

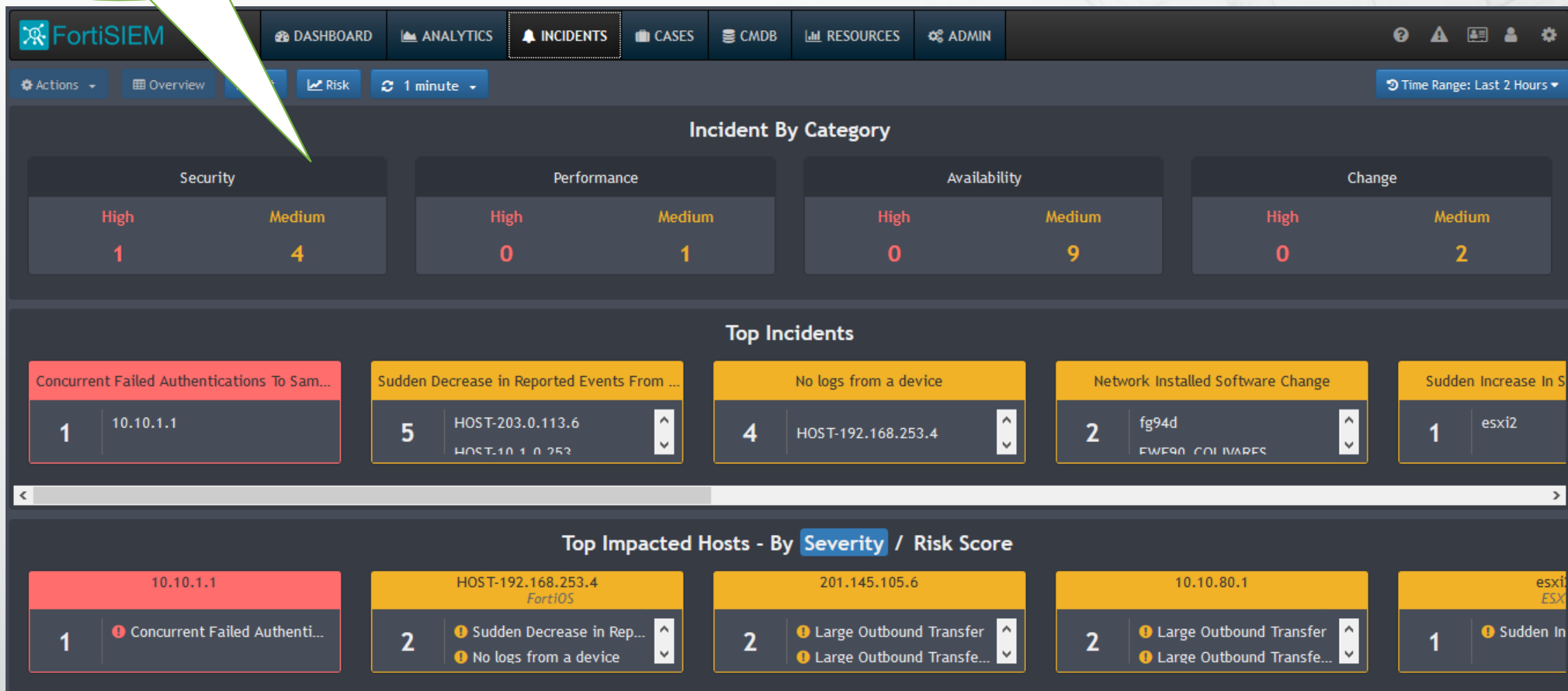
FortiSIEM

Ejemplo de Interfaz de Usuario



Se muestran los incidentes mas recientes, así como los mas críticos e histórico de eventos por categoría.

Dashboard de incidentes de las últimas 2 hrs.



Incidentes de seguridad de nivel medio



FortiSIEM

DASHBOARDANALYTICSINCIDENTSCASESCMDBRESOURCESADMIN

ActionsOverviewListRisk1 minute

1/14

Security Incidents: HIGH: 1MEDIUM: 4LOW: 0

	Last Occurred	Incident	Reporting	Source	Target	Detail
🔔	Aug 18 2018, 12:33:00 PM	End User DNS Queries to Unauthorized DNS Servers	fg94d	192.168.1.65		Triggered Event Count: 13
🔔	Aug 18 2018, 12:12:30 PM	Large Outbound Transfer	Penthouse	10.10.80.1	🇮🇹 201.145.105.6	Sent Bytes: 52.41 MB
🔔	Aug 18 2018, 12:12:30 PM	Large Outbound Transfer To Outside My Country	Penthouse	10.10.80.1	🇮🇹 201.145.105.6	Sent Bytes: 52.41 MB
🔔	Aug 18 2018, 11:56:30 AM	Sudden Increase in Successful Logons To A Host	Penthouse		Penthouse 10.10.10.1	Count: 13 Avg Matched Events: 8.52

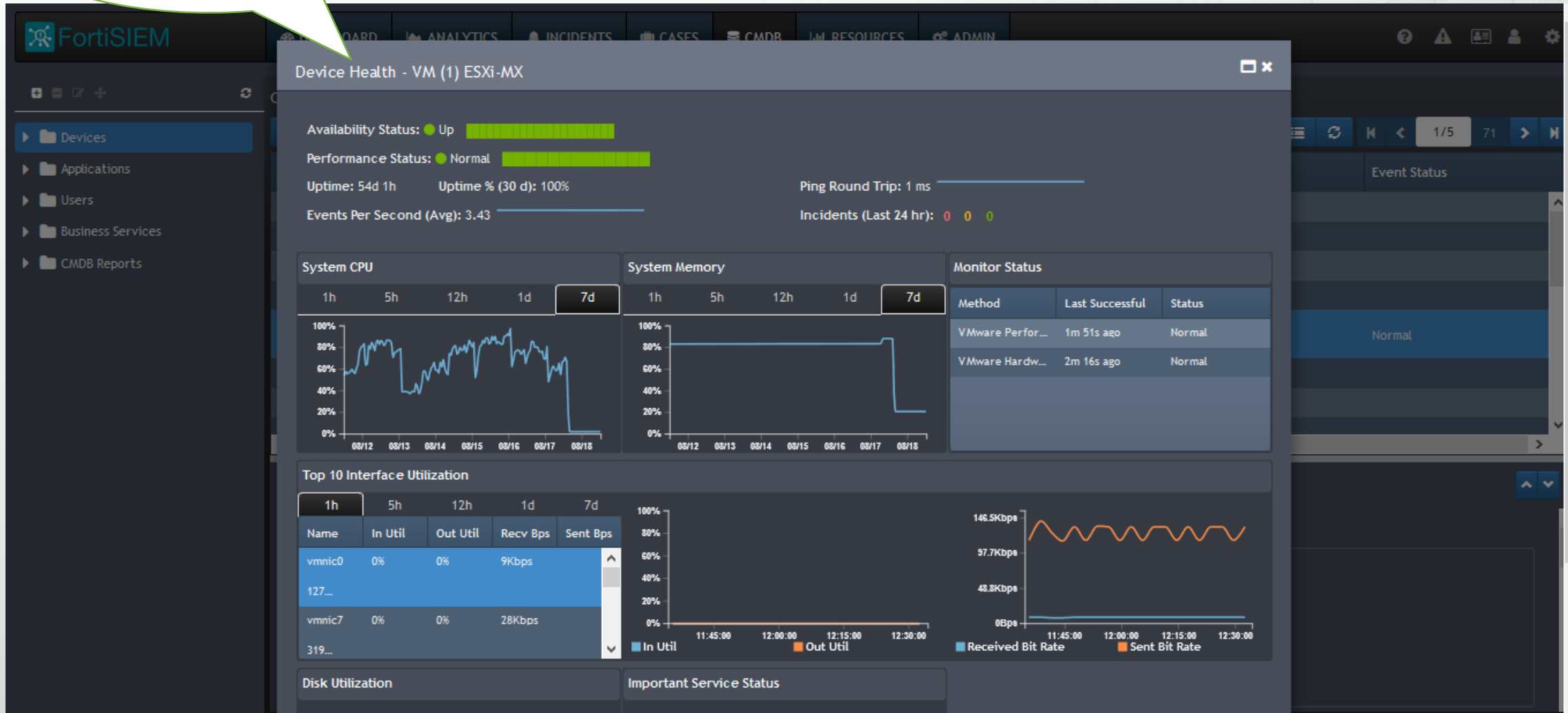
DetailsEventsRuleAuto expand

Los eventos se categorizan, dependiendo del nivel de importancia previamente asignado, se muestran por orden de aparición



Es posible realizar diagnóstico y monitoreo de equipos en tiempo real

Salud de un dispositivo



Monitoreo de redes con generación de eventos con estampa de tiempo y descripción del origen.

Detalle de un incidente



FortiSIEM

DASHBOARD ANALYTICS INCIDENTS CASES CMDB RESOURCES ADMIN

Actions Overview List Risk 1 minute

Incident Concurrent Failed Authentications To Same Account From Multiple Countries for 10.10.1.1 for Last 2 Hours

Last Occurred	Incident	Reporting	Source	Target	Detail
Aug 18 2018, 12:02:00 PM	Concurrent Failed Authentications To Same Account From Multiple Countries	fg94d		fg94d 10.10.1.1 User: root	

Details Events Rule Subpattern: MultiCountryLogon Auto expand

Event Receive Time	Event Type	Event Name	Source Country	Source IP	User	Reporting Device	Reporting IP	Win Logon Type	Raw Event Log
Aug 18, 2018 12:01:39 PM	FortiGate-event-login-f...	Failed admin logon	Taiwan	220.133.209.1	root	fg94d	10.10.1.1		<9>date=2018-08-18 time=12:01:39 devname="fg94d" devid="FG94DP...
Aug 18, 2018 11:44:32 AM	FortiGate-event-login-f...	Failed admin logon	Korea, Republic of	218.38.121.17	root	fg94d	10.10.1.1		<9>date=2018-08-18 time=11:44:31 devname="fg94d" devid="FG94DP...