پائیز ۱۳۹۹

مستند امنیت در سیستم های مقیاس بزرگ
(مین فریم)
اندیشه نگار پارس

مقدمه

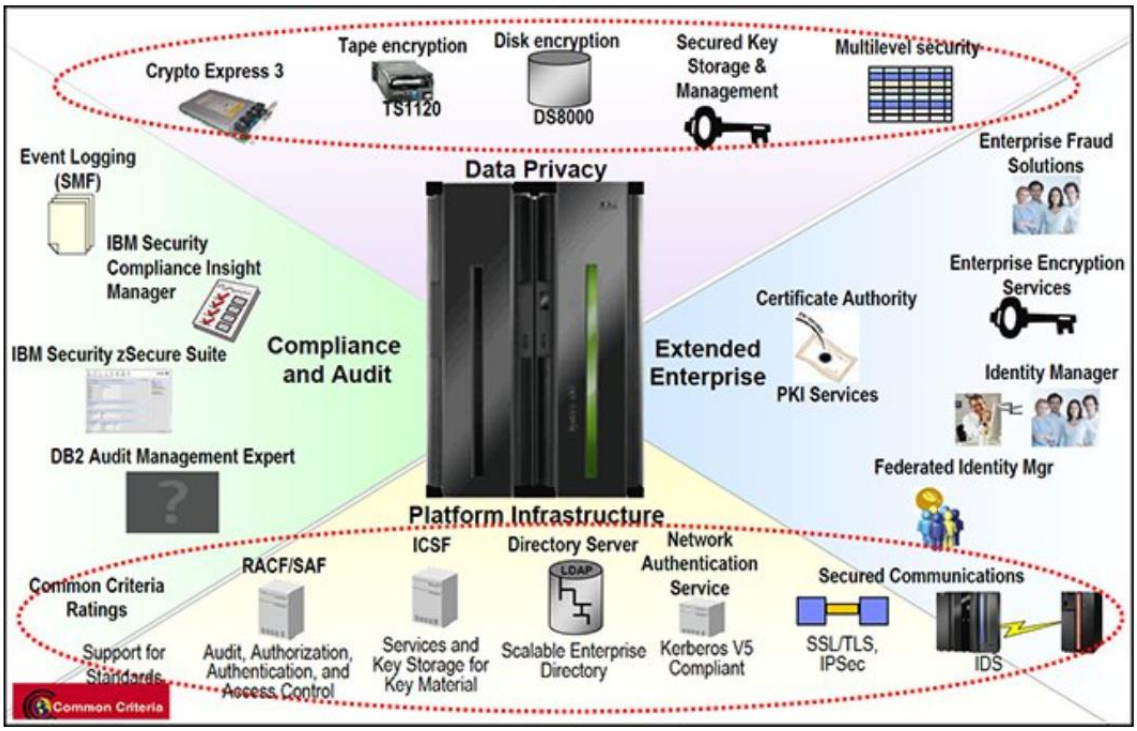
مستند پیش رو شرح مختصری از استقرار امنیت (امن سازی) ماشینهای مقیاس بزرگ IBM (مین فریم – Mainframe) میباشد.

این امن سازی در لایه های متفاوت سخت افزار و نرم افزار قابل پیاده سازی است. از این روست که مین فریمها عمدتا به عنوان امن ترین ماشینهای کامپیوتری در دنیا شناخته میشوند.

امن سازی در مین فریمهای IBM

مبحث امن سازی در مین فریم بسیار متفاوت از آن چیزی است که احتمالا در سیستمهای سرور مبتنی بر لینوکس با ویندوز دیده باشید. پیچیدگیهای این نوع ماشینهای سخت افزاری و نرم افزارهای مبتنی بر آن باعث شده است که از ابتدای ظهور کامپیوتر در زندگی انسان تا کنون، مین فریمها به عنوان یک ساختار تقریبا غیر قابل نفوذ همواره مطرح باشند.

یک نمای کلی از موارد با قابلیت امن سازی را در شکل زیر مشاهده مینمایید:



همانطور که در شکل بالا مشاهده مینمایید، امنیت در لایه های سخت افزاری اعم از کارت رمز نگاری سخت افزاری، امن سازی نوارگردان ها ، امن سازی دستگاههای ذخیره سازو ... در لایه شبکه امن سازی مسیر مکالمه بین مین فریم و ماشینهای دیگر ، امن سازی دسترسی در شبکه ، استفاده از پروتکهای امن رد و بدل کردن پیام و رمز نگاری پیامها درون بستر شبکه و ... در لایه سیستم عامل و نرم افزاری، استفاده از لایه

امنیتی مبتنی بر سیستم عامل و امن سازیهای اختصاصی هر لایه نرم افزاری اعم از امن سازی پایگاه داده، تولید کلید امن ، سیستم کشف تقلب و ... پیاده سازی میشود.

نکات قابل توجه

عمدتا سیستم عامل z/OS که بر روی ماشینهای مین فریم سری Z نصب میگردد، به عنوان امن ترین سیستم عامل عملیاتی شناخته میشود.از این رو بزرگترین سیستمهای تجاری/ مالی دنیا بر روی مین فریم و سیستم عامل z/OS قرار دارند. سیستم Z امنیت را در لایه میکروکدهای سخت افزاری پیاده سازی میکند، این مدل از پیاده سازی باعث میشود که ماشینهای System Z در برابر هک شدن مقاوم ترین باشند. از این رو سیستم هایی که مبتنی بر سیتسم عامل Z هستند غیرقابل نفوذ به حساب میآیند.

سیستم عامل z/OS ، یکپارچگی سیستم را ضمانت میکند. این مطلب در بیانیه صداقت MVS در سال ۱۹۷۳ تاکید شده است. این بیانیه را میتوانید در آدرس زیر مشاهده نمایید:

http://www.ibm.com/systems/z/os/zos/features/racf/zos_integrity_statement.html

ارزش تجاری

هک کردن تنها بخشی از فرآیند برای دستیابی به داده های سازمانی با قصد مخرب است. در صورت دسترسی به یک بخش از یک محیط فناوری، اطلاعات سازمانی بدست می آید ، سپس می توان از این دسترسی برای گسترش دسترسی به دیگری استفاده کرد.

نقض اولیه کنترل های امنیتی برای ایجاد یا بدست آوردن یک نقض دیگر استفاده می شود. و نتیجه این عملیات مخرب معمولاً داده ها هستند.

این حملات معمولاً بر روی نرم افزارهای مبتنی بر لینوکس ، یونیکس یا ویندوز اجرا می شوند. هدف در بسیاری از این حملات دستیابی داده هایی است که در قسمت اصلی نگهداری می شوند.

بر روی System z و سیستم عامل z/OS برای امن سازی باید به موارد زیر توجه کرد:

- مدیریت هویت
- مدیریت دسترسی به منابع و داده ها
- مدیریت لاگ
- هوشمند سازی امنیت و تحلیلهای آماری
- مدیریت امن سازی برنامه های کاربردی
- مدیریت روالها و پردازشها
- مدیریت امن سازی فیزیکی و شبکه ای

در عکس زیر لایه های امن سازی مین فریم را مشاهده میفرمایید:


Governance, Risk and Compliance
Security Intelligence and Analytics
Advanced Fraud Protection
People
Data
Applications
Infrastructure
Advanced Security and Threat Research

راهکارهای کاربردی

اکثر سازمانها سیاستهای امن سازی را در لایه داده ها و دسترسی به آنها تعیین میکنند. این امن سازی در لایه دسترسی حداقلی به کاربران و نقشهای کاربردی وجود دارد.

طی سالها ، IBM قابلیت ها و کنترل های جدید امنیتی را معرفی کرده است. با این حال ، بسیاری از سازمان ها تصمیم گرفته اند بسیاری از این کنترل ها را بر اساس ارزیابی تهدید امنیتی عملی نکنند. زیرساخت های امن با برنامه های ایمن صرفا اتفاق نمی افتند. هر کدام جداگانه باید طراحی شود ، پس از آن طرح را پیاده سازی کرده و در هر فرآیند کیفیت ، پیشرفت مداوم داده شوند. این موضوع برای مدیریت امنیت نیز باید در نظر گرفته شود ، و بطور کلی باید برای هر فرآیند دیگر نیز در نظر گرفته شود.

کنترل های امنیتی از نظر نوع متفاوت هستند. برخی از کنترل ها برای اعطای یا جلوگیری از اقدامات افراد در این زمینه طراحی شده اند. اشیاء و سایر کنترلها ممکن است عملکردهای رخ داده را رصد کرده و سپس آنها را ضبط کنند. برخی از کنترل ها ممکن است هشدار تولید کنند. کنترل های پیشگیرانه مانع از دسترسی غیرمجاز می شوند .

یک مدیر پیشرفته امنیت (ESM) مانند RACF دسترسی به یک منبع برای یک کاربر خاص را سلب/مجاز می کند. دسترسی اعطا شده توسط ESM ها ، مانند RACF ، تنظیماتی را ارائه می دهند که می تواند سطح امنیت را تعیین کند

دسترسی ها باید کنترل شود. هر زمان که تغییر غیرمجاز توسط کاربر یا یک فرآیند ایجاد شود ، یک هشدار می تواند توسط یک کارآگاه کنترل شود. پس از یک رویداد برای تعیین علت اصلی ترکیبی از همه این نوع کنترل ها همیشه توصیه می شود.

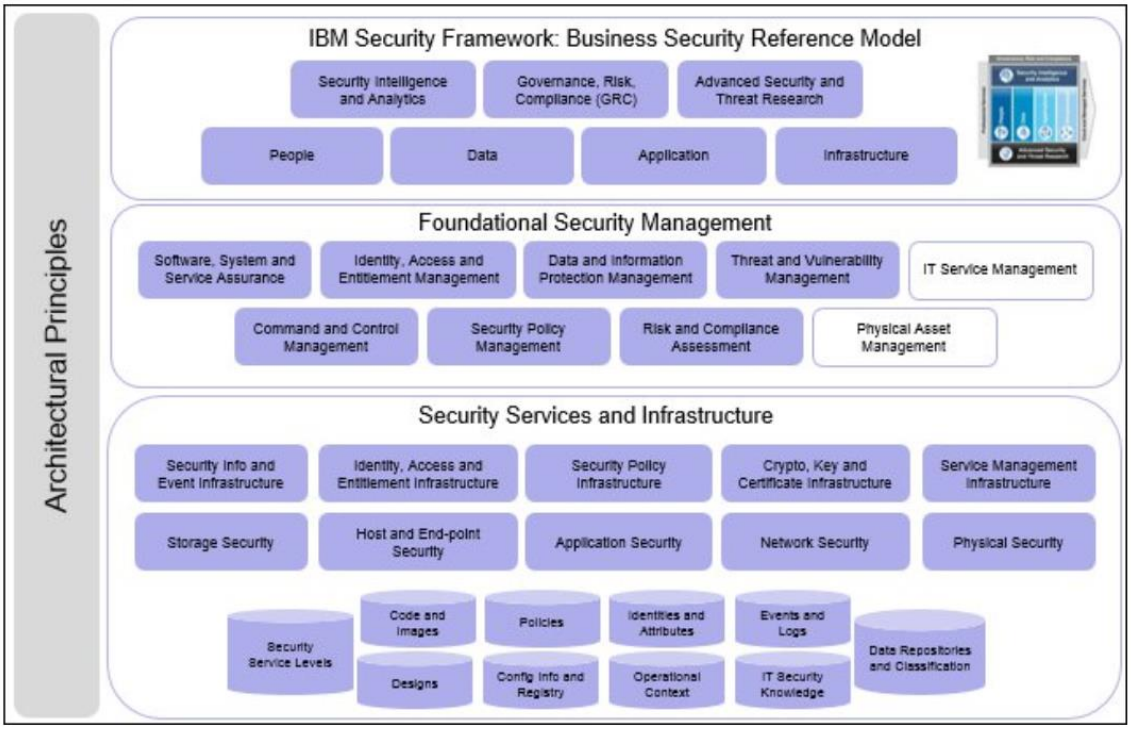
اخیراً ، راه حل های بسیاری در دسترس است که می تواند به اجرای امنیت در سیستمهای IBM Z کمک کند.

امنیت ، اطلاعات امنیتی و تجزیه و تحلیل ، سیاست ها و فرآیندها ، ممیزی و انطباق ، برنامه ها، مدیریت دسترسی و امتیازات ، کشف و پیشگیری از کلاهبرداری ، مدیریت هویت و محافظت از شبکه ، این محصولات یا خدمات امنیتی داخلی را تکمیل کرده یا آنها را تشکیل می دهند.

در اینجا لیستی از این راه حل های امنیتی IBM آورده شده است:

- **IBM InfoSphere Guardium for z/OS**
- **IBM Security QRadar**
- **IBM Security zSecure Suite**
- **IBM Security Key Lifecycle Manager**
- **IBM Enterprise Key Management Foundation**
- **IBM Encryption Facility for z/OS**
- **IBM Security AppScan**
- **IBM Security Access Manager**
- **IBM Security Trusteer**
- **IBM Security Identity Manager**
- **IBM Security Federated Identity Manager**
- **IBM Security Network Protection**

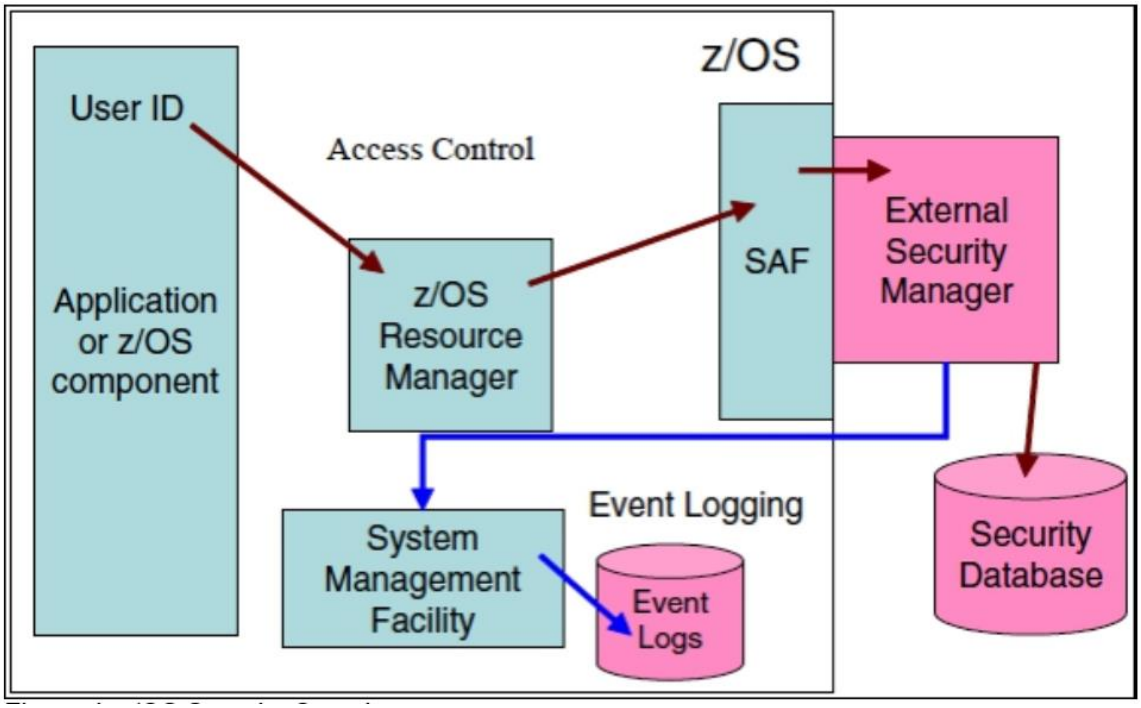
معماری لایه های امنیتی



شکل بالا طرح امنیتی IBM را به روش معماری سرویس گرا (SOA) نشان میدهد.

ویژگیهای امنیتی در مین فریم ها به شدت به سخت افزار و حتی هر تراشه یک پردازنده وابسته است. این مدل از طراحی امنیتی تا لایه HyperVisor و برنامه های کاربردی نیز گسترش پیدا میکند. این امن سازی حتی در سطح فرآیندها نیز پیاده میشوند. این حالت از پیاده سازی امنیتی باعث یکپارچگی در سطح امنیتی مین فریم میشوند.

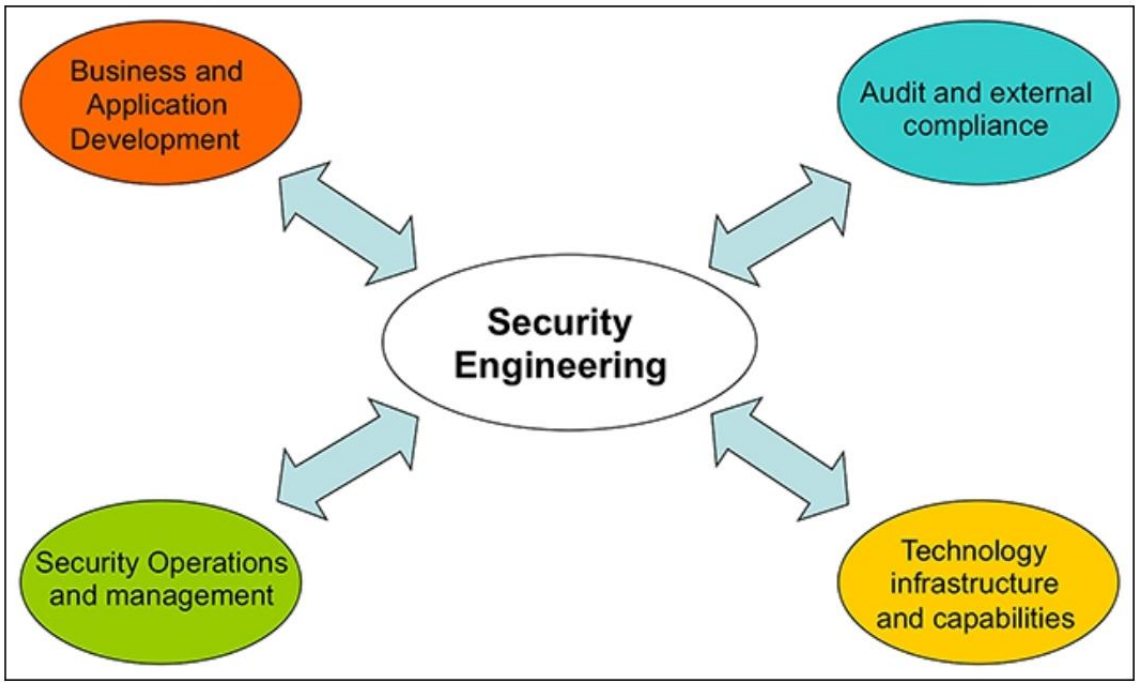
امنیت در سیستم عامل به شکل زیر پیاده سازی میشود:



ESM ماژول خارجی برقراری امنیت در z/OS است . به همین ترتیب RACF در برقراری امنیت داخلی در محیط سیستم عامل عمل میکند.
RACF به عنوان یک زیر سیستم درون سیستم عامل با کارکردهای زیر به امن سازی محیط کمک میکند:

- کنترل منعطف بر روی دسترسی منابع حفاظت شده
- حفاظت از نرم افزارهای نصب شدنی بر روی سیتم عامل
- توانایی ذخیره سازی اطلاعات امنیتی مربوط به هر نرم افزار به صورت جداگانه
- انتخاب بین کنترل متمرکز یا غیر متمرکز بر روی پروفایلهای سیستم
- رابط کاربری ساده و شفاف از نظر کاربران (کاربران قادر به دیدن اطلاعات داخلی آن نیستند)
- گزینه های بومی سازی برای تطابق با بیانیه های امنیتی

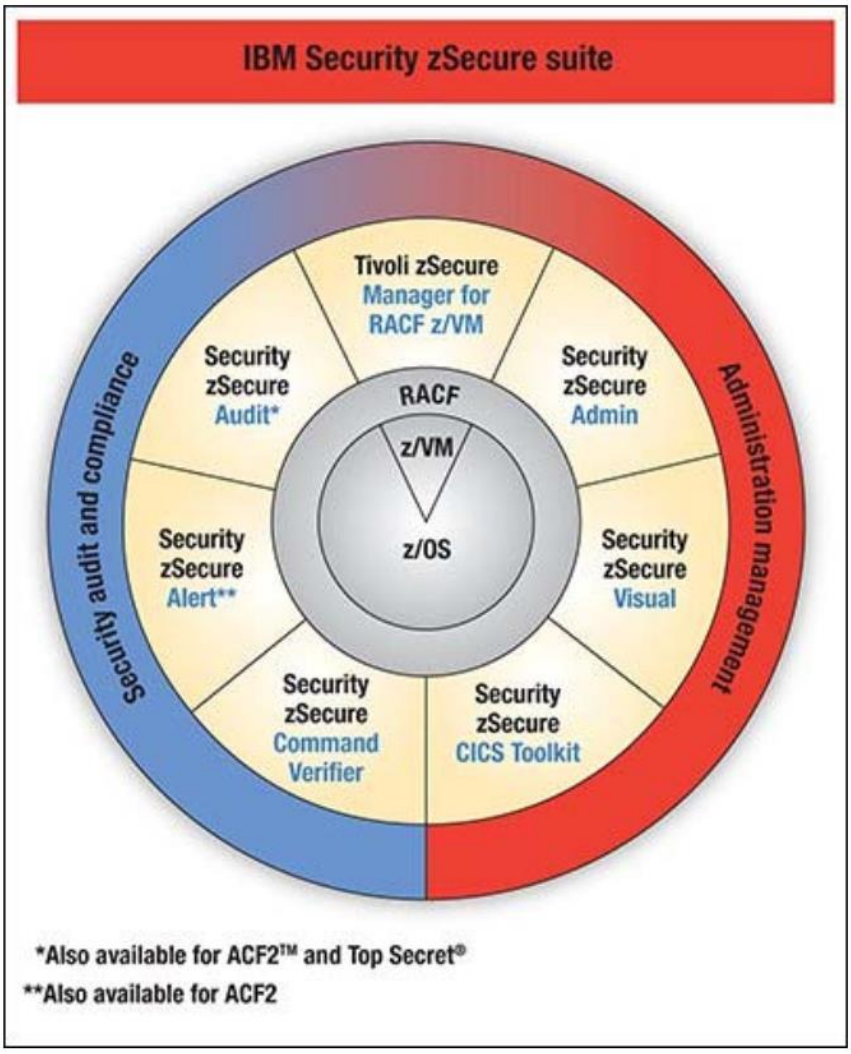
مهندسی امنیت



مهندسی امنیت در سیستمهای مین فریم IBM از چهار منظر قابل پیاده سازی است. همانطور که در شکل بالا مشتهده مینمایید این مهندسی شامل چهار وجه است:

- توسعه برنامه های کاربردی و تجاری
- مدیریت عملیات امن سازی
- زیرساخت تکنولوژی و توانمندیهای آن
- بازرسی و انطباق خارجی

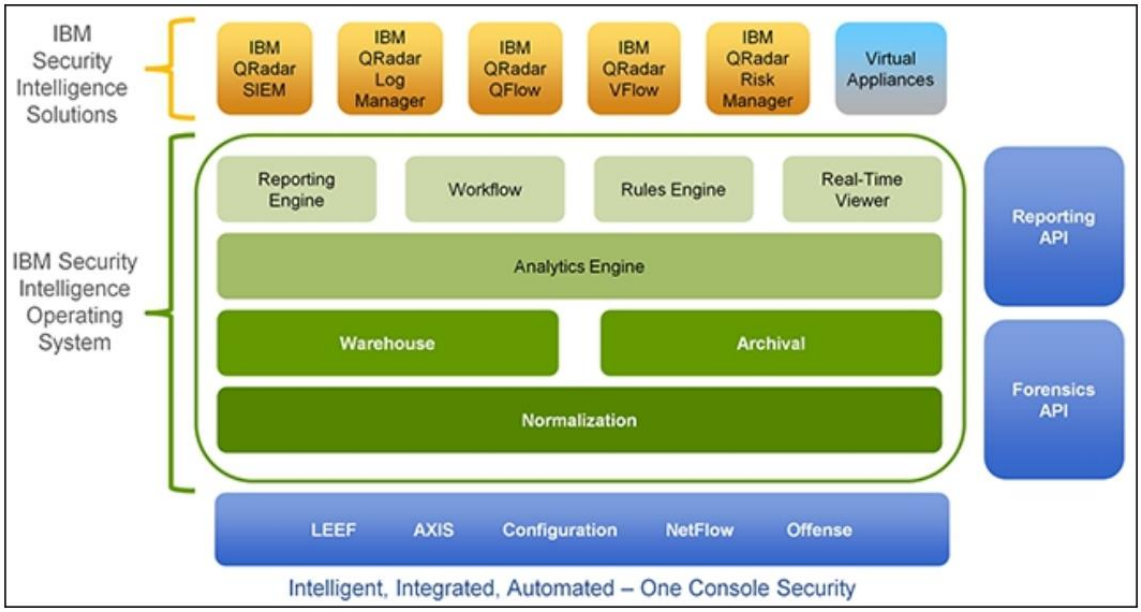
معرفی IBM Security zSecure Suit



در این ابزار که در شکل بالا مشاهده میکنید نحوه امن سازی در لایه سیستم عامل و زیر سیستمهای مربوط به آن را مشاهده میفرمایید:

- نقطه اصلی خود سیستم عامل z/OS است
- لایه سیستم عامل z/VM (سیستم عامل مرتبط با مجازی سازی بر روی محیط مین فریم) تحت پوشش امنیتی ماشین و سیستم عامل قرار میگیرد.
- RACF لایه نرم افزاری است که مسئولیت امن سازی در سطح دسترسی ها ، سیستم عامل و برنامه های کاربردی و زیر سیستم های اصلی نصب شده روی محیط مین فریم، را بر عهده دارد.

معرفی اجمالی خانواده امن سازی IBM



در ابتدای این مستند به نرم افزارهایی که در امن سازی مین فریم کابرد دارند اشاره شد. در اینجا طرح معماری از نحوه استفاده از این نرم افزارها را به شکل نمایشی مشاهده میفرمایید.

پیاده سازی امنیت در ماشینهای مین فریم سیستم Z و بر روی پلتفرمهای زیر قابل اجراست:

- **IBM System z**
- **IBM z/OS**
- **IBM z/VM**
- **Linux on System z**

منابع

IBM Redbooks: Security on the IBM Mainframe: Volume 1- A Holistic Approach to Reduce Risk and Improve Security, SG24-7803
http://www.redbooks.ibm.com/abstracts/sg247803.html

System z product page
http://www.ibm.com/systems/z/

System z Security solutions page
http://www.ibm.com/systems/z/solutions/security.html

z/OS product page
http://www.ibm.com/systems/z/os/zos/

z/VM product page
http://www.vm.ibm.com/

Linux on z product page

http://www.ibm.com/systems/z/os/linux/