ClearSkies™

Redefining SIEM

Incorporating the power of Big Data Advanced Security Analytics

www.clearskiessa.com

The Threat Landscape is changing.

Are you prepared?

As the boundaries of organizational networks begin to blur with the introduction of cloud, mobile services and IoE technologies, organizations face new challenges when it comes to effectively protecting their valuable information and assets.

1. Organizational networks expand both in size and complexity making it more difficult to detect data breaches.

2. The new generation of sophisticated and highly skilled cyber-criminals and malicious insiders are far more effective in exploiting vulnerabilities and weaknesses.

3. Meeting legal and regulatory compliance obligations has become an extremely complex, time-consuming and costly process.

MAIN CHALLENGES FACED BY ORGANIZATIONS TODAY

- Early detection and response to targeted attacks and data breaches
- Prediction of suspicious and/or detection of malicious and abnormal behavior
- Clear, real-time visibility of the organizational security posture
- Meet, accelerate and validate complex compliance requirements

In this rapidly changing landscape, traditional SIEM solutions fall short in facing the new challenges.

ClearSkies™ ***Next Generation*** *SIEM-as-a-Service*

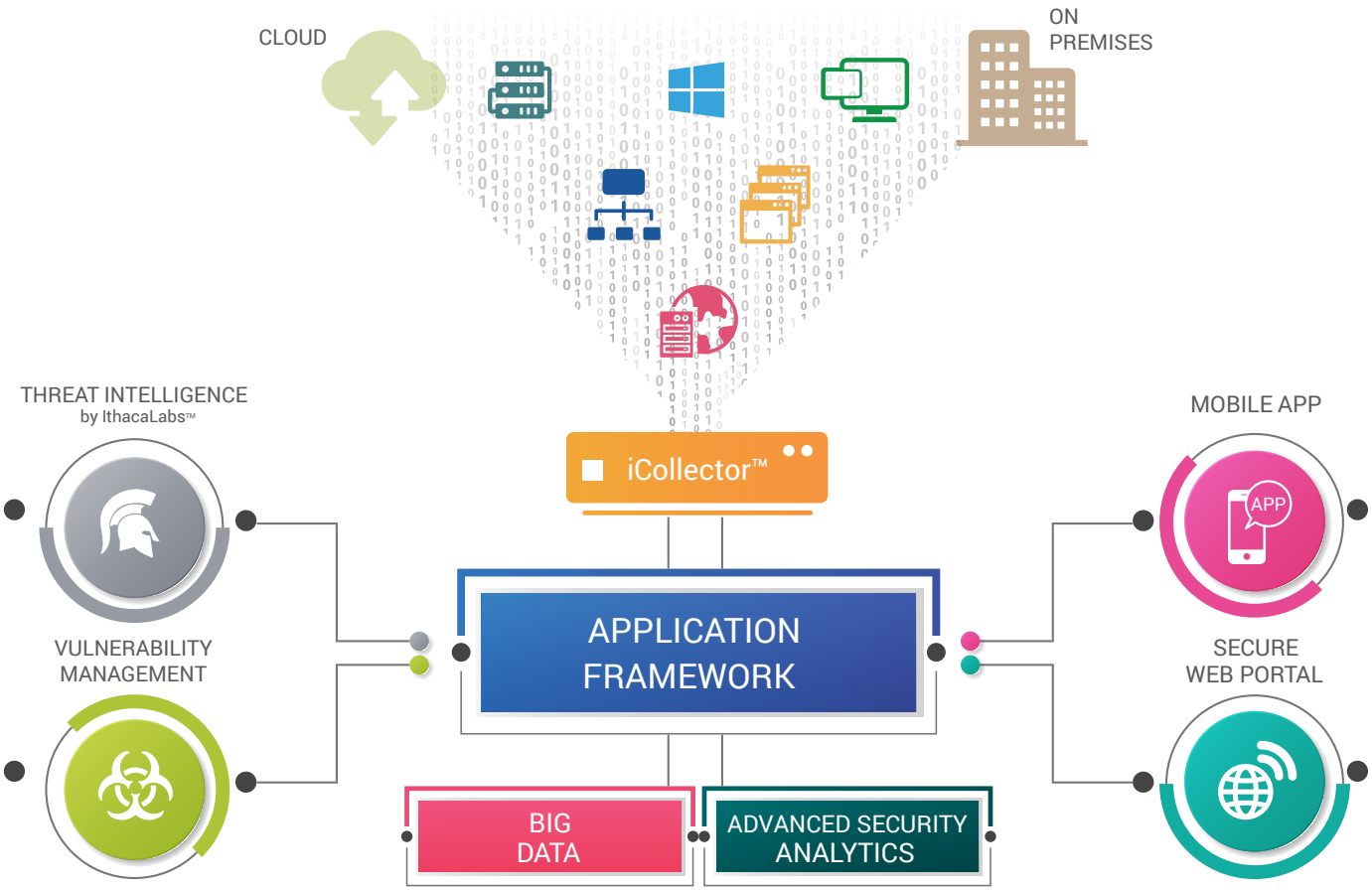
IS BUILT to address them!

Redefining SIEM

Incorporating the power of Big Data Advanced Security Analytics

Having received the 2015 Data Impact Award for the most admirable architecture, ClearSkies™ NG SIEM is a fast, robust, flexible, scalable and cost-effective Next Generation SIEM offered in a **SIEM-as-a-Service model.**

It addresses the need of organizations of any size, complexity or industry to improve their detection and response capability - "Detection Deficit" - to targeted attacks and data breaches before it is too late.



Big Data Advanced Security Analytics

Your most powerful ally

against emerging threats and vulnerabilities

ClearSkies™ NG SIEM-as-a-Service Collects, Archives, Digitally Signs, Encrypts, Normalizes, Correlates, Masks and **Intelligently Analyzes** using in-depth User & Entity Behavior Analysis (UEBA), Artificial Intelligence, Predictive and Machine Learning models, vast volumes of both historical and current log data **in real time**, from heterogeneous data sources ranging from servers, IoT, applications, network/security devices and user activities. It does so with speed, depth and breadth that **conventional SIEM systems are simply incapable of delivering.**

Advanced Security Analytics

By combining current and historical log data for real-time analysis, ClearSkies™ can identify new event patterns which are related to events that occurred in the past.

Through this process, ClearSkies™ is able to identify outliers and patterns which indicate malicious or suspicious activity that would otherwise be impossible to track.

Adaptive Correlations

Having vast volumes of historical log data available for analysis also significantly enhances the ongoing calibration of user and entity activity to normal patterns of behavior.

Combining all these capabilities also allows the early detection and response to potentially harmful, ongoing malicious activities and user suspicious behavioral pattern changes.

ClearSkies™ further enhances this process by using contextual information in combination with evidence-based knowledge (Threat Intelligence) of emerging threats and vulnerabilities.

Drastic Reduction in False Positives

Unlike traditional SIEM solutions, this unique combination of advanced security analytics and adaptive correlation capabilities helps security personnel to focus on combating real cyber-threats, as it minimizes false positives generating only a small number of security alerts.

Calibration based on Risk Appetite

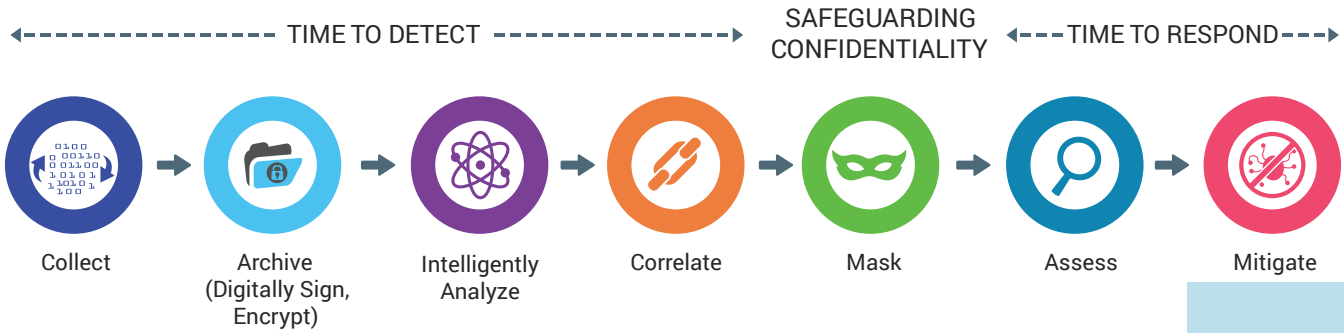
To make things even easier these alerts are ranked by severity and impact, based on a preselected risk model, which reflects the organization's risk appetite.

The alerts generated are even enriched with additional forensic information, thus considerably simplifying a security analyst's job in responding to cyberattacks before it is too late.

Streamlining

your Threat Management Process

ClearSkies™ NG SIEM-as-a-Service streamlines your Threat Management Process by significantly accelerating your proactive cyber-threat detection and response capabilities thus drastically reducing your **"Detection Deficit"** (time between breach and discovery), while at the same time safeguards the Confidentiality, Integrity and Availability of sensitive information found within log data.



Why ClearSkies™ NG SIEM-as-a-Service

KEY FEATURES	KEY BENEFITS
• Collects, stores, processes, aggregates and analyzes vast volumes of historical and current log data from heterogeneous data sources	The combination of current and historical log data for real-time analysis enables the identification of new event patterns and outliers indicating malicious or suspicious activity
• Achieves up to 95% reduction in the number of false positive alerts by combining advanced analytics and adaptive correlation capabilities	Security personnel can focus on combating real cyber-threats
• Generates alerts enriched with evidence-based knowledge and contextual information	Simplifies security analysts' job in responding to cyberattacks
• Intelligently analyzes and correlates data by incorporating evidence-based knowledge and contextual information about users, assets, threats and vulnerabilities	Early detection and response to targeted attacks and data breaches
• Digitally signs and encrypts raw log data, safeguarding the confidentiality and integrity of sensitive information	Raw log data can be utilized for forensic investigation purposes and/or legal evidence should the need arise
• Facilitates the timely response to security incidents anytime, anywhere through ClearSkies™ Mobile App	Real-time visibility while on the go
• Flexible license and delivery model	Offered in different flavours (Express, Enterprise, Co-Managed, Hybrid) based on the customer's needs and budget

SIEM-as-a-Service vs On-Premises SIEM

ClearSkies™ NG SIEM is offered as **SIEM-as-a-Service** so that you can avoid costs associated with hardware obsolescence, software updates and other operational costs. It can be easily scaled to suit your needs and budget.

	On-premises SIEM	ClearSkies™ NG SIEM-as-a-Service
Big Data Advanced Security Analytics	NO	YES
Threat Intelligence	NO	YES
Upfront investment	YES	NO
Administration and software maintenance (Operational Expenses)	YES	NO
Hardware obsolescence	YES	NO
Hybrid license model (SIEM with Managed Security Line of Services)	NO	YES
Scalable based on your needs and budget	YES*	YES
Fast implementation, immediate results	6-18 months	Within 4-6 weeks

* Trading in or replacing an on-premises SIEM with a more powerful one could result in an organization losing more than 75% of their initial investment.

Flexible & Scalable
License Delivery Model

Not a "one size fits all" SIEM solution

ClearSkies™ NG SIEM-as-a-Service "Express"

Designed for small and medium size IT environments, **ClearSkies™ NG SIEM "Express"** offers all powerful features at an affordable price. It addresses the pivotal, proactive security monitoring and management needs of organizations in this sensitive economic sector.

ClearSkies™ NG SIEM-as-a-Service "Enterprise"

Offered in a modular manner, **ClearSkies™ NG SIEM "Enterprise"** addresses the needs of organizations regardless of their size, complexity or industry, in accordance to their environment and budget.

PRODUCT DELIVERY

SERVICE DELIVERY

SERVICE MODULES	Dashboard	Analytics	Vulnerability Management	Reports	Event Management	Compliance	Threat Intelligence	Performance & Availability	Endpoint Agent	CO-MANAGED	MANAGED SECURITY
Express	•	•	•	•	•	•	•	•	•	–	–
Enterprise	•	•	•	•	•	•	•	•	•	•	•

Co-Managed SIEM

Many SIEM implementations fail due to lack of expertise, limited internal information security resources and lack of appropriate organizational structures.

Odyssey's **Co-Managed** services maximize the value and effectiveness of a SIEM investment by supplementing your organization's IT security staff with world-class cybersecurity experts.

Our cybersecurity experts can help you daily with log data analysis, alerts review, event management, incident response, development of correlation policies and preparation of relevant reports, ensuring the continuous enhancement of your security and compliance posture.

Hybrid (SIEM & Managed Security Line of Services)

Consolidating your cybersecurity management function regardless of responsibility ownership, **ClearSkies™ NG SIEM-as-a-Service** allows for an asset-based **Hybrid management model** where the same platform is used to manage both; assets you want to manage/monitor internally as well as assets you decide to outsource to Odyssey's Managed Security Services team of highly specialized and experienced professionals. Access to this pool of experience and expertise may include Managed Detection & Response (MDR) services for preventing targeted attacks and data breaches for which your organization might not be prepared. This directly accelerates your Threat Management Process and by extension, your organization's incident detection and response capabilities.

ClearSkies™ NG Endpoint Detection & Response (EDR) Agent

detects and stops suspicious/malicious activities and user abnormal behaviors with the use of Behavioral Analysis and File Integrity Monitoring (FIM).

Today's sophisticated cyber-threats require more than traditional antivirus protection.

Deploy ClearSkies™ NG Endpoint Detection & Response (EDR) Agent on your critical workstations or servers, either on-premises and/or cloud, to

- Gain real-time visibility
- Stop data leakage
- Block Malware, 0-day exploits and APTs
- Detect user, network and host suspicious/malicious behavior
- Know Who did What from Where and When
- Enhance/simplify your compliance and auditing requirements

ClearSkies™ NG Endpoint Detection & Response (EDR) works on workstations and servers as Standalone, or it integrates into ClearSkies™ NG SIEM.

NO Signature-based detection

NO Security Expertise required

NO Performance degradation

NO Connectivity required

Features


Blocking and Isolation of Suspicious/Malicious Activities


Facilitation and Validation of Regulatory Compliance


User Activity Monitoring


File Content Modifications


Real-Time Visibility


Built-In Threat Intelligence


Ease of Use

Benefits


Behavioral Analytics - User & Entity Behavior Analysis (UEBA)


Malware, APTs and 0-day Detection


File Integrity Monitoring (FIM)


Incident Management


Unauthorized Network Traffic


Reporting


Policy enforcement


Maintenance

ClearSkies™

Big Data Advanced Security Analytics Platform

An award-winning service delivery vehicle

The increasing rate at which information data is being produced creates an equally expanded need for storing, processing and analyzing these huge volumes of heterogeneous data sets.

Since conventional SIEM systems and Security Analytics methods have proved to be unable to handle organizations' unprecedented processing and analytic needs, new concepts, approaches and technologies are sought.

Odyssey managed to address this challenge through the development of its homegrown **ClearSkies™ Big Data Advanced Security Analytics Platform** which is capable of storing, processing and intelligently analyzing in **real time** vast volumes of both historical and current log data.

Through the achievement of high levels of speed and accuracy during the analysis of log data collected from IoT, servers, applications, network/security devices or even from user activities, the platform maximizes the management efficiency and the effectiveness of the threat detection and response process.

Built-in capabilities which made this endeavor a success

Storage Capacity

Data which was previously too expensive to store and impossible to manage, can now be made available for real-time analysis.

Processing Power

Ability to process in real time vast volumes of log data, both historical and current.

Analytic Capabilities

Early detection and response of potentially harmful, ongoing malicious activities and user behavioral pattern changes.

Reliable Architecture

Realization of high-level log data reliability, availability and fault tolerance.

Flexibility

Vast expansion of the platform's capability to process new types of log data, including smart devices of the Internet of Things era, further enhances the log data management efficiency and effectiveness of the threat mitigation process.

The award-winning* **ClearSkies™ Big Data Advanced Security Analytics Platform** is the vehicle delivering Odyssey's flagship service lines namely:

ClearSkies™ NG SIEM-as-a-Service, ClearSkies™ NG Endpoint Detection & Response (EDR) Agent and Managed Security Line of Services.

***In 2015 Odyssey won the Data Impact Award in 'Operational Analytics' for Most Admirable Architecture**

ClearSkies™ Secure Web Portal

Full visibility of your security posture made easy

Gain control, transparency and real-time visibility of your security posture and activities through the ClearSkies™ Secure Web Portal, a highly customizable centralized management console.

Designed to optimize user experience, ClearSkies™ Secure Web Portal's attributes include:

Real-time visibility: Provides real-time visibility of your organization's security posture and helps you meet compliance for on-premises, cloud or both in hybrid critical IT environments.

Highly Customizable Environment: Enables users to customize their working environment based on their job responsibilities, operational needs and work habits.

User-friendly Interface: Enhances users' experience by offering a user-friendly working environment.

Easy to understand: Its functional interface provides enhanced visibility and understanding of your log and event data.

Odyssey at a glance

Odyssey was founded in 2002 with the main objective of providing High-Quality, Cutting-Edge, Cybersecurity, Managed Security and Risk Management Services to organizations that value their information assets.

We provide innovative services and solutions, which span the whole spectrum of People - Process - Technology. Our core aim is to help organizations in all industries regardless of size and complexity, to effectively and efficiently manage their cybersecurity risk. Innovation, Passion for Perfection and Customer Focus rule our daily business, being the corporate values that we cherish the most.

Our ability to always meet YOUR needs and constantly exceed YOUR highest expectations has placed us in a market leadership position with a global footprint. Our fast expanding presence includes Odyssey offices in Cyprus, Greece and the USA as well as an extensive international network of Value Added Resellers and Distributors.

Odyssey is ISO 27001 certified and has been accredited by the Payment Card Industry Security Standards Council (PCI SSC) as a Qualified Security Assessor (QSA) and an Approved Scanning Vendor (ASV).

ClearSkies Timeline

2002
> Odyssey founded
> Managed Security Services (MSS) provided on customer premises

2003
> 1st MSS contract, still in effect today, signed

2004
> Opened local office in Athens, Greece

2005
> Opened MSS SOC in Athens, Greece

2006
> Released the 'Cyber-Threat Alert' service

2007
> Launched MSS Secure Web Portal

2008
> Signed the 1st MSS contract with an organization with offices in multiple countries

2009
> Incident response services provided to customers

2010
> ClearSkies™ SIEM launched

2011
> Established IthacaLabs™ Threat Intelligence Unit

2013
> Launched ClearSkies™ Big Data Security Analytics Platform v4.0
> Transitioned ClearSkies™ SIEM to Big Data & Security Analytics Platform
> ClearSkies™ NG iCollector v1.0 released

2014
> Released ClearSkies™ NG Endpoint Agent v1.0

2015
> Released ClearSkies™ NG SIEM Mobile App v1.0
> Won the "Data Impact Award" in the "Operational Analytics" category for "Most Admirable Architecture" for ClearSkies™ Big Data Security Analytics Platform

2016
> Opened local office in New York, USA
> Asset-based Hybrid management model introduced

2017
> Released ClearSkies™ NG Endpoint Agent v5.0 Enterprise edition including FIM & Antimalware capabilities
> ClearSkies™ NG SIEM Express model introduced

2018
> Expansion to the Middle East
> Launched an intelligent User & Entity Behavior Analysis (UEBA) model on the ClearSkies™ Platform.

HEADQUARTERS

CYPRUS
1 Lefkos Anastasiades Str.
2012 Strovolos, Nicosia
Tel.: +357 22463600, Fax: +357 22463563
Email: info@odysseycs.com

OFFICES: CYPRUS | GREECE | USA

ODYSSEY™
Impossible Challenges, Possible Solutions

www.odysseycs.com