامع امنیتی سازمان با رویکرد استاندارد محور در حوزه های زیر:
- ارزیابی امنیتی معماری شبکه بر اساس الگوی Cisco SAFE
- ارزیابی تجهیزات شبکه و تجهیزات امنیتی بر اساس CIS و Cisco NFP
- ارزیابی سرویس ها، سرورها، و کلاینت ها بر اساس چکلیست های CIS و اختصاصی نآد
- ارزیابی مرکز عملیات امنیت (SOC) بر اساس SOC-CMM، SANS Sec 511

کاربرد و ضرورت

- شناخت نقاط ضعف امنیتی پیش از وقوع حمله، امکان تخصیص منابع بهینه و انطباق با الزامات بالادستی مانند افتا و پدآفند

مزیت رقابتی ما

- تجربه موفق در ارزیابی امنیتی سازمان های دولتی، بانکی و صنعتی با بیش از 15 پروژه ملی.
- پوشش کامل امنیت سازمان در حوزه های مختلف.
- ارائه مستندات فنی به زبان ساده برای تسهیل تصمیم گیری.

Hardening

امن سازی

شرح خدمت

-خروجی خدمت ارزیابی امنیتی سازمان فهرستی از تهدیدات امنیتی در سطح مختلف است. به ازای هرکدام از تهدیدات، اقدامات امن سازی در سطوح کوتاه مدت، میان مدت، و بلندمدت تعریف می شود.

کاربرد و ضرورت

-ارزیابی امنیتی سازمان بدون امن سازی آن فایده ای برای سازمان ندارد. امن سازی زیرساخت ها و سرویس های سازمانی، اولین خط دفاعی در برابر تهدیدات سایبری است.

مزیت رقابتی ما

-طراحی سفارشی راهکارها بر اساس معماری و ریسک های خاص سازمان.
-تجربه اجرای موفق در ده ها پروژه ملی با تمرکز بر سازمان های حساس و حیاتی

Security Operations Center

راه اندازی SOC

شرح خدمت

- پیاده سازی مرکز عملیات امنیت (SOC) با ابزارهای نظارتی پیشرفته (مانند Splunk و ELK)، آموزش تیم تحلیلگر، و تعریف فرآیندهای پاسخ به حوادث.

کاربرد و ضرورت

- SOC به سازمان ها امکان رصد بلادرنگ تهدیدات، کاهش زمان پاسخگویی، و یکپارچه سازی ابزارهای امنیتی را می دهد

مزیت رقابتی ما

- راه اندازی مرکز عملیات امنیت (SOC) برای چند سازمان خصوصی
- استفاده از استانداردها و منابع مرجع در راه اندازی SOC مانند 11 Strategies of a World-Class SOC

Vulnerability Assessment

ارزیابی آسیب پذیری ها

شرح خدمت

-اسکن مستمر دارایی های IT با ابزارهایی مانند Tenable، اولویت بندی ریسک ها بر اساس CVSS، و ارائه راهکارهای اصلاحی.

کاربرد و ضرورت

-شناسایی و رفع آسیب پذیری ها قبل از سوء استفاده مهاجمان، امنیت سازمان ها را در بلندمدت تضمین می کند.

مزیت رقابتی ما

-تجربه VA در ده ها سازمان بانکی و دولتی
-ارائه گزارش فنی مفصل و گزارش مدیریتی ساده و قابل فهم
-ارائه مشاوره برای برطرف کردن آسیب پذیری های شناخته شده

Secure Software Development Lifecycle (SDLC) Implementation and Auditing

پیاده‌سازی و ممیزی چرخه توسعه امن نرم افزار

شرح خدمت

-مشاوره در طراحی فرآیندهای توسعه امن (SSDLC)، آموزش تیم‌های توسعه و DevOps و ممیزی کد با ابزارهایی مانند SonarQube.

کاربرد و ضرورت

-پیشگیری از باگ‌های امنیتی در مراحل اولیه توسعه، هزینه‌های اصلاحی را به شدت کاهش می‌دهد.

مزیت رقابتی ما

-ارائه چکلیست‌های سفارشی متناسب با فناوری‌های سازمان
-تجربه ارائه خدمت SSDLC به سازمان‌های خصوصی

External Attack Surface Management

راه اندازی (EASM)

شرح خدمت

- تیم ما با بهره‌گیری از Shodan ، Censys و اسکنرهای اختصاصی، دارایی‌های آنلاین سازمان را کشف، طبقه‌بندی و به صورت مستمر پایش می‌کند.

کاربرد و ضرورت

- مدیریت سطح حمله خارجی با ارائه دید کامل از نقاط در معرض خطر و آسیب‌پذیری‌ها، از حملات ناشناخته و نشت داده پیشگیری می‌کند.

مزیت رقابتی ما

- دسترسی به پلتفرم‌های پیشرو مانند Censys ، RiskIQ و مخازن جهانی برای پوشش جامع دارایی‌های اینترنتی
- پایش ۷/۴۲ و هشدار آنی

Computer Security Incident Response Team

عملیات CSIRT

شرح خدمت

-تشکیل تیم پاسخگویی به حوادث امنیتی (CSIRT) با تمرکز بر بازیابی سریع سامانه‌ها، جمع آوری شواهد دیجیتال، و تحلیل ریشه‌ای علل حوادث.

کاربرد و ضرورت

-حوادث امنیتی به سرعت می‌توانند به بحران‌های مالی و اعتباری تبدیل شوند. این خدمت زمان پاسخگویی را به شدت کاهش داده و از تشدید آسیب‌ها جلوگیری می‌کند.

مزیت رقابتی ما

-تجربه مدیریت موفق ده‌ها بحران سایبری در سازمان‌های بانکی و دولتی
-استفاده از چارچوب‌های معتبر (مانند NIST SP 800-61) برای واکنش ساختاریافته.
-ارائه گزارش مفصل برای بهبود سطح امنیتی سازمان

Threat Hunting

شکار تهدید

شرح خدمت

-پایش فعالانه شبکه و نقاط انتهایی با استفاده از ابزارهای Threat Hunting (مانند Thor) برای شناسایی تهدیدات پنهان و TPAها.

کاربرد و ضرورت

-شکار تهدید با شناسایی فعالیت‌های مشکوک و تهدیدات پنهان پیش از وقوع حملات مخرب یا استخراج داده‌های حساس سازمان، امکان واکنش پیش‌دستانه را برای سازمان فراهم می‌کند. این رویکرد موجب کاهش ریسک نفوذهای پیشرفته می‌شود.

مزیت رقابتی ما

-تجربه ارائه خدمت شکار تهدید در ده‌ها سازمان بانکی و دولتی
-گزارش دهی به زبان مدیریتی با ارائه نقشه مسیر مقابله و همچنین، ارائه گزارش مفصل فنی برای ارتقاء تشخیص حملات در سازمان

ICS/OT Security

امنیت سیستم‌های کنترل صنعتی و فناوری‌های عملیاتی

Network Security Architecture

ارزیابی امنیتی معماری شبکه بر اساس مدل مرجع ICS 410

شرح خدمت

-ارزیابی معماری شبکه‌های صنعتی مطابق با مدل مرجع ICS 410 SANS ، با تمرکز بر دو محور حفاظت (Protection) و تشخیص (Detection).

کاربرد و ضرورت

-شناسایی نقاط ضعف طراحی شبکه‌های صنعتی و به‌روزرسانی زیرساخت‌های امنیتی برای مقابله با تهدیدات پیشرفته.

مزیت رقابتی ما

- ارائه گزارش‌های فنی همراه با نقشه‌های شبکه به زبان ساده.
- تجربه عملی در ارزیابی امنیتی شبکه‌های ICS/SCADA در صنایع حیاتی کشور.
- تحلیل‌های بومی‌سازی شده متناسب با الزامات سازمان‌ها و زیرساخت‌های صنعتی داخلی.
- ارائه راهکارهای اصلاحی قابل اجرا با توجه به محدودیت‌های عملیاتی محیط‌های صنعتی.

ICS/OT Penetration Testing

تست نفوذ صنعتی

شرح خدمت

- شبیه سازی حملات کنترل شده بر پروتکل های ارتباطی، Firmware و تجهیزات صنعتی (ICS/OT) برای شناسایی آسیب پذیری های پنهان با حداقل اختلال در فرآیندهای تولید.

کاربرد و ضرورت

- پیشگیری از اختلالات عملیاتی و سوءاستفاده مهاجمان با کشف زود هنگام نقاط ضعف.

مزیت رقابتی ما

- اجرای تست نفوذ با حداقل ریسک و بدون ایجاد اختلال در فرآیندهای حساس صنعتی.
- استفاده از ابزارهای تخصصی و تیم مجرب با سابقه در صنایع حساس.
- گزارش های عملیاتی با راهکارهای اصلاحی فوری.

Industrial Security Operations Center

راه اندازی مرکز عملیات امنیت (SOC) صنعتی

شرح خدمت

- پیاده سازی SOC صنعتی با راهکارهای خاص این حوزه، شامل آموزش نیروی متخصص، راه اندازی SIEM صنعتی (مانند Splunk)، و تعریف فرآیندهای نظارت بلادرنگ.

کاربرد و ضرورت

- کاهش زمان پاسخگویی به رخدادهای امنیتی و یکپارچه سازی ابزارهای نظارتی در محیط های صنعتی.

مزیت رقابتی ما

- تجربه مشاوره راه اندازی SOC در صنایع مختلف
- ارائه مدل Managed SOC برای کاهش هزینه های عملیاتی.

SANS ICS 410

آموزش SANS ICS410: معماری امن شبکه‌های صنعتی

شرح خدمت

- دوره آموزشی مبتنی بر استاندارد SANS ICS 410 برای آموزش طراحی و پیاده‌سازی معماری امن شبکه‌های صنعتی با تمرکز بر چالش‌های واقعی.

کاربرد و ضرورت

- ارتقای دانش فنی پرسنل جهت طراحی زیرساخت‌های مقاوم در برابر تهدیدات سایبری.

مزیت رقابتی ما

- محتوای آموزشی مبتنی بر سناریوهای عملی و هماهنگ با نیازهای بومی
- تجربه آموزش به ده‌ها سازمان دارای شبکه صنعتی

Industrial Security Operations Center Setup Training

آموزش راه اندازی مرکز عملیات امنیت (SOC) صنعتی

شرح خدمت

-آموزش نیروهای سازمان در راه اندازی و مدیریت SOC صنعتی، شامل پیاده سازی SIEM (Splunk/ELK)، NSM، و فرآیندهای مدیریت رخدادها

کاربرد و ضرورت

-توانمندسازی تیمها برای تشخیص و پاسخ به تهدیدات خاص حوزه صنعتی.

مزیت رقابتی ما

-ارائه چکلیستهای عملیاتی و شبیه سازی سناریوهای واقعی.
-پشتیبانی پس از آموزش جهت اجرای موفقیت آمیز پروژه ها.



Credits

اعتبارات







مشتریان ناآد



شرکت خدمات انفورماتیک



سازمان برنامه و بودجه کشور



جمهوری اسلامی ایران
وزارت صنعت معدن و تجارت



مشتریان نآد



مهسان



دانشگاه صنعتی شریف



بانک ملت



ارایه کننده راهکارهای بانکی و پرداخت



کسارت ایران (سهامی خاص)
هلدینگ فن آوری و نوآوری مصاد



بانک مرکزی جمهوری اسلامی ایران

Positive Technologies



شرکت Positive Technology با برند PT در سال ۲۰۰۲ در روسیه تاسیس گردیده است و یکی از بازیگران جدی امنیت سایبری در این کشور می باشد که از سال ۲۰۰۹ به عرصه بین المللی ورود پیدا کرده است.

شرکت PT از ابتدای سال ۱۴۰۳ به شکل رسمی به بازار ایران ورود پیدا کرده است و نآد توزیع کننده (distributor) اصلی و پشتیبان فنی محصولات PT در ایران می باشد و تاکنون به چندین شرکت معتبر مجوز نمایندگی فروش اعطا کرده است.

Product Portfolio by Positive Technologies

Meta Products

- MaxPatrol O2
- MaxPatrol Carbon

Solutions

- | | | |
|----------------------------|------------------------------|-------------------------------|
| ■ Secure Development | ■ Infrastructure Development | ■ Industrial Network Security |
| ■ PT BlackBox | ■ PT Sandbox | ■ PT ISIM |
| ■ PT Application Inspector | ■ PT NGFW | ■ PT Knockin |
| ■ PT Application Firewall | ■ PT NAD | |
| | ■ MaxPatrol VM | |
| | ■ MaxPatrol EDR | |



Exhibitions



نمایشگاه اینوتکس ۲۰۲۴



نمایشگاه پدافند غیرعامل ۲۰۲۳

Exhibitions



نمایشگاه الکامپ ۲۰۲۴



گرفه مشترک ناَد و PT در نمایشگاه الکامپ ۲۰۲۴



Naad Secure



www.naadsecure.ir



info@naadsecure.ir



+98-2166013542



No.2 , Sadeqi St. , East Side of Sharif Univ. , Tehran, Iran