مدیریت یکپارچه تهدیدات امنیتی (میتا)

UNIFIED THREAT MANAGEMENT

MITA Unified Threat Management

www.mitautm.com

مقدمه

اطلاعات، دارایی است که همانند سایر دارایی‌های مهم برای سازمان، حائز اهمیت بوده و باید مورد حفاظت قرار گیرد. امروزه با گسترش امنیتی شبکه‌های رایانه‌ای که می‌تواند به نوعی پتانسیل ایجاد وقایع ناخواسته با امکان منجر شدن یا وارد آمدن آسیب به سیستم و یا سازمان به صورت عمدی و یا سهوی، توسط انسان و یا قهری، بوده باشد، وجود یک ساختار امن در سازمان‌ها و ادارات ضروری به نظر می‌رسد.

در همین راستا مطابق تاکید نهادهای متولی امر در کشور، دپارتمان امنیت شبـکه گـروه شرکت‌های افق اندیشه غرب، اقدام به طراحی، تولید و پیاده‌سازی **سیستم مدیریت یکپارچه تهدیدات امنیتی شبکه‌های رایانه‌ای (میتا)** (اینترنت، اینترانت) با هدف تامین امنیت شبکه و جلوگیری از نفوذهای غیرمجاز، جلوگیری از ورود نرم‌افزارهای جاسوسی به داخل شبکه، امکان برقراری ارتباط امن بین مراکز سازمان در یک بستر عمومی، نظیر اینترنت، امکان مدیریت بهینه منابع اینترنتی (پهنای باند) و افزایش بهره‌وری و مدیریت یکپارچه ساختار اینترنت اعم از گـزارش‌گیری‌های مختلف، مـدیریت کاربران و ... (به تفصیل در بخش بعدی آمده است) نموده و پس از تست محصول در محیط آزمایشگاهی و عملیاتی، اقدام به بهره‌برداری تجاری نموده است.

چالش‌ها

بطور اختصار از چالش‌های پیش روی شبکه‌های رایانه‌ای می‌توان به موارد زیر اشاره نمود:

- اتلاف منابع مالی سازمان طی آسیب رسیدن به اطلاعات سازمانی و سخت‌افزارها از طریق نفوذهای مخرب و نرم‌افزارهای جاسوسی، ویروسی و ...
- کاهش بهره‌وری سازمان طی گردش‌های بدون هدف کاربران در وب
- عدم امکان مدیریت و کنترل منابع قابل دسترس کاربران و فایل‌های دریافتی (دانلود شده) توسط کاربران
- عدم امکان گزارش‌گیری میزان کارکرد استفاده از منابع، نظیر پهنای باند
- عدم امکان پیگیری و ردگیری رخدادهای کاربری و سیستمی
- عدم امکان تخصیص منابع (پهنای باند) با اولویت سرویس‌های ارزشمند مطابق با نیاز کاربران
- عدم امکان برقراری ارتباط امن و کاملا خصوصی بین مراکز مختلف سازمان
- اتلاف منابع نظیر پهنای باند جهت استفاده مجدد در ارتباط با سایت‌های مورد بازدید قبلی
- عدم وجود ساختار "**شرایط بروز خطا**" به هنگام رخداد قطعی در لینک ارتباط سازمان
- عدم امکان ایجاد ساختار احراز هویت کاربران جهت استفاده از منابع اینترنتی

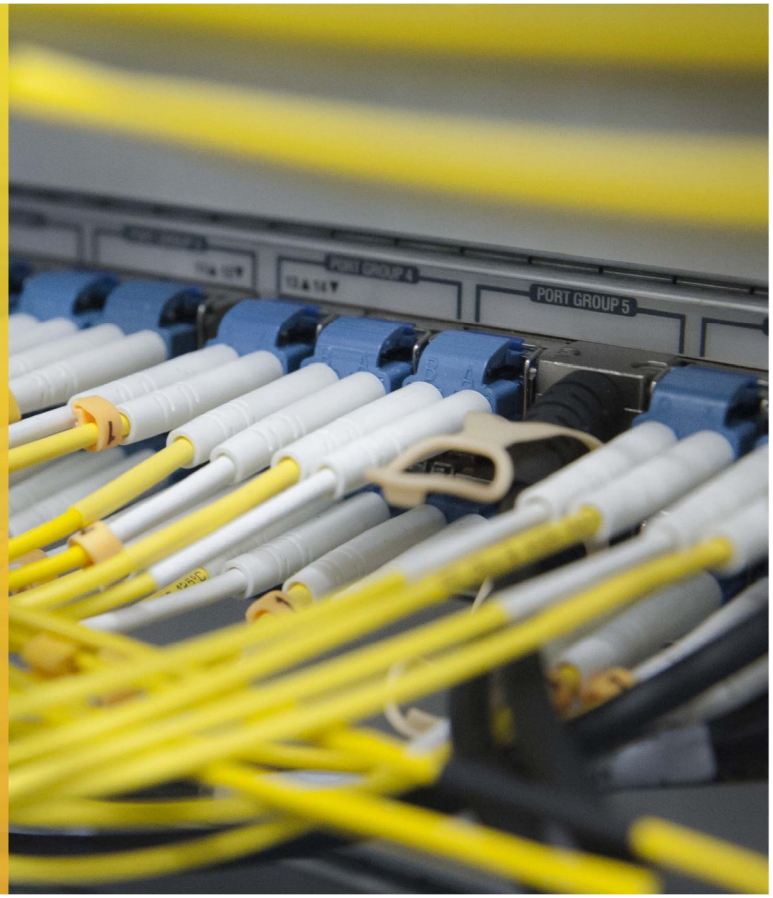
ویژگی‌های فنی

- فایروال
- QOS
- WAF
- VPN
- FailOver / Load Balancing
- IDS / IPS
- ابزارهای شبکه
- سرویس‌های شبکه
- مدیریت پهنای باند
- اکانتینگ
- مسیریابی
- اکتیو دایرکتوری
- انتقال / بررسی‌کننده DNS
- وب فیلتر
- آنتی اسپم
- گزارشگیری
- DHCP/DHCPv6
- NTP
- مدیریت گواهینامه‌های دیجیتال
- مدیریت کاربران

ویژگی‌های منحصربفرد میتا

برخی از ویژگی‌های کلی و منحصر بفرد محصول میتا، به شرح زیر است :

- دارای تاییدیه فنی از شورای عالی انفورماتیک و گواهینامه ارزیابی امنیتی از سازمان فناوری اطلاعات
- تولید محصول به صورت کاملا بومی، توسط متخصصین دپارتمان امنیت شبکه
- واسط مدیریت تحت وب کاملا فارسی جهت مدیریت ساده و قابل دسترس در کل شبکه
- دارای ۸ رده سیستم سخت افزاری با مشخصات مختلف جهت کارآیی‌های متفاوت
- دارای ۳۰ زیر سیستم کاربردی تحت مدیریت متمرکز
- پشتیبانی کامل از تاریخ شمسی و میلادی
- پشتیبانی از خدمات پس از فروش توسط کارشناسان شرکت و نمایندگان سراسر کشور
- امکان مدیریت احراز هویت تحت ۳ روش مستقل :
  - سیستم احراز هویت میتا
  - VPN
  - پروکسی
- دارای ابزارهای مدیریت سرویس‌های شبکه تحت واسط کاربری نظیر (Trace Route/DNSlook up/ SNMP Packet Capture / ...)
- امکان ارائه سرویس Load Balancing برای دو حالت دروازه‌ها (GateWays) و سرویس‌ها و سرورهای داخلی



ماژول فایروال

فراهم نمودن پارامترهای مختلف امنیت شبکه‌های رایانه‌ای و جلوگیری از نفوذهای غیرمجاز و مسدود کردن حملات با امکانات فنی ذیل:

- قابلیت تعریف سطوح مختلف امنیتی جهت هر واسط نظیر (.../Internal/External/DMZ)
- سازگاری با مکانیزم NAT تحت ۳ متد (Port Forwarding, Static NAT,Outbound NAT)
- قابلیت تعریف قواعد جهت مکانیزم‌های فوق بر اساس پارامترهایی هم چون (آدرس‌های IP مبدا و مقصد، آدرس پورت‌های مبدا و مقصد، پروتکل، واسط
- قابلیت ایجاد سیاست‌های امنیتی به تفکیک هر واسط بر اساس:
  - آدرس‌های IP مبدا و مقصد
  - پروتکل
  - شماره پورت مبدا و مقصد (شماره پورت‌های رزرو شده به تفکیک پروتکل‌ها، محدوده پورت)
  - سیستم عامل مبدا
- قابلیت اختصاص دروازه (Gateway) به ازاء هر قاعده (Rule)
- قابلیت شناسایی شماره کدهای TOS به ازاء هر قاعده
- قابلیت محدود کردن تعداد حالات (State) برای هر قاعده
- قابلیت اعمال زمانبندی برای هر قاعده
- قابلیت گروه‌بندی و نام‌گذاری سفارشی آدرس‌ها، میزبان‌ها، پورت‌ها و ... جهت مدیریت ساده‌تر (Aliases)
- قابلیت اعمال Flagهای TCP به ازا هر قاعده
- قابلیت اعمال سایر پارامترهای مدیریت کیفیت سرویس (QOS) نظیر محدودکننده‌های پهنای باند، انواع صف‌ها و ... برای هر قاعده
- قابلیت تعریف همگام‌سازی (Sync) یا عدم همگام‌سازی یک قاعده در ساختار "شرایط بروز خطا" در سیستم پشتیبان (Fail Over)

- امکان ثبت وقایع و ارائه گزارش ترافیک تطبیق یافته با هر قاعده
- امکان مشاهده اتصالات برقرار شده بصورت آنلاین
- قابلیت اعمال یک قاعده بر روی چند واسط بصورت همزمان
- قابلیت تعریف انواع آدرس‌های مجازی (آدرس Fail Over, IP Alias)
- قابلیت اختصاص آدرس‌های مجازی به واسط خاص
- قابلیت اختصاص آدرسها بصورت آدرس تکی و یا آدرس شبکه
- قابلیت استفاده از این آدرس‌ها در انواع مکانیزم‌های NAT
- قابلیت استفاده به عنوان IP و یا IPهای جانبی یک واسط، جهت استفاده در پروسه مسیریابی

ماژول مسیریابی

- قابلیت ایجاد چندین دروازه
- قابلیت ایجاد مسیر های استاتیک
- قابلیت گروه‌بندی دروازه‌ها (LoadBalancing/FaiOver/LoadSharing)
- قابلیت ایجاد دروازه های IPv6
- پشتیبانی از RIP نسخه ۱ و ۲
- پشتیبانی از پروتکل OSPF
- پشتیبانی از پروتکل BGP

ماژول مدیریت کیفیت سرویس

- قابلیت فعال کردن مکانیزم‌های زمانبندی شامل: (HFSC, CBQ FAIRQ, PRIQ) به ازاء هر واسط
- قابلیت اختصاص پهنای باند
- قابلیت اضافه کردن‌های صف‌های متعدد بر اساس مکانیزم‌های صف‌های فوق به ازاء هر واسط
- قابلیت تعریف انواع محدودکننده‌ها (Limiter) بر اساس عرض باند، آدرس مبدا، آدرس مقصد، تاخیر، نرخ Packet Loss، سایز صف، سایز Bucket و تعریف منحنی سرویس
- قابلیت استفاده از پارامترهای تعریف شده در قواعد فایروال
- قابلیت گزارشگیری از وضعیت صف‌ها در قسمت گزارشگیری سیستم
- قابلیت گارانتی کردن عرض باند خاص به ازاء سرویس‌های تعریف شده

ماژول مدیریت پهنای باند

قابلیت مدیریت و تخصیص پهنای باند تحت زیر سیستم‌های :

- مدیریت کیفیت سرویس (QOS)
- فایروال
- سیستم جامع اکانتینگ به ازاء کاربر یا هر گروه
- درگاه احراز هویت
- پراکسی
- VPN

ماژول VPN

- سازگاری با زیر سیستم جامع اکانتینگ میتا
- پشتیبانی از پروتکل‌های IPsec, PPTP, PPPoE, L2TP, SSL VPN, IKEv2 L2TP / Ipsec
- قابلیت مشاهده اتصالات و کاربران آنلاین با قابلیت Kill کردن کاربران
- امکان بر قراری ارتباطات بین مراکزی امن (Ipsec,SSL VPN)
- سازگاری با زیر سیستم مدیریت پهنای باند جهت اختصاص پهنای باند به اتصالات VPN
- سازگاری با زیر سیستم فایروال جهت ایجاد قواعد امنیتی مختص اتصالات VPN
- سازگاری با زیر سیستم وب فیلترینگ جهت ایجاد قواعد فیلترینگ مختص اتصالات VPN
- امکان تعریف سرویس برای کاربران موبایل
- دارای کلاینت اختصاصی ویندوزی

ماژول WAF

- امکان تعریف پورت‌های متعدد برای سرویس‌دهی
- امکان تعریف میزبان‌های مجازی متعدد
- امکان تعریف پروتکل‌های http, https
- پشتیبانی از حالت Reverse Proxy
- دارای قواعد پرمیوم OWASP
- پشتیبانی از بیش از ۴۰،۰۰۰ قاعده
- امکان بروزرسانی قواعد از سرورهای میتا
- قابلیت تبدیل سرویس های HTTP به HTTPS
- قابلیت تعریف بالانسر برای سرویس های مختلف
- قابلیت اضافه شدن یک لایه احراز هویت کاربری

ماژول Fail over / load balancing

- قابلیت گروه‌بندی دروازه‌ها
- قابلیت اولویت‌بندی دروازه‌های یک گروه
- قابلیت استفاده همزمان از چند دروازه (Load Sharing)
- قابلیت مدیریت بروز خطا و تقسیم بار بر اساس دروازه‌ها و سرویس دهنده‌های داخل شبکه
- قابلیت همگام‌سازی (Sync) بین چند دستگاه میتا جهت پیاده‌سازی مدیریت بروز خطا (Failover)
- استفاده از پارامترهای ارزیابی شامل: Down بودن دروازه، درصد Packet Loss، حداکثر میزان تاخیر و یا ترکیب چند پارامتر
- قابلیت تقسیم بار بین سرورهای داخلی جهت ترافیک ورودی به منطقه (Zone) و یا DMZ
- قابلیت اختصاص گروه دروازه‌ها در قواعد فایروال
- قابلیت اختصاص گروه دروازه‌ها برای هر واسط
- قابلیت تعریف دروازه‌ها به عنوان جایگزین دروازه اصلی
- قابلیت ویرایش هر کدام از پارامترهای کنترلی فوق
- قابلیت مشخص کردن پارامترها جهت همگامسازی
- پارامتر ارزیابی توسط: ICMP, TCP, HTTP, HTTPS, SMTP
- قابلیت تعریف واسط مورد استفاده بین دو دستگاه جهت همگامسازی
- قابلیت تعریف FailOver برای همه ماژول های میتا

ماژول استقال دهنده DNS

- قابلیت استقرار در شبکه به عنوان سرور DNS اصلی
- قابلیت تعریف انواع رکوردهای DNS
- قابلیت رونویسی میزبان ها
- قابلیت رونویسی دامنه ها
- پشتیبانی از DNS
- قابلیت تعریف سطوح دسترسی جهت استفاده از سرور

ماژول IDS / IPS

قابلیت تعریف سیاست‌های IPS به ازاء هر واسط با قابلیت اعمال:
شاخه‌ها و زیر شاخه‌های از پیش تعریف گردیده شامل:

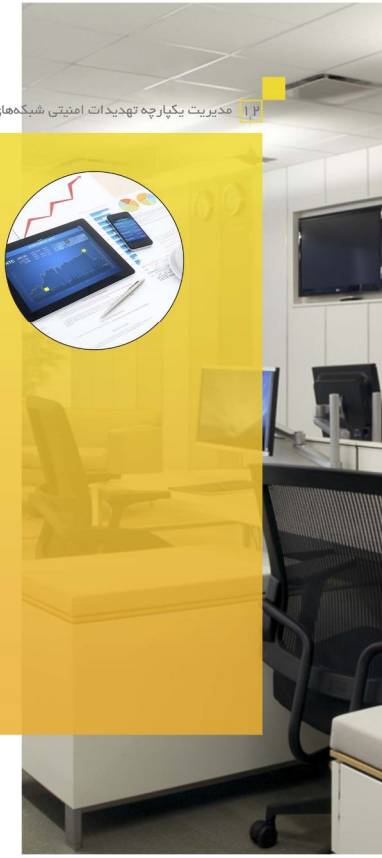
- حملات مشخص نظیر : Dos, DDos, Session Attack, Sniffing Scanning, Phishing, SQL, Oracle, MySQL, Web, ...
- کدهای مخرب، ویروسها، تروجان‌ها، SpyWare, MalWare Spam,Worm و ...
- انواع Exploit ها
- انواع حملات مبتنی بر سرویس نظیر : DNS, ICMP, Netbios, Rpc, Telnet, FTP, SNMP, SMTP, POP3, IMAP, SSH , ... و بیش از یکصد شاخه اصلی و چندین هزار زیر شاخه تعریف گردیده
- قابلیت فعال یا غیر فعال نمودن قواعد هر شاخه
- قابلیت تعریف سرویس‌های موجود در شبکه جهت فعال نمودن IPS به آن سرویس
- قابلیت به روز رسانی بانک اطلاعاتی IPS بصورت خودکار از سرورهای داخل کشور
- قابلیت بروزرسانی به صورت آفلاین برای شبکه‌های بدون دسترسی اینترنت
- قابلیت ارائه گزارش و اخطار سفارشی از کارکرد IPS به صورت آنلاین
- قابلیت مشاهده و مدیریت میزبان‌های بلوک شده توسط سیستم IPS
- قابلیت تعریف لیست سفید حاوی (آدرس IP، دامنه، سرورهای مجازی، اتصالات VPN) قابل اعتماد جهت عدم بررسی توسط IPS
- قابلیت تعریف فیلتر بر اساس واژه کلیدی خاص جهت عدم بررسی توسط IPS
- پشتیبانی از Multi-Threading در سوریکاتا
- اضافه شدن قواعد پرمیوم لابراتوار سورس فایر (سیسکو)
- اضافه شدن قواعد پرمیوم لابراتوار Emerging Threats Pro
- امکان بروزرسانی روزانه از سرور های داخل کشور و سایت میتا
- اضافه شدن ۱۰ تا ۳۰ قاعده بصورت روزانه برای جلوگیری از ویروس‌ها، تروجان ها و کدهای مخرب
- امکان انتخاب یکی از دو ماژول IDS/IPS (اسنورت، سوریکاتا)

ماژول ابزارهای شبکه

- امکان ارائه ابزارها و سرویس‌های مدیریت شبکه در پانل اصلی جهت سهولت در مدیریت شبکه نظیر: DNS Lookup Ping, Tracert, Packet Capture, ARP Table, SNMP Service
- قابلیت تعریف مقادیر جایگزین سفارشی (Aliases) جهت پارامترهای کاربری نظیر: واسطها، میزبان‌ها، آدرسهای IP، پورت‌ها و . . . جهت سهولت در مدیریت سیستم

ماژول اکتیو دایرکتوری

- سازگاری کامل با اکتیو دایرکتوری ویندوز جهت احراز هویت و اکانتینگ
- پشتیبانی از اکتیو دایرکتوری نسخه ۲۰۰۳،۲۰۰۸،۲۰۱۲
- قابلیت احراز هویت از چندین سرور اکتیو دایرکتوری بصورت بلادرنگ (بدون ورود اطلاعات کاربران به میتا)
- قابلیت اختصاص سطوح دسترسی به گروه‌ها و کاربران اکتیو دایرکتوری در سرویس احراز هویت
- امکان اختصاص خاصیت‌های اکانتینگ به کاربران اکتیو دایرکتوری شامل: اختصاص پهنای باند، حجم زمانی، حجم ترافیکی، زمان اتصال، ... (برای اولین بار)
- پشتیبانی از قابلیت SSO برای کاربران اکتیو دایرکتوری
- امکان استفاده از کاربران اکتیو دایرکتوری جهت احراز هویت در تمامی سرویس‌های میتا



ماژول اکانتینگ

- قابلیت تعریف پارامترهای مختلف اکانتینگ (کاربر، گروه، ایستگاه)
- سازگاری با زیر سیستم‌های درگاه احراز هویت میتا، VPN و پراکسی
- قابلیت پشتیبانی از گروه کاربری LAN, Dialup و xDSL
- پشتیبانی از LDAP جهت Import کردن گروه‌های کاربری از Windows Active Directory / Linux LDAP Server
- قابلیت تعریف پروفایل کاربری شامل: نام، نام خانوادگی، ایمیل، تلفن، آدرس و مشاهده آن در بخش کاربران آنلاین
- قابلیت تعریف محدودیت‌های حجم ترافیکی و زمانی، بصورت دائمی، روزانه، هفتگی، ماهانه به ازاء گروه یا کاربر
- قابلیت تعریف محدودیت عرض باند ارسال و دریافت برحسب کیلو بیت برثانیه به ازاء گروه یا کاربر
- قابلیت زمان اتصال در ایام هفته بصورت ۲۴ ساعته به ازاء گروه یا کاربر
- قابلیت تعریف تعداد اتصال همزمان به ازاء یک نام کاربری
- قابلیت اختصاص آدرس (IP، پورت، پروتکل، نوع سرویس و . . .) به نام کاربری
- قابلیت تعریف متد احراز هویت (PAP, CHAP , . . .) به ازاء گروه یا کاربر
- قابلیت تعریف آدرس صفحه وب جهت مشاهده هنگام ورود و خروج کاربر یا گروه
- قابلیت تعریف سایر پارامترهای اکانتینگ به صورت سفارشی
- قابلیت تعریف ایستگاههای خارجی مانند Router, Access Server, RRAS, Linux, VPN جهت استفاده از امکانات اکانتینگ میتا
- قابلیت تعریف کاربران بصورت دسته‌ای در قالب فایل متنی و اکسل
- پشتیبانی از متدهای احرازهویت شامل : پراکسی، پرتال احرازهویت، VPN

ماژول گزارشگیری

- گزارشات دسترسی : قابلیت ایجاد گزارش‌های دسترسی بر اساس نام کاربری، آدرس IP، آدرس اینترنتی، تاریخ و بازه زمانی
- گزارشات حجمی و زمانی : قابلیت ایجاد گزارش‌های حجمی و زمانی ترافیک بر اساس نام کاربری، آدرس IP، تاریخ و بازه زمانی
- قابلیت استخراج کلیه گزارشات با فرمت اکسل
- قابلیت حذف گزارشات ایجاد شده

گزارشات واسط ها

- قابلیت ارائه گزارش‌های آماری، اطلاعاتی هر واسط بر اساس وضعیت واسط (UP, Down)، آدرس سخت‌افزاری، مشخصات TCP/IP، میزان بسته‌های ورودی و خروجی مجاز یا غیرمجاز، میزان خطاهای ورودی و خروجی.

سوابق :

- ثبت سوابق دسترسی کاربران در بازدید از سایت ها و فایل های دریافتی
- ثبت کلیه سوابق حجمی و زمانی کاربران میتا
- ثبت کلیه سوابق سیستمی و سرویس های سیستم
- ثبت سوابق فایروال، وف ، IDS/IPS
- امکان ارسال کلیه سوابق سیستم به سرور سیسلاگ خارجی

ماژول رویس‌های شبکه

- پشتیبانی از پروتکل‌های BGP, OSPF, RIP V1,2
- قابلیت ایجاد پارامترهای مسیریابی (Routing) تحت مکانیزم ایستا (Static) و پویا (Dynamic)
- قابلیت تعریف دروازه پیش فرض (Default Gateway) و دروازه‌های سیستم
- قابلیت تعریف آدرس مانیتور به ازاء هر دروازه جهت کنترل Down بودن، میزان Ping Time, Packet Loss
- قابلیت تعریف واسط‌ها و امکان اعمال پارامترهای Q-i-Q, GIF, GRE PPP-X پل (Bridge, Link Aggregation) به ازاء هر واسط
- قابلیت ایجاد VLANها بر اساس هر واسط
- قابلیت گروه‌بندی واسط‌ها
- قابلیت تعریف هر واسط بر اساس انواع اتصالات شامل (Static, DHCP, PPP, PPPoE, PPTP)
- قابلیت ایجاد سرور DHCP و امکان تخصیص سرویس به ازاء هر واسط
- پشتیبانی از پروتکل DHCP Relay
- قابلیت ایجاد سرور DNS و سرویس RFC2136
- قابلیت تعریف انتقال دهنده DNS و (DNS Forwarder)
- قابلیت تعریف سرور PPPoE
- قابلیت تعریف سرور NTP

نمودارهای گرافیکی

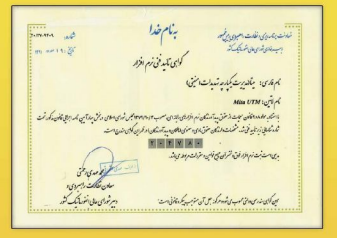
- قابلیت ارائه نمودارهای گرافیکی وضعیت سیستم براساس : پردازنده، حافظه اصلی، جدول حالات، ترافیک عبوری سیستم و تجمیع همه حالات
- قابلیت ارائه نمودارهای گرافیکی وضعیت ترافیک براساس: واسط‌ها، ترافیک ورودی و خروجی
- قابلیت ارائه نمودارهای گرافیکی وضعیت بسته‌های ترافیکی
- قابلیت ارائه نمودارهای گرافیکی وضعیت کیفیت سرویس بر اساس : دروازه‌ها، ترافیک ورودی و خروجی
- قابلیت ارائه نمودارهای گرافیکی سفارشی براساس موارد فوق در بازه زمانی دلخواه

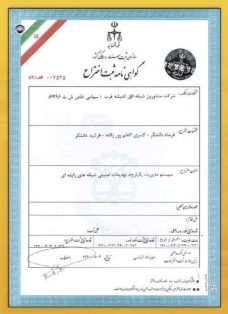
گزارشات سیستمی

- قابلیت ارائه گزارش‌های آنلاین و ثبت شده از زیرسیستم‌های: فایروال، VPN, QOS و سرویس‌های شبکه براساس پارامترهای هر سیستم.
- قابلیت سفارشی نمودن گزارشات براساس نوع رخداد و امکان ارسال به سرور syslog خارجی

گواهینامه ها و مجوزها

- گواهی رتبه بندی و احراز صلاحیت شرکت های انفورماتیکی
- گواهینامه ثبت اختراع سیستم مدیریت یکپارچه تهدیدات امنیتی شبکه‌های رایانه‌ای
- گواهی ارزیابی امنیتی محصول میتا
- گواهینامه تائید فنی نرم افزار میتا





نسخه **Standard** جهت کاربری در شبکه‌های استاندارد

نسخه **Enterprise** جهت کاربری در مراکز داده متوسط

نسخه **Advance** جهت کاربری در زیرساخت شبکه‌های متوسط تا بزرگ

نسخه **Ultimate** جهت کاربری در مراکز داده

برخی از مشتریان

گروه شرکت‌های افق اندیشه

آدرس : تهران، ملاصدرا، شیرازی جنوبی، کوی بهاران، پلاک ۱۰، واحد ۲
تلفن : ۸۸۹۷۰۹۲۶ فکس : ۸۸۹۷۰۹۲۷
info@oanc.ir – www.oanc.ir وب سایت میتا : www.mitautm.com