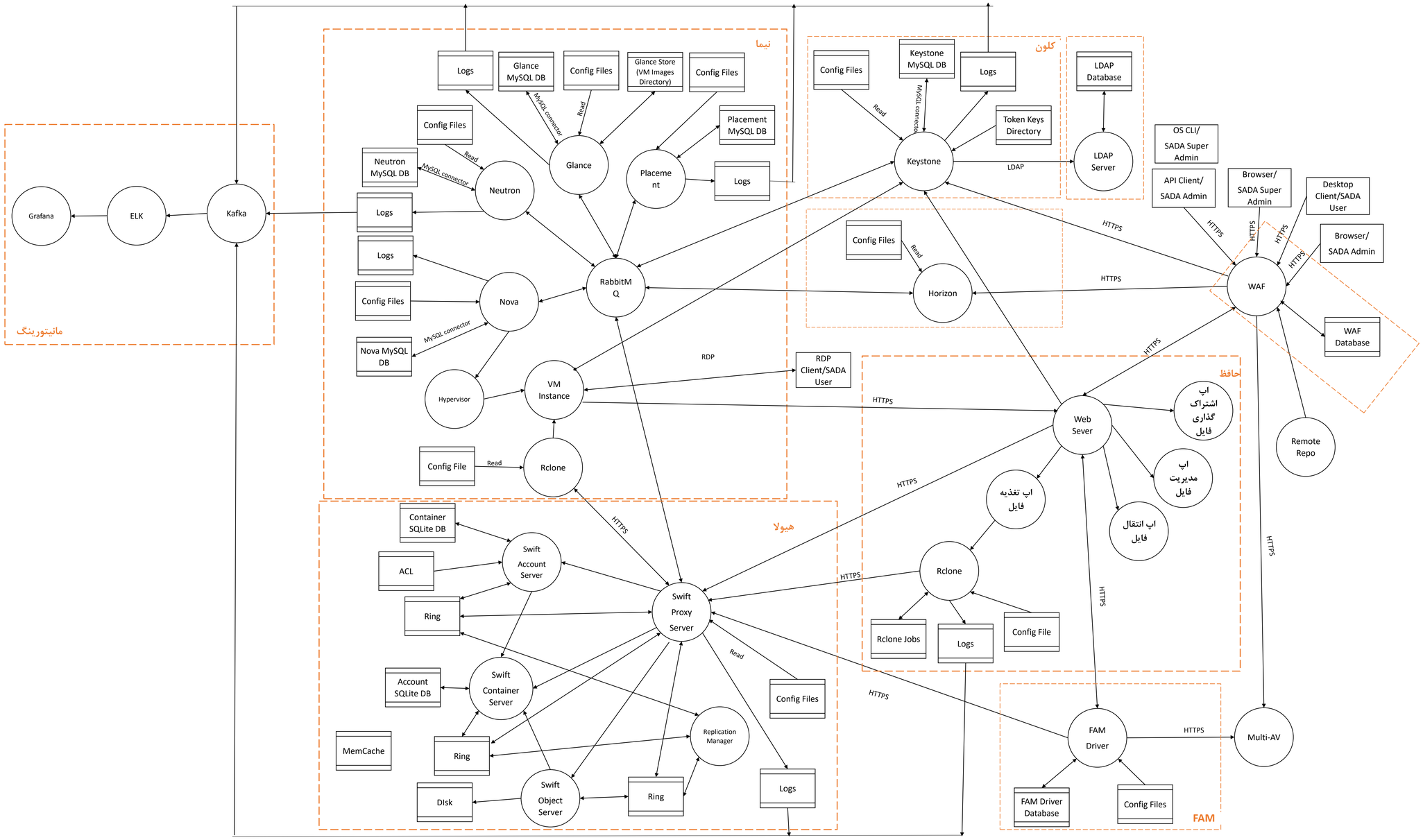
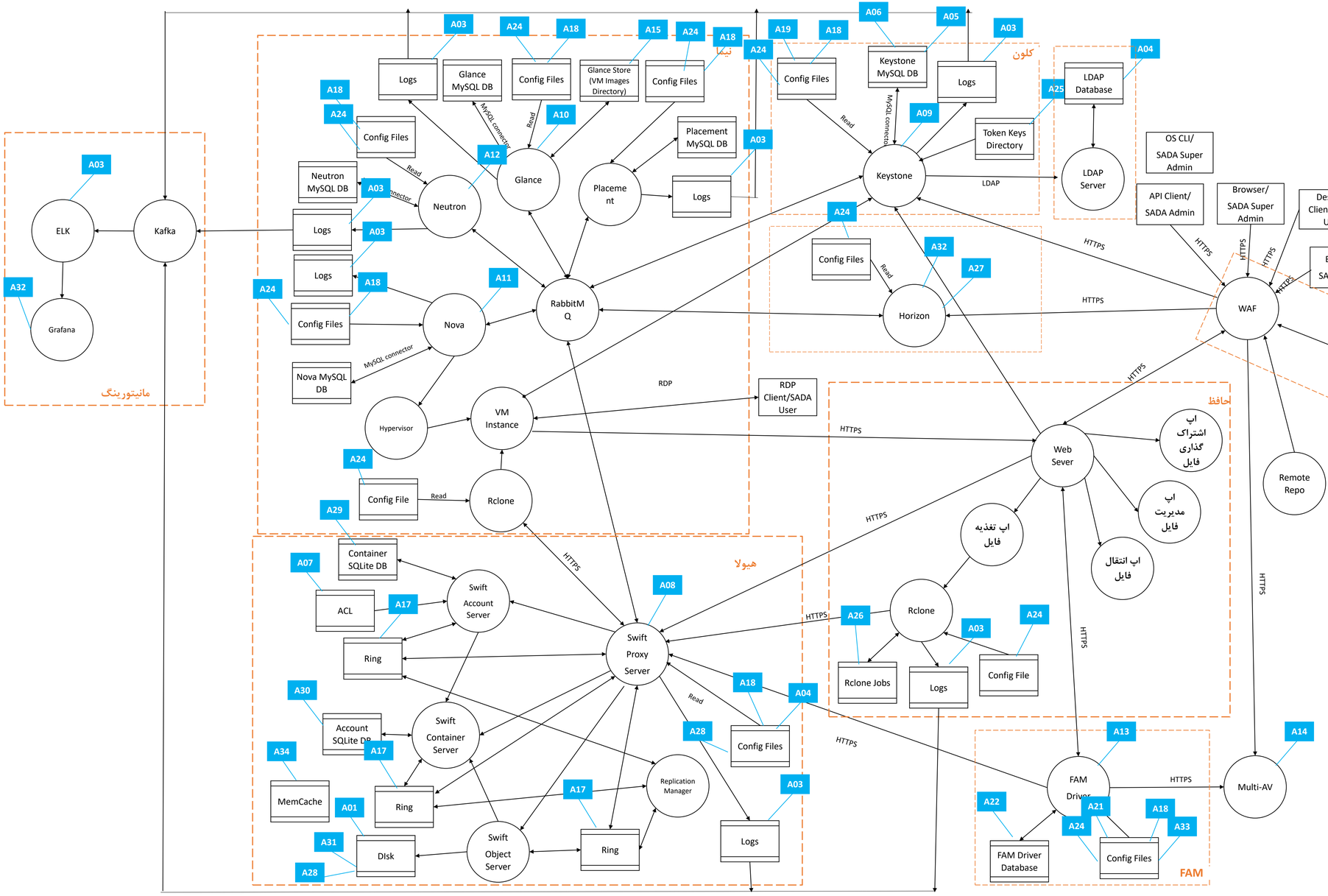
مدل تهدید سیستم سادا

شرکت برنا

۱۵ مرداد ۱۴۰۲

System Model





دارایی‌های اطلاعاتی حیاتی سیستم (داده‌ها و عملکردها)

A01: داده‌های ذخیره‌شده در objectها

A02: توکن‌های احرازهویت (Fernet)

A03: لاگ‌ها

A04 : فهرست همه کاربران اعم از کاربران بهره‌بردار، مدیران و مدیران ارشد سادا

A05: فهرست کاربران مدیران ارشد سادا (برای کار با ACL کی استون)

A06: فهرست مشخصات کاربران سادا شامل ویژگی‌های امنیتی آنها اعم از نام کاربری، پسورد (برای مدیران ارشد سادا)، نقشها، گروه‌ها، دامنه‌ها، پروژه‌ها، وضعیت فعال و غیرفعال بودن

A07: ACLهای تنظیم شده برای Containerها که به صورت متادیتا برای Containerها در نظر گرفته می‌شوند.

A08: APIهای Swift Proxy

A09: APIهای Keystone

A10: APIهای Glance

A11: APIهای Nova

A12: APIهای Neutron

A13: APIهای FAM Driver

A14: APIهای Multi-AV

A15: Imageهای VMها

A16: اطلاعات مرتبط با imageها شامل مشخصات آنها، ویژگی‌های آنها و محل قرارگیری آنها

A17: Ringها شامل آدرس بهترین محل قرارگیری objectها در سرورهای مختلف

A18: اطلاعات کاربری (Credential)ها سرویس‌ها برای دسترسی به دیتابیس‌ها

A19: اطلاعات کاربری دسترسی Keystone به LDAP

A20: اطلاعات کاربری دسترسی حافظ به FAM driver

A21: اطلاعات کاربری دسترسی FAM Driver به Multi-AV

A22: نتایج اسکن Multi-AV بر روی فایلها که به کمک تگ مشخص می‌شود.

A23: نمونه‌های Image (VM)ها

A24: پارامترهای پیکربندی مختلف مورد استفاده سرویس‌ها

A25:کلیدهای رمزنگاری مورداستفاده در Fernet

A26: درخواست‌های انتقال فایل در قالب jobها

A27: قابلیت‌های داشبورد Horizon

A28: کلیدهای مورداستفاده برای رمزنگاری objectها

A29: آدرس قرارگیری objectها در containerها

A30: تعداد objectهای موجود در containerهای مربوطه

A31: متادیتای objectها

A32: انواع گزارش‌ها

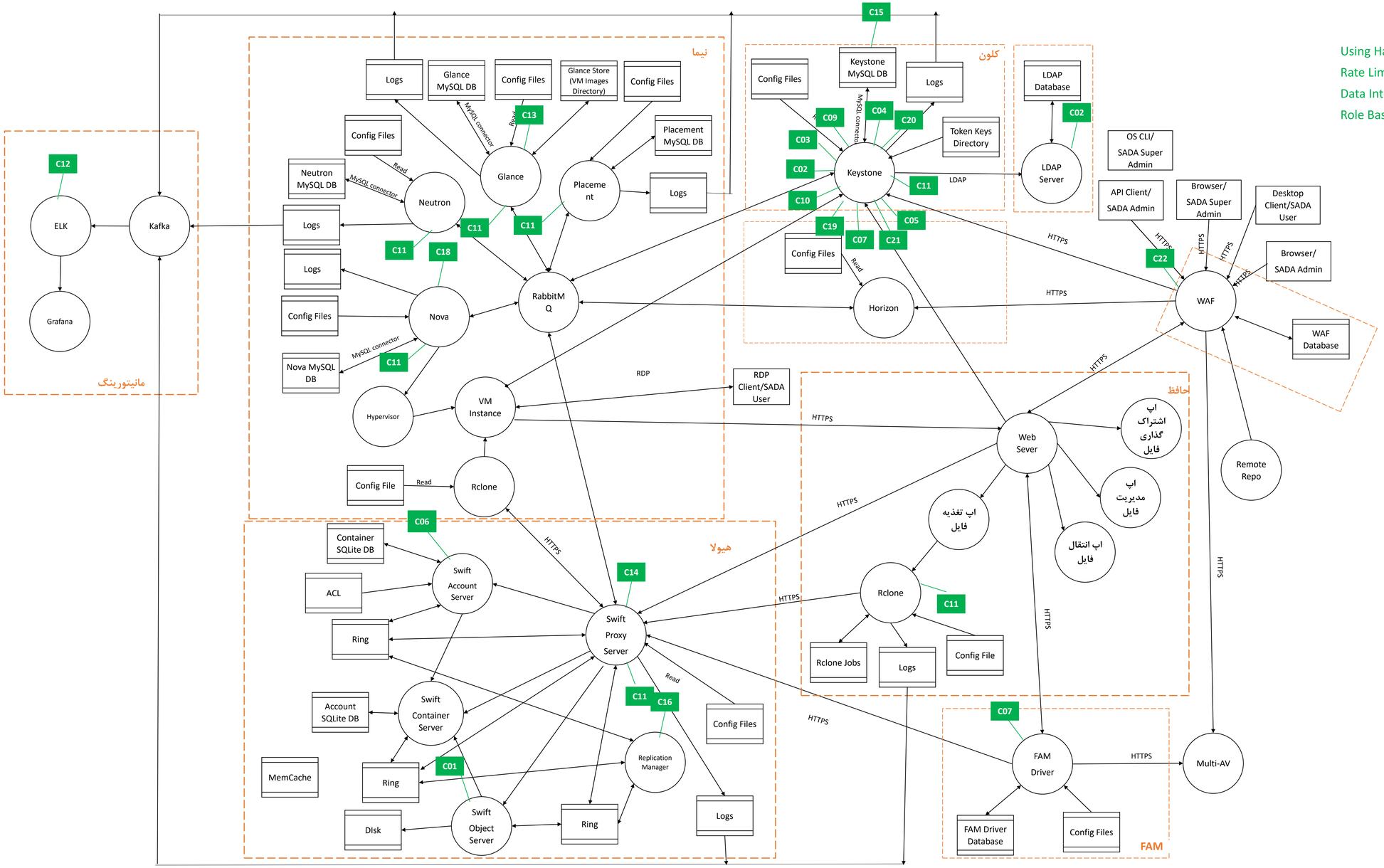
A33: پارامترهای Risk Score و دیگر پارامترهای تعیین شده سازمان برای اسکن فایلها

A34: اطلاعات موقت موردنیاز در پردازشهای انجام شده در سرویسها

A35: قوانین فایروالی

A36:snapshotهای ماشین مجازی

A37: حافظه



کنترل‌های امنیتی

Using Hash for Ring

Rate Limiting

Data Integrity Check

Role Based File Extension Validation

C01: رمزنگاری داده‌های ذخیره شده در Objectها

C02: احرازهویت کاربران

C03: استفاده از توکن‌های Fernet که اطلاعات هویتی را به صورت رمزنگاری شده نگهداری می‌کنند.

C04:کنترل دسترسی کاربران به سامانه ذخیره‌سازی هیولا برمبنای نقش آنها در دامنه، پروژه و گروه مربوطه

C05:کنترل دسترسی کاربران به قابلیتهای مختلف داشبورد Horizon

C06:کنترل دسترسی کاربران به Containerها برمبنای Account ACL

C07: کنترل دسترسی به کیسه‌های حساب متمرکز در حافظ برمبنای نقش کاربر

C08: اسکن فایل‌ها قبل از انتقال به هیولای مطمئن

C09: مدیریت مدت زمان اعتبار توکن‌ها

C10: پیکربندی‌هایی همانند تعیین و مدیریت پالیسی‌های مربوط به پسوردها (طول عمر پسورد، پیچیدگی پسورد، تکراری نبودن پسورد و غیره) حداکثر تعداد تلاشهای موفق برای لاگین ناموفق، قفل کردن حساب کاربری به دلیل لاگینهای ناموفق متوالی، حداکثر مدت زمان قفل ماندن حساب کاربری،الزام کاربر به تغییر گذرواژه در اولین ورود (البته برای حالت بدون LDAP)

C11: رویدادنگاری (logging)

C12: نظارت و پایش (monitoring) ماشین‌های مجازی شامل بررسی وضعیت مصرف منابع رایانشی و شبکه‌ای

C13: اعتبارسنجی imageها هنگام آپلود شامل بررسی اندازه image و تعداد کل imageهای قابل آپلود و اعتبارسنجی متادیتای imageها براساس مقادیر قابل قبول

C14: اعتبارسنجی داده‌ها هنگام آپلود در هیولا

C15: ذخیره سازی پسوردها به صورت Hash شده

C16: طراحی HA (Replication) داده‌ها در هیولا)

C17: استفاده از TLS/SSL

C18: سهمیه‌بندی منابع رایانشی و شبکه‌ای برای دامنه‌ها و پروژه‌ها

C19: نامگذاری امن پروژه‌ها

C20: مدیریت کلیدهای رمزنگاری مورداستفاده برای Fernet مثلا محل ذخیره‌سازی آنها

C21: کنترل دسترسی کاربران به اپ‌های حافظ برمبنای نقش آنها

C22: فایروالینگ

عاملین تهدید (Threat Agents)

TA1: کاربر بهره‌بردار سادا (SADA User)
TA2: کاربر مدیر سادا (SADA Admin)
TA3: کاربر مدیر ارشد سادا (SADA Super Admin یا همان Sys Admin)
TA4: توسعه دهنده سادا (SADA Developer)
TA5: پیمانکار Mult-AV
TA6: سرویس‌های دیگر
TA7: مهاجمین داخلی