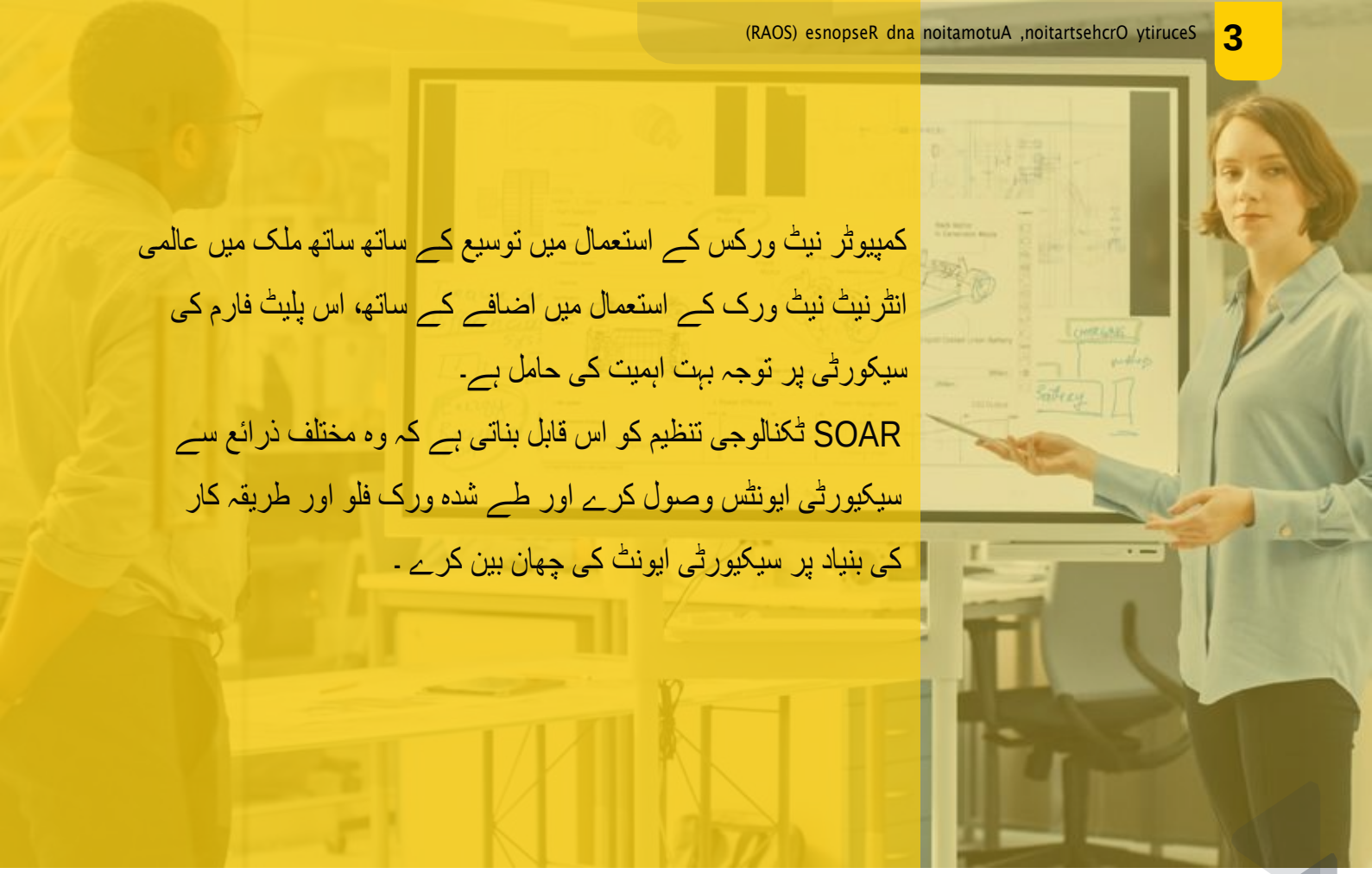
The Complete Guide to
گارڈین سائبر ایونٹ مینجمنٹ سسٹم

کی طرف سے

اندیشہ پردازان گویا نظام

9131046856 (98+)

گارڈین سائبر ایونٹ مینجمنٹ سسٹم



کمپیوٹر نیٹ ورکس کے استعمال میں توسیع کے ساتھ ساتھ ملک میں عالمی انٹرنیٹ نیٹ ورک کے استعمال میں اضافے کے ساتھ، اس پلیٹ فارم کی سیکورٹی پر توجہ بہت اہمیت کی حامل ہے۔

SOAR ٹکنالوجی تنظیم کو اس قابل بناتی ہے کہ وہ مختلف ذرائع سے سیکیورٹی ایونٹس وصول کرے اور طے شدہ ورک فلو اور طریقہ کار کی بنیاد پر سیکیورٹی ایونٹ کی چھان بین کرے ۔

کیوں سوار

SOAR ٹیکنالوجی کی ضرورت کی وجوہات یہ ہیں:

1. معائنے کی فیس میں اضافہ سیکیورٹی کے واقعات
2. بار بار کام کرنا
3. محدود تجزیہ کی طاقت
4. حفاظتی جائزہ کے عمل کا انتظام
5. انسانی وسائل پر انحصار کو کم کرنا

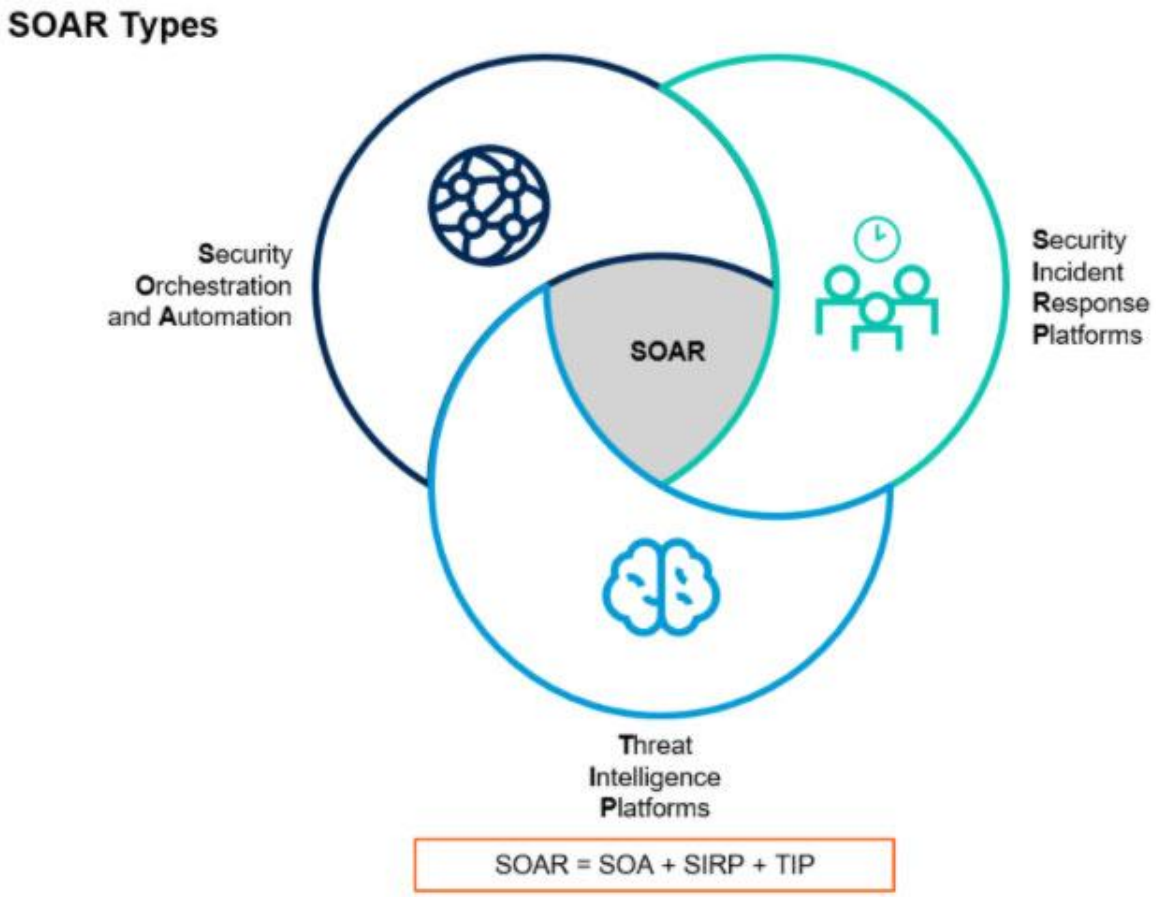
فائدہ استعمال کریں۔ سے سوار

کے جواب کو مضبوط اور بہتر بنائیں خطرے کی انٹیلی جنس کے ساتھ واقعات	فعال درستگی حفاظتی انتباہات
کارکردگی میں اضافہ معیار کے ساتھ خودکار	انتظام کو بہتر بنائیں سیکیورٹی آپریشن سینٹر یا ایس او سی معیاری عمل کے ساتھ

SOAR ماڈیولز

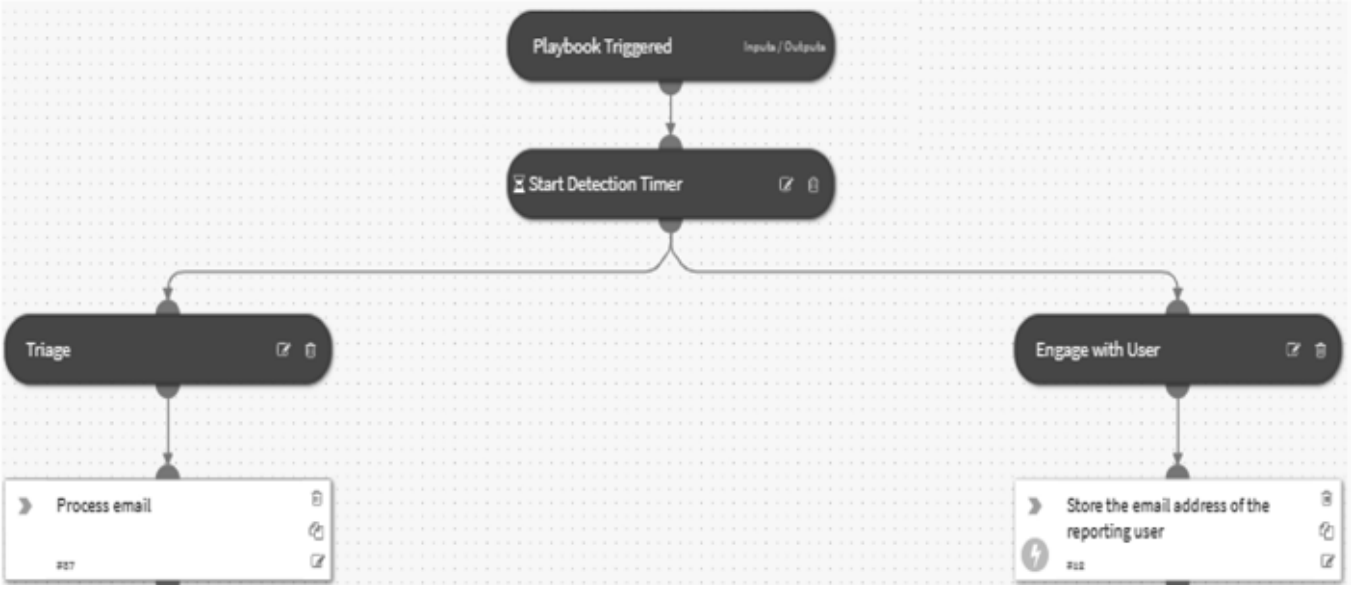
نامکمل معلومات کی تکمیل جمع	ڈیٹا اکٹھا کرنا نیٹ ورک پر مختلف ذرائع سے
اقدامات کریں۔ واقعہ کا جائزہ کا استعمال کرتے ہوئے عمل دستی	دوسرے سیکورٹی ذرائع سے کنکشن واقعات کو چیک کرنے کے لیے
واقعات کا جواب دیں۔ دستی اور خود بخود	

SOAR کا جائزہ



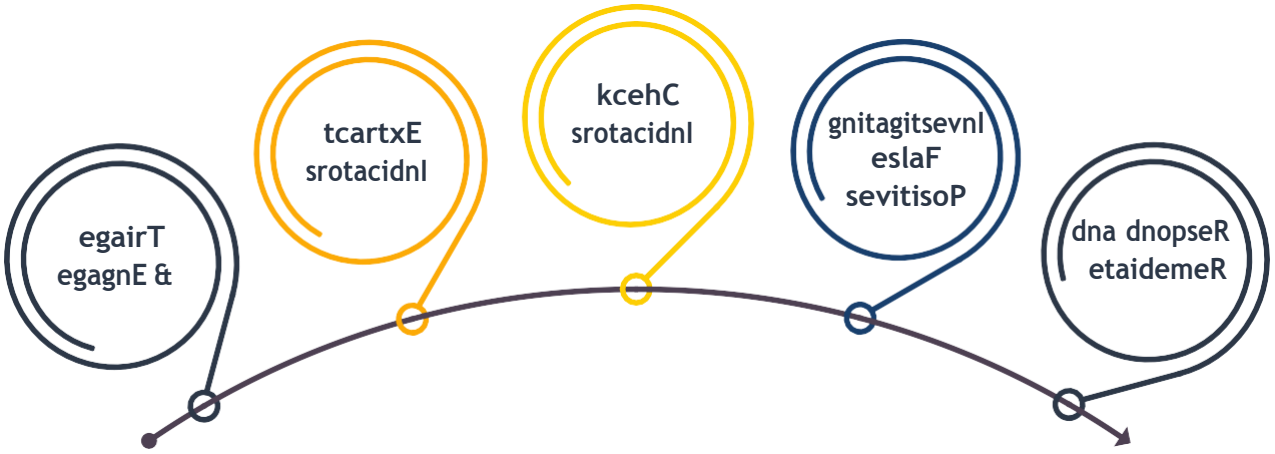
نظام کے اہم اجزاء کی خصوصیات کا حصہ

- ✓ کنیکٹر صارف
- ✓ عمل دستی کی تعریف
- ✓ رپورٹ اور ڈیش بورڈ
- ✓ جمع کریں۔ ڈیٹا
- ✓ ممکن کنکشن کو نظام ہائے DI دوسرے
- ✓ ممکن تصدیق صارف سمت DI حملے
- ✓ ممکن تعریف اشارے حملوں کا پتہ لگانے کے لیے
- ✓ ...

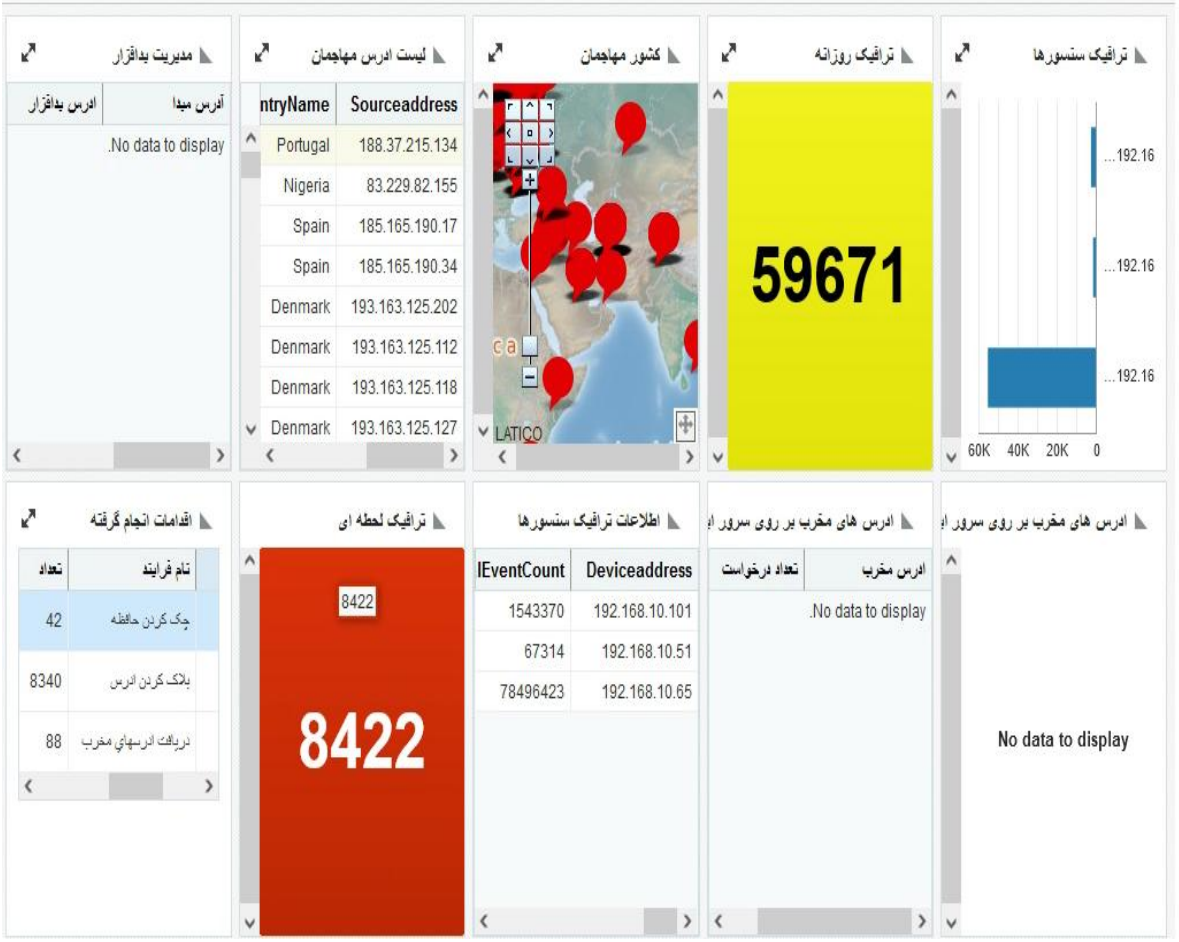


دیگر سہولیات

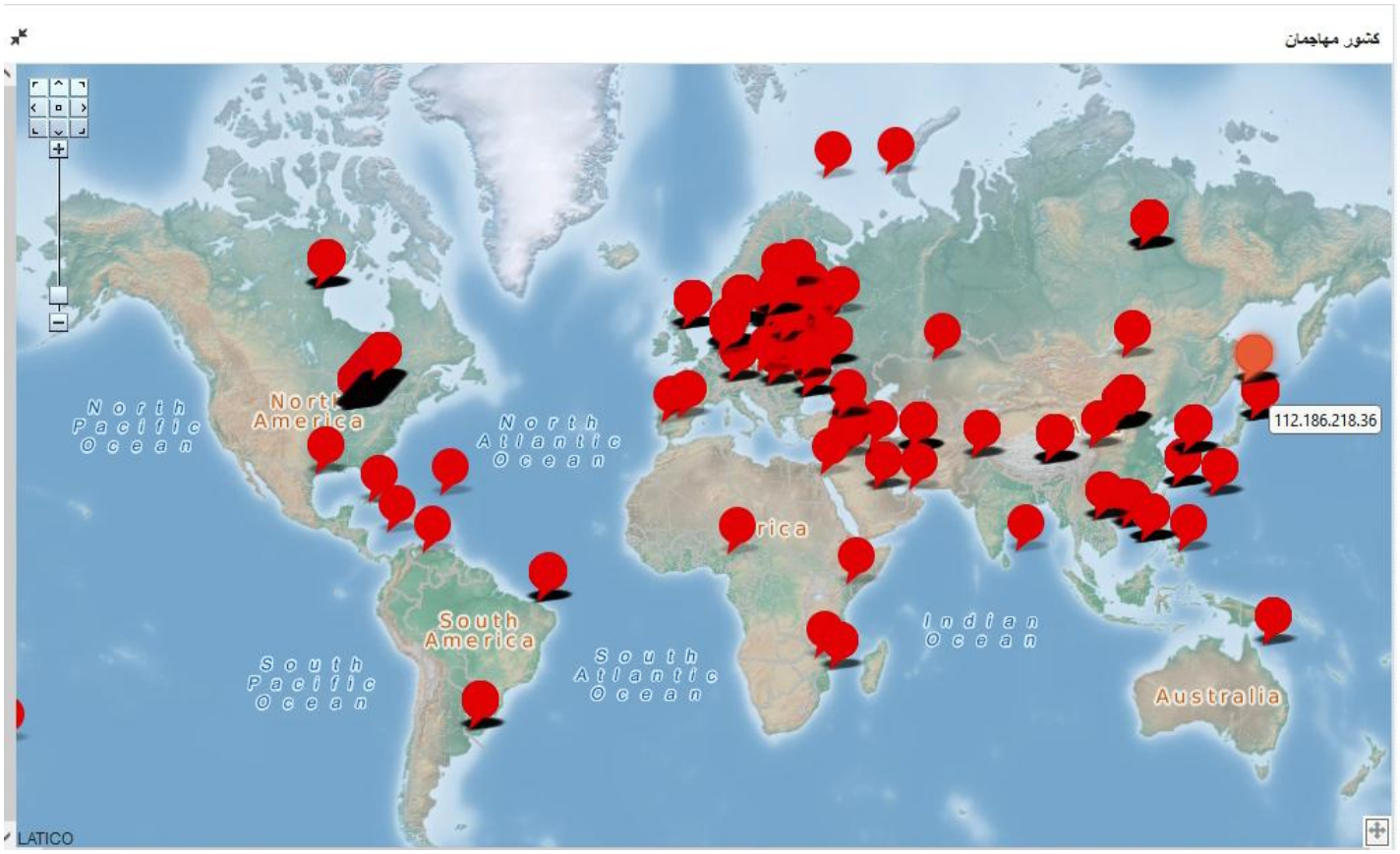
- ✓ عدم موجودگی حد بندی پر نمبر پالیسیاں اور قابلیت ٹیوننگ اور اضافہ ایسا کرنے کے لئے منظرنامے سیکورٹی کی طرف سے صارف
- ✓ بنیاد علم (نالج ڈیٹا بیس) مکمل اور ترقی یافتہ
- ✓ ممکن تعریف صارفین اور گروپس صارف کو نمبر لامحدود اور انتظام ترقی یافتہ صارفین
- ✓ ممکن جمع کرائیں ای میل اور پیغام کو کب پیداوار وارننگ اور سسٹم ٹکٹنگ
- ✓ قابلیت تعامل کے ساتھ دوسرے مراکز آپریشن سیکورٹی
- ✓ ممکن پروسیسنگ نتائج دریافت کرنا کمزوریاں پر انجن پروسیسنگ ارتباط
- ✓ قابلیت نگرانی مکمل ٹریفک داخلہ اور آؤٹ پٹ نیٹ ورک کو علیحدگی اجزاء
- ✓ قابلیت اپ ڈیٹ کریں۔



نمونه مینجمنٹ رپورٹ فارم



نمونہ مینجمنٹ رپورٹ فارم



اسی طرح کی مصنوعات کا موازنہ کریں۔

اشارے	سولر ونڈز	سپلنک	آرکسائٹ	radaRQ	گارڈ
کیس استعمال کریں۔	ٹھیک ہے	ٹھیک ہے	ٹھیک ہے	ٹھیک ہے	ٹھیک ہے
ڈیٹا کا ذریعہ	-	زیادہ تر	+400	+400	زیادہ تر
SPE XAM	M25 فی دن	پیٹا بائٹ ڈیلی	100,000	1000000	1000000
انٹیلی جنس	غیر معمولی رویہ	مشین لرننگ اور ABEU	مشین لرننگ	مشین لرننگ اور UEBA اور فارنسک	مشین لرننگ
ترسیل	ورچوئل ایپلائینس	سافٹ ویئر یا کلاؤڈ	آلات یا سافٹ ویئر یا کلاؤڈ	آلات یا سافٹ ویئر یا کلاؤڈ	سافٹ ویئر یا کلاؤڈ
سپورٹ ایجنٹ	MES	یو ایف	SC، Syslog	Wincollect، golsyS	SC، UF، Syslog، کسٹم
قیمتوں کا تعین	فی نوڈس	زیادہ سے زیادہ روزانہ ڈیٹا کی بنیاد YAD/BG	زیادہ سے زیادہ روزانہ ڈیٹا یا EPS کی بنیاد	فی مہینہ	زیادہ سے زیادہ روزانہ ڈیٹا یا EPS کی بنیاد

شکریہ

Sales Manager:
Mr.KARIMI
+989219427704
info@socguard.ir