Detailed Info

www.novacybersecurity.com

NETAS TELEKOMUNIKASYON A.Ş.
Yenişehir Mah. Osmanlı Bulvarı No:11 34912 Kurtköy - Pendik/İstanbul/Turkey
www.netas.com.tr/en

E-mail: info@novacybersecurity.com
Tel: +90 216 522 20 00
Fax: +90 216 522 22 22

/NetasTR
/NetasTR
/NetasTR
/company/netas
/NetasTR

NETAS

Netas provides innovative end-to-end value added systems integration and technology services in information and communications technologies (ICT). Its customers range from telco providers to public and private enterprises in domestic and international markets. Netas's constant focus on productivity is based on its next generation competencies around technology skillset and expertise. The company holds a track-record of 50 years and continues its foray in the next generation technologies, supported with its experienced, best of breed research and development teams.

The company, provides its customer with solutions in various domains such as networking, cyber security, unified communications, virtualization, cloud computing, broadband mobility, optical and carrier Ethernet, GSM-R. Netas is a leader in IT integration services, managed services and software development solut-ions. Netas also plays an important role in the modernization of the Turkish Armed Forces' communication networks. Also, the company serves armed forces of some other countries in North Africa, Asia-Pacific and the CIS.

NOVA
Cyber Security Solutions by NETAS

Are you aware that you are vulnerable to many threats on the Internet?

With increasing voice and video transmission over IP and emerging new technologies such as 4G LTE and 5G, data vulnerabilities and lack of security are the main concerns due to the nature of IP infrastructure systems. Reports show that most of attacks occur in the application layer. Therefore our products and services focus on the application layer security. Discover vulnerabilities, detect and prevent attacks, enable secure media communication with our solution.

Find out your vulnerabilities and protect your network with NOVA!

Create and operate a secure VoIP infrastructure with comprehensive VoIP Penetration Test relies on, NOVA PENTEST Services via NOVA V-SPY Vulnerability Scanning and Analysis Tool.

V-SPY is an automated enriched VoIP penetration test suite including rich variety of VoIP attack modules, detailed reports of security measures via expert system.

Detect and prevent VoIP threats using VoIP Application Firewall, NOVA V-GATE.

V-GATE is ready to guard your VoIP infrastructure by performing deep packet inspection, statistical and behavioral analysis, detecting anomalies and preventing VoIP attacks, VoIP monitoring and operational management.

Detect telecommunication frauds using Fraud Management System, NOVA FMS.

FMS offers an intelligent, agile and economical solution that can perform security analysis on massive data volume with machine-learning techniques in real-time to detect frauds and threats.

Make a secure multimedia communication via Secure Media Communication Platform, NOVA S/COM.

S/COM can achieve secure media transfer with its support for various security methods and flexible crypto algorithm, enabling secure voice and video communication, whiteboard usage, file and message transfer.

Maintain a secure operation in UC network, VoIP ad Web applications with NOVA Product Family.

NOVA is a product name of NETAS Cyber Security Technology Development Group developments. VoIP, Web, IoT, Mobile security are the main areas with real time data analysis, artificial intelligence, big data analytics methods usage.

NOVA FMS

NEXT GENERATION FRAUD MANAGEMENT SYSTEM

NETAS

www.novacybersecurity.com

Next Generation Fraud Management System

NOVA FMS is a big data security analytics platform that supports deep, holistic, correlative assessment using statistical and machine learning approaches. Key points include complex anomalies, cyber-attacks, cyber-threats, cyber fraud, user behavioral analysis, analytical rule engine and advanced network monitoring (Web, VoIP, and Netflow data).

Overview

The ongoing digitalization of the business world is putting companies at risk of cyber-attacks more than ever before. Big & fast data analytics has the potential to offer protection against these attacks.

NOVA FMS platform provides

- Near-real time analyze for high volume of telecom data
- Rule-based detection of known patterns, anomalies and attacks
- Advanced machine learning to learn normal user and entity behavior and detect changes and anomalies in each user's account and call usage
- Operational monitoring and data analysis framework with rich visualizations.

The goal of **NOVA FMS** platform is to provide an *Intelligent*, *Agile* and *Economic* solution that can perform security analysis on massive data volume with machine-learning techniques in real-time to detect frauds and threats.

- **NOVA FMS** platform is intelligent because it uses machine learning, user profiling, behavior analysis, threat modeling and combines them to obtain better results.
- **NOVA FMS** platform is agile because it can be deployed quickly with out-of-the-box collectors and connectors and machine learning-based threat models.
- **NOVA FMS** platform is affordable because it is established with an acceptable cost for both licensing and maintenance with open source big data platforms

Key Features and Benefits

Fraud Detection with Streaming Data: The traditional CIA (Confidentiality, Integrity, and Availability) model of cyber security is insufficient to prevent fraud as a threat. In the fast detection of credit card fraud in the financial sector or toll fraud in the telecom sector, streaming data is an important part of the solution. **NOVA FMS** has a distributed, scalable and stream-based architecture.

Analytic Rule Engine (ARE): It enables to create and manage rules in **NOVA FMS**. There is a Rule Build Wizard which is designed to specify the rules in detail field by field. Also, there are two modes of the rule engine: streaming mode and batch mode.

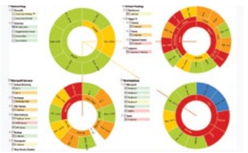
Anomaly Detection with Machine Learning, User Profiling and Behavior Analysis: Anomaly detection is to detect unusual patterns that do not fit the expected behavior. **NOVA FMS** correlates and applies security analytics and machine learning algorithms on the preprocessed data in order to detect complex anomalies, attacks and threats in near-real time with minimal false-positives.

Visualization and Reporting: **NOVA FMS** provides pre-defined and customizable dashboards and historical reports, efficient access to historical data, and investigation tools such as drill downs, ad-hoc search and query of all data for forensic analysis.

Alert Management: **NOVA FMS** offers scored and labeled alerts to decrease false positives and to speed up the investigation.

Out-of-the-box Collectors and Connectors: **NOVA FMS** presents out-of-the-box collectors and connectors and also allows collaborations with other Nova products as a solution.

Sample Use Cases



Telecom Fraud Analytics

Due to various frauds, there is a loss of 38.1 billion dollars in the telecommunication sector according to CFCA report. It is a challenge task to be alerted in a timely manner by processing huge volume of call records. Especially, **Nova FMS** focuses on to detect international revenue share fraud (IRFS, $10.8 billion), premium rate service fraud ($3.8 billion) and traffic fraud (interconnect bypass - $6.0 billion) in real time.

VoIP and Web Applications Analytics

NOVA FMS is also an instrumental in helping teams increase their productivity, providing the detailed statistical analysis of VoIP and Web applications, presenting real-time and historic key performance metrics and making these stats easily visible.