راهکار مایکروسافت برای ایمن‌سازی شبکه‌های سازمانی چیست؟

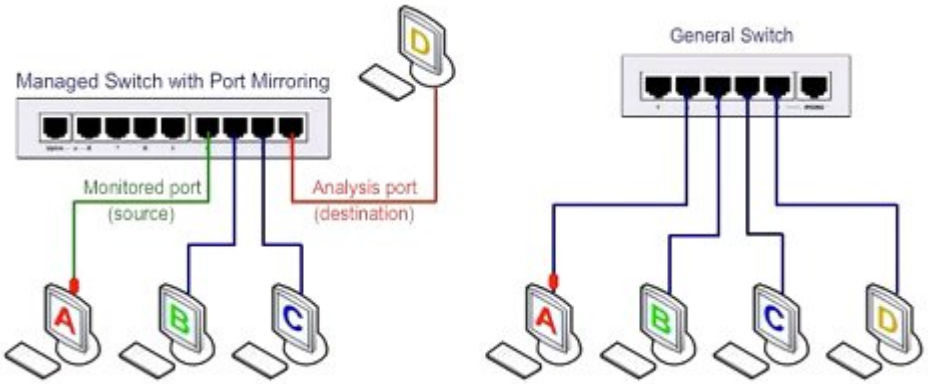
آشنایی با معماری تجزیه و تحلیل پیشرفته تهدیدات (ATA)

فناوری تجزیه و تحلیل پیشرفته تهدیدات (ATA) سرنام Advanced Threat Analytics یک زیرساخت درون سازمانی است که برای مقابله با حملات سایبری پیشرفته برون و درون سازمانی استفاده می‌شود. فناوری فوق برای تایید مجوزها، اعتبارنامه‌ها و جمع‌آوری اطلاعات از یک موتور اختصاصی و پروتکل‌های مختلفی همچون ، Kerberos NTLM ، RPC ، DNS و نمونه‌های مشابه برای ضبط و تحلیل ترافیک شبکه استفاده می‌کند.

مایکروسافت برای محافظت از شبکه‌های سازمانی در برابر تهدیدات بالقوه‌ای که ممکن است سامانه‌های امنیتی قادر به کشف آن‌ها نباشند و همچنین پیشگیری از نشت اطلاعات توسط کارمندان داخلی پیشنهاد می‌کند سازمان‌ها از فناوری تجزیه و تحلیل پیشرفته تهدیدات استفاده کند. با توجه به اهمیت فناوری فوق در ایمن‌سازی شبکه‌های کامپیوتری در این مطلب به‌طور اجمالی معماری داخلی این فناوری را بررسی می‌کنیم. اگر مدیر یک شبکه سازمانی متوسط یا کوچک هستید یا نگران تهدیدات سایبری در شبکه هستید، پیشنهاد می‌کنیم در اولین فرصت نگاهی جدی به این راهکار قدرتمند داشته باشید. ابزار تجزیه و تحلیل پیشرفته تهدیدات به راحتی از سایت مایکروسافت قابل دریافت است و مشکل خاصی در ارتباط با نصب آن وجود ندارد، البته به شرطی که سیستم‌عامل سرور شبکه یا مرکز داده بیش از اندازه قدیمی نباشد.

معماری تجزیه و تحلیل تهدیدات پیشرفته چیست؟

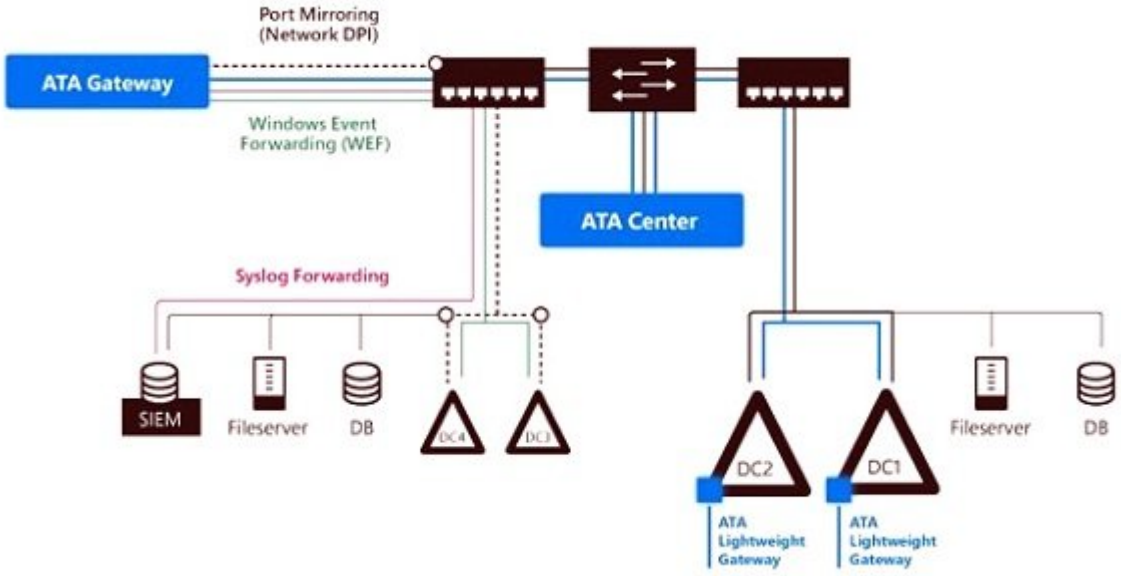
معماری فوق برای تجزیه و تحلیل ترافیک یک کنترل کننده دامنه شبکه از الگوی نظارت بر درگاه (Port Monitoring) مرتبط با مولفه ATA Gateway استفاده می‌کند. در این روش سوئیچ یا روتر یک کپی از تمامی بسته‌های اطلاعاتی که از یک درگاه خاص یا کل شبکه محلی عبور می‌کنند را برای درگاه دیگری ارسال می‌کنند تا ارزیابی و تحلیل شوند. در این روش روی یکی از درگاه‌های سوئیچ ویژگی نظارت بر درگاه فعال می‌شود تا اطلاعات برای یک سیستم ناظر در شبکه ارسال شود. در شکل 1 نحوه عملکرد دو سوئیچ مختلف را مشاهده می‌کنید که روی یکی از آن‌ها ویژگی Port mirroring فعال شده، در حالی که سوئیچ دوم (سمت راست) به شکل عادی در شبکه استفاده شده است.



اگر مولفه ATA Lightweight Gateway به شکل مستقیم در کنترل‌کننده‌های دامنه پیاده‌سازی شود، ضرورتی ندارد از فناوری نظارت بر درگاه استفاده شود، زیرا ATA می‌تواند از رخدادهای ثبت شده در کنترل‌کننده دامنه یا اطلاعات سرور SIEM برای تجزیه و تحلیل داده‌ها و شناسایی تهدیدات استفاده کند. ATA Gateway و ATA Lightweight Gateway دو مولفه مهم معماری تجزیه و تحلیل تهدیدات پیشرفته هستند. البته دقت کنید مولفه ATA Lightweight Gateway عملکردی یکسان با ATA Gateway دارد و درون ATA Center قرار می‌گیرد.

مولفه‌های معماری تجزیه و تحلیل پیشرفته تهدیدات

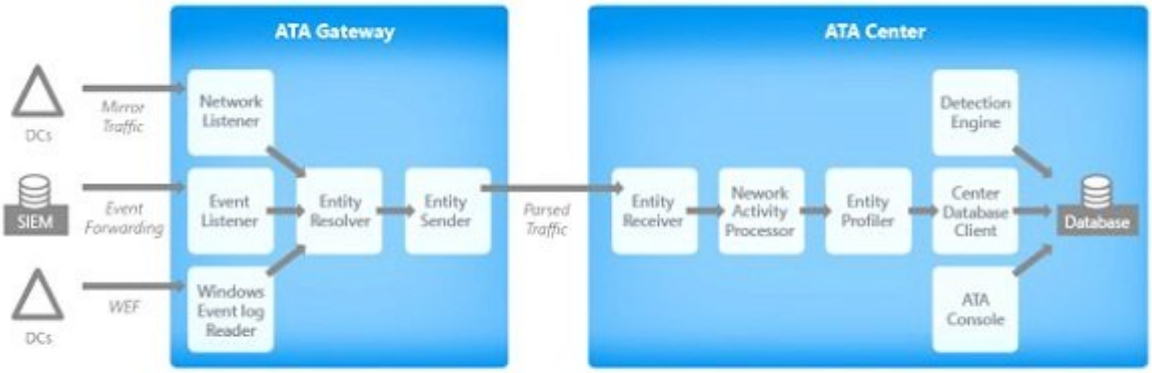
شکل 2 معماری فناوری تجزیه و تحلیل پیشرفته تهدیدات (ATA) سرنام Advanced Threat Analytics را نشان می‌دهد. فناوری فوق از سه مولفه مهم زیر ساخته شده است:



Advanced Threat Analytics Center: این مولفه داده‌ها را از ATA Gateway یا ATA Lightweight Gateway که در ساختار شبکه پیاده‌سازی شده‌اند دریافت می‌کند.

ATA Gateway: مولفه فوق درون یک سرور اختصاصی نصب می‌شود تا ترافیک ارسال شده از کنترل‌کننده‌های دامنه را بررسی کنید. برای دریافت ترافیک مولفه ATA Gateway می‌توان از راهکار Port Mirroring یا Network TAP استفاده کند.

ATA Lightweight Gateway: مولفه فوق به شکل مستقیم در کنترل‌کننده دامنه نصب می‌شود و ترافیک را بدون نیاز به سرور اختصاصی یا پیکربندی Port Mirroring کنترل می‌کند. در برخی شبکه‌ها مولفه فوق جایگزین ATA Gateway می‌شود. در زمان پیاده‌سازی معماری تجزیه و تحلیل پیشرفته تهدیدات این امکان وجود دارد که مولفه ATA Center نیز در شبکه اضافه شود تا دسترسی به هر دو مولفه ATA Gateway، ATA Lightweight Gateway یا ترکیبی از هر دو مورد امکان‌پذیر شود. شکل 3 نحوه پیاده‌سازی فناوری ATA در یک شبکه سازمانی را نشان می‌دهد.



پیاده‌سازی معماری تجزیه و تحلیل پیشرفته داده‌ها

سازمان‌ها می‌توانند به شکل ترکیبی گیت‌های مربوط به ATA را در شبکه سازمانی نصب کنند. برای این منظور گزینه‌های زیر در دسترس سازمان‌ها قرار دارد:

به‌کارگیری ATA Gateways بدون مولفه‌های دیگر: در روش فوق تنها گیت‌وی‌های مربوط به این فناوری نصب شده و خبری از نصب ATA Lightweight نخواهد بود. در روش فوق لازم است تمامی کنترل‌کننده‌های دامنه به شکلی پیکربندی شوند تا Port Mirroring روی درگاه‌های سوئیچ یا روتر فعال شوند و به یک ATA Gateway یا Network TAP برای انتقال ترافیک متصل شوند.

به‌کارگیری ATA Lightweight Gateway بدون مولفه‌های دیگر: روش دوم به‌کارگیری مولفه ATA Lightweight Gateway بدون مولفه‌های دیگر است. در روش فوق درون هر یک از کنترل‌کننده‌های دامنه پیاده‌سازی می‌شود. در این روش نیازی نیست هیچ سرور مضاعفی اضافه شده یا پیکربندی خاصی در ارتباط با Port Mirroring انجام شود.

به‌کارگیری دو مولفه Lightweight Gateway و ATA Gateway: در روش فوق هر دو مولفه یاد شده در یک شبکه نصب می‌شوند. راهکار فوق زمانی استفاده می‌شود که یک سازمان شعب مختلفی در یک شهر یا شهرهای دیگر دارد و هر یک کنترل‌کننده دامنه محدود به خود را دارند و لازم است بر روند اطلاعات مبادله شده در این کنترل‌کننده‌های دامنه نظارت کرد. در تمامی موارد، گیت‌وی‌ها داده‌های خود را برای مولفه ATA Center ارسال می‌کنند.

ATA Center چیست؟

ATA Center یکی از مولفه‌های کلیدی معماری فوق بوده و کارهای زیر را انجام می‌دهد:

- مدیریت و نظارت بر پیکربندی ATA Lightweight Gateway و ATA Gateway
- دریافت داده‌ها از ATA Gateway و ATA Lightweight
- ردیابی فعالیت‌های مشکوک
- پیاده‌سازی و اجرای الگوریتم‌های یادگیری ماشین ATA با هدف تشخیص رفتارهای غیر عادی
- پیاده‌سازی و اجرای الگوریتم‌های قطعی (Deterministic) برای شناسایی حملات پیشرفته بر مبنای زنجیره حملات
- پیاده‌سازی کنسول تجزیه و تحلیل پیشرفته تهدیدات

مدیران شبکه می‌توانند ATA Center را به گونه‌ای پیکربندی کنند تا در صورت شناسایی یک فعالیت مشکوک ایمیل یا هشداری را ارسال کند.
ATA Center ترافیک پالایش شده توسط مولفه‌های ATA Gateway و ATA Lightweight را دریافت می‌کند و در ادامه الگوریتم‌های یادگیری ماشین را برای ارزیابی الگوی رفتاری ترافیک‌ها فراخوانی می‌کند تا هرگونه بدافزار یا

ترافیک غیرقابل شناسایی را پیدا کرده و گزارشی برای مدیر شبکه ارسال کند. به‌طور مثال، تعاملات روزانه یک کارمند با سامانه‌ها مشخص است، حال اگر این کارمند تصمیم بگیرد رفتار خارج از قاعده‌ای انجام دهد که سامانه‌های تشخیص و پیشگیری از نفوذ قادر به شناسایی آن نیستند، معماری تجزیه و تحلیل پیشرفته تهدیدات این حالت را تشخیص داده، گزارشی آماده کرده و برای دپارتمان امنیت اطلاعات یا شبکه ارسال می‌کند. عناصر تشکیل دهنده مولفه ATA Center به همراه عملکرد آن‌ها در جدول1 نشان داده شده است.

Entity Receiver	تمامی اطلاعات مرتبط با ATA Gateway و ATA Lightweight را در قالب دسته‌هایی (Batch) دریافت می‌کند.
Network Activity Processor	تمامی فعالیت‌های تحت شبکه درون هر دسته (Batch) را پردازش می‌کند. به‌طور مثال، تطابق دادن مراحل مربوط به پروتکل کربروس که ممکن است در کامپیوترهای مختلف اجرا شود از جمله این موارد است.
Entity Profiler	تمامی موجودیت‌های منحصر به فرد تحت شبکه را بر مبنای ترافیک و رخدادهایی که تولید می‌کنند طبقه‌بندی می‌کند. به‌طور مثال، ATA می‌تواند فهرست تمامی ورودها به کامپیوترهای مختلف را بر مبنای هر پروفایل کاربری به‌روزرسانی کند.
Center Database	بر فرآیند نوشتن مولفه Network Activities و رخدادهای مرتبط با بانک اطلاعات نظارت می‌کند.
Database	ATA از بانک‌اطلاعاتی MongoDB برای ذخیره‌سازی تمامی داده‌های مربوط به فعالیت‌های انجام شده در شبکه، فعالیت‌های مرتبط با رخدادها، فعالیت‌های مشکوک، پیکربندی ATA و فعالیت‌های منحصر به فرد استفاده می‌کند.
Detectors	این مولفه از الگوریتم‌های یادگیری ماشین و خط‌مشی‌های قطعی برای کشف فعالیت‌های مشکوک و رفتارهای غیر عادی در شبکه استفاده می‌کند.
ATA Console	داشبوردی برای پیکربندی فناوری تجزیه و تحلیل تهدیدات پیشرفته و نظارت بر فعالیت‌های مشکوک شناسایی شده توسط ATA ارائه می‌کند. داشبورد فوق مستقل از ATA Center است و حتا زمانی که سرویس فوق غیر فعال شود، اما ارتباط با بانک اطلاعاتی برقرار باشد به کار خود ادامه می‌دهد.

جدول ۱

قبل از آن که درمورد تعداد ATA Centerهایی که قرار است در یک شبکه نصب شوند تصمیم‌گیری کنید به دو نکته زیر دقت کنید:

• یک ATA Center منفرد می‌تواند یک جنگل اکتیودایرکتوری (Active Directory Forest) را زیر نظر بگیرد. اگر تعداد ADFها بیشتر از یک مورد است، به ازای هر مورد حداقل به یک ATA Center نیاز است.

• یک ATA Center منفرد شاید نتواند به ترافیک تمامی کنترل‌کننده‌های دامنه رسیدگی کند. در این حالت به چند ATA center نیاز است. تعداد ATA Centerها باید مطابق با ظرفیت فناوری ATA استفاده شوند.

کارکرد اصلی گیت‌وی

ATA Gateway و ATA Lightweight هر دو عملکردهای کلیدی یکسانی دارند که به شرح زیر است:

• ضبط و بازرسی ترافیک شبکه مربوط به کنترل‌کننده دامنه. در این حالت ترافیک Port Mirror برای ماژول ATA Gateway ارسال شده و ترافیک محلی کنترل‌کننده دامنه نیز توسط ATA Lightweight Gateway دریافت می‌شود.

• دریافت رخدادهای ویندوز از سرور SIEM، سرور Syslog یا کنترل‌کننده دامنه توسط Windows Event Forwarding

• بازیابی داده‌های مرتبط به کاربران و کامپیوترها از دامنه اکتیودایرکتوری

• تفکیک کردن موجودیت‌های شبکه (کاربران، گروه‌ها و کامپیوترها)

• انتقال داده‌های موردنیاز به ATA Center

• نظارت بر چند کنترل‌کننده دامنه توسط یک ATA Gateway منفرد یا نظارت بر یک کنترل‌کننده دامنه منفرد توسط یک

ATA Lightweight Gateway

ATA Gateway ترافیک شبکه و رخدادهای ویندوز را دریافت می‌کند و توسط مولفه‌های نشان داده شده در جدول 2

پردا

Network Listener	مولفه فوق ترافیک شبکه را ضبط و تحلیل می‌کند. فرآیند فوق توان پردازشی زیادی از پردازنده مرکزی دریافت می‌کند، بنابراین زمانی که قرار است از ATA Gateway یا ATA Lightweight Gateway استفاده کنید، پیش‌نیازهای سخت‌افزاری مربوطه را مطالعه کنید.
Event Listener	رخدادهای ویندوز که توسط سرور SIEM جمع‌آوری و ارسال شده را ضبط و تحلیل می‌کند.
Windows Event Log Reader	رخدادهای ویندوز که توسط مولفه کنترل‌کننده دامنه (Windows Event Log) برای ATA Gateway ارسال شده را دریافت و تحلیل می‌کند.
Network Activity Translator	ترافیک تحلیل شده را به نمونه‌های منطقی که قابل استفاده توسط مولفه NetworkActivity هستند ترجمه می‌کند.
Entity Resolver	داده‌های تجزیه شده در ارتباط با ترافیک شبکه و رخدادها را دریافت می‌کند و آن‌ها به شکلی ترجمه و تبدیل می‌کند تا بتوان با کمک گرفتن از اکتیو دایرکتوری اطلاعات هویتی و حساب کاربری را پیدا کرد. در ادامه داده‌های فوق با آدرس‌های آی‌پی پیدا شده مطابقت داده می‌شوند. مولفه فوق به شکل کارآمدی سرآیند بسته‌ها را بازرسی می‌کند تا بتواند اطلاعات مربوط به احراز هویت ماشین‌ها، ویژگی‌ها و شناسه‌های هویتی را تجزیه کند. به عبارت ساده‌تر، بسته‌های احراز هویت تجزیه شده را با داده‌های واقعی (اسامی ملموس برای مدیر شبکه) ترکیب می‌کند.
Entity Sender	داده‌های تجزیه و مطابقت داده شده را برای ATA Center ارسال می‌کند.

جدول ۲

ویژگی‌های کاربردی و کلید ATA Lightweight Gateway

• ATA Lightweight Gateway بدون نیاز به پیکربندی ارسال رخدادها قادر است رخدادها را به شکل محلی بخواند.

• همگام‌سازی کنترل‌کننده دامنه: گیت‌وی هماهنگ‌کننده دامنه مسئولیت همگام‌سازی تمامی موجودیت‌های درون یک دامنه اکتیو دایرکتوری را عهده‌دار است. عملکرد فوق مشابه با مکانیزمی است که کنترل‌کننده‌های دامنه برای همگام‌سازی اطلاعات و خط‌مشی‌ها از آن استفاده می‌کنند. یک گیت‌وی به شکل تصادفی از میان کاندیداهای موجود انتخاب می‌شود تا به عنوان همگام‌کننده دامنه استفاده شود. اگر هماهنگ‌کننده بیش از 30دقیقه آفلاین باشند، داوطلب دیگری انتخاب می‌شود. اگر ATA موفق نشود هیچ داوطلب هماهنگ‌کننده دامنه‌ای برای یک دامنه مشخص پیدا کند، خودش فعالیت‌های مربوطه به هماهنگ‌سازی را بر عهده می‌گیرد و هر زمان بخش‌های جدیدی نیازمند نظارت بودند، آن‌ها را به فهرست خودش اضافه می‌کند. در حالت پیش‌فرض تمامی ATA Gatewayها به عنوان یک داوطلب برای هماهنگ کننده دامنه شناخته می‌شوند. در محیط‌هایی که محدود به Lightweight Gateway هستند، مایکروسافت پیشنهاد می‌کند دو مورد از گیت‌وی‌ها به عنوان داوطلب هماهنگ‌سازی تعیین شوند تا یکی از آن‌ها به شکل پیش‌فرض این فرآیند را مدیریت کند و دیگری به عنوان پشتیبان برای زمانی که گزینه اصلی برای مدت بیش از 30 دقیقه آفلاین است در نظر گرفته شود.

• محدودیت منابع: ATA Lightweight Gateway مولفه‌های نظارتی قدرتمندی دارد که ظرفیت حافظه و منابع مورد استفاده کنترل‌کننده دامنه را ارزیابی می‌کنند. فرآیند فوق هر 10 ثانیه یکبار انجام می‌شود تا میزان مصرف پردازنده مرکزی و حافظه در ATA Lightweight Gateway به شکل پویا بررسی شود تا اطمینان حاصل شود کنترل‌کننده دامنه حداقل به 15 درصد از منابع دسترسی دارد. اگر مولفه فوق با کمبود منابع روبرو شود، هشدار Dropped port mirrored network traffic روی صفحه Health ظاهر می‌کند و تنها نیمی از ترافیک بررسی می‌کند. جدول 3 نمونه‌ای از یک کنترل‌کننده دامنه با منابع کافی را نشان می‌دهد.
اگر اکتیو دایرکتوری منابع زیادی را مصرف کند، منابع کمتری در اختیار ATA Lightweight Gateway قرار می‌گیرد. به‌طور مثال، در جدول 4 مشاهده می‌کنید ATA Lightweight Gateway به منابع بیشتری نیاز دارد، اما در دسترس نیست، در نتیجه تنها روی بخشی از ترافیک شبکه نظارت می‌کند.

Gateway dropping	ATA Lightweight Gateway Quota	Miscellaneous (other processes)	ATA Lightweight Gateway (Microsoft.Tri.Gateway.exe)	Active Directory (Lsass.exe)
خیر	45%	10%	20%	30%

جدول ۳

Gateway dropping	ATA Lightweight Gateway Quota	Miscellaneous (other processes)	ATA Lightweight Gateway (Microsoft.Tri.Gateway.exe)	Active Directory (Lsass.exe)
بله	15%	10%	15%	60%

جدول ۴

برای آنکه بتوانید از قابلیت‌های ATA استفاده کنید باید مطمئن شوید مولفه Port Mirroring در شبکه در حال اجرا است. اگر قرار است از ATA Gateway استفاده شود، باید قابلیت Port Mirroring برای کنترل‌کننده‌های دامنه و روی سوئیچ‌های فیزیکی یا مجازی تنظیم شود تا امکان تحلیل اطلاعات فراهم شود. گزینه دیگر در دسترس Network TAP است. با توجه به این‌که Port Mirroring انعکاسی از تمامی ترافیک کنترل‌کننده دامنه را در اختیار ATA Gateway قرار می‌دهد، تنها درصد کمی از ترافیک برای تحلیل به شکل فشرده در اختیار ATA Center قرار می‌گیرد. لازم به توضیح است که کنترل‌کننده‌های دامنه و ATA Gatewayها می‌توانند فیزیکی یا مجازی باشند. برای دانلود این نرم‌افزار و نحوه نصب آن روی ویندوز سرور به آدرس زیر مراجعه کنید:
https://docs.microsoft.com/en-us/advanced-threat-analytics/install-ata-s...

منبع:
microsoft
تاریخ انتشار:
01 خرداد 1399

نشانی منبع:
https://www.shabakeh-mag.com/security/16878/%D8%A2%D8%B4%D9%86%D8%A7%DB%8C%D9%89-%D8%A8%D8%A7-%D9%85%D8%B9%D9%85%D8%A7%D8%B1%D9%89-%D8%AA%D8%AC%D8%B2%DB%8C%D9%87-%D9%88-%D8%AA%D8%AD%D9%84%DB%8C%D9%84-%D9%BE%DB%8C%D8%B4%D8%B1%D9%81%D8%AA%D9%87-%D8%AA%D9%87%D8%AF%DB%8C%D8%AF%D8%A7%D8%AA-ata