ClearSkies™

UNLOCK THE INTELLIGENCE OF YOUR LOG & EVENT DATA

Your data have a story to tell. Discover patterns of suspicious/malicious behavior hidden inside your network activity.

AN **ODYSSEY**™ PRODUCT
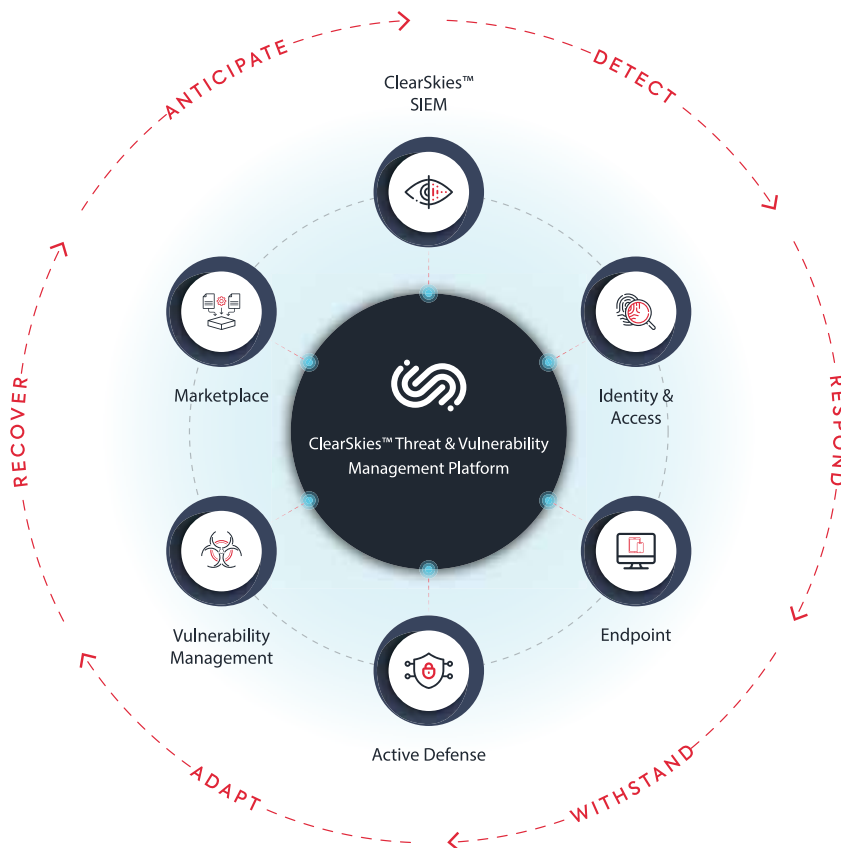cybersecurity

ClearSkies™

THREAT & VULNERABILITY MANAGEMENT PLATFORM

ClearSkies™ Threat & Vulnerability Management Platform is a flexible Extended Detection & Response ecosystem that intelligently transforms log and event data into actionable security intelligence, enabling the rapid detection and response to sophisticated threats and vulnerabilities.

With ClearSkies™, you minimize digital risks along your digital transformation journey, essentially realizing your return on your investments.

The platform's Extended Detection & Response ecosystem grants cross-layered visibility of your digital infrastructure and security posture in real time, with the ability to anticipate, withstand, adapt, meet legal and regulatory frameworks, and quickly recover from data breaches.

THREAT & VULNERABILITY MANAGEMENT PLATFORM
CROSS-LAYERED VISIBILITY FOR EXTENDED DETECTION AND RESPONSE

Pay-as-you-grow while taking your cyber defense maturity to the next level with a flexible service delivery model.

The innovative ClearSkies™ Threat & Vulnerability Management Platform is a flexible ecosystem of products for Enterprises and MSSPs. Deployed as SaaS, On-Prem or the Cloud, it associates threats with corresponding vulnerabilities as they emerge, for timely and accurate detection and response capabilities.

With advanced security intelligence, machine learning and AI at the core of its adaptable architecture, the platform grants Extended Detection & Response (XDR) capabilities through powerful tools including SOAR and Cyber Response Playbooks.

- ⊘ Contextual security awareness
- ⊘ Optimized security posture according to your risk appetite
- ⊘ Simplified regulatory compliance
- ⊘ Streamlined threat management
- ⊘ Efficient automation and orchestration

FOR MSSPS
Cut resources. Boost your profits. Provide top value. Stand out from your competition.

- Centralized Management ⊘
- Multitenancy ⊘
- Onboarding ⊘
- Streamlined alert management ⊘
- Enhanced incident investigation ⊘
- Automation and orchestration ⊘
- Efficiency ⊘
- Reliability ⊘

FOR ENTERPRISES
Your information security and compliance challenges... covered.

- ⊘ Contextual security awareness
- ⊘ Optimized security posture according to your risk appetite
- ⊘ Simplified regulatory compliance
- ⊘ Streamlined threat management
- ⊘ Efficient automation and orchestration

SIEM
HOLISTIC TELEMETRY. STREAMLINED INCIDENT MANAGEMENT

Cloud-ready ClearSkies™ SIEM focuses on multi-telemetry data ingestion, advanced security intelligence and proactive Threat Hunting to deliver Extended Detection & Response.

The ClearSkies™ SIEM experience

- Accelerated MTTR
- Minimized impact of attacks
- Privacy control
- Reduced alert fatigue
- Efficiency and lower operational costs
- Streamlined incident management workflows
- Fast time to value
- Forensic-based Threat Hunting
- Modular flexibility

Well-rounded features

- User & Entity Behavior Analysis (UEBA)
- Security Orchestration, Automation and Response (SOAR)
- Data enrichment and third-party integrations
- Embedded Threat Intelligence
- Enhanced legal and regulatory compliance
- Sensitive data obfuscation
- Cyber-Threat Taxonomy
- Advanced correlation engine
- Malware detection based on textual or binary patterns
- Cyber Response Playbooks

It streamlines your Threat Management Process by significantly accelerating your proactive threat detection and response capabilities, thus drastically reducing your **"Detection Deficit"** (time between breach and discovery).

TIME TO DETECT			SAFEGUARDING CONFIDENTIALITY		TIME TO RESPOND	
Collect	Archive (Digitally Sign, Encrypt)	Intelligently Analyze	Correlate	Mask	Assess	Respond	Mitigate

GET COVERED WITH A WELL-ROUNDED SET OF SERVICEMODULES

Threat Intelligence

A continuously updated, analyzed and contextualized feed of evidence-based knowledge of emerging cyber-threats and vulnerabilities.

Compliance

Real-time monitoring of your compliance status through customizable dashboards and reports enables a broad compliance overview.

Reports

A plethora of ready-made report templates or by creating you own reports that help you meet the regulatory framework and/or internal audit requirements.

Event Management

A centralized event management interface that lets you monitor, classify and manage events according to their severity while delegating actions and responsibilities where necessary.

User & Entity Behavior Analysis (UEBA)

A powerful feature for profiling of user-related host/network /application activities for detecting suspicious/malicious behavior and intrusions.

Performance & Availability

Proactive monitoring of the performance and availability of network devices, systems and communication links by collecting and processing Netflow and SNMP log and event data.

Real-Time Analysis

A powerful tool for creating complex search queries using various operators for analyzing large volumes of data/threats with intelligent parameters, while also providing visualizations for simplified analysis of search query results.

SOAR

A state-of-the-art tool providing security administrators with the ability to orchestrate and automate responses based on the outcome of a correlation rule.

ADD-ONS
CUSTOMIZE AND EXPAND YOUR SIEM'S CAPABILITIES

ClearSkies™ SIEM expands with over-and-above add-ons and third-party integrations for optimal visibility and effectiveness, according to your specific needs and operational maturity levels.

Active Defense
Post-Breach Detection

Identity & Access
User Identities Management

Endpoint
Endpoint Detection & Response

Vulnerability Management
Vulnerability & Configuration Weakness Remediation

Marketplace
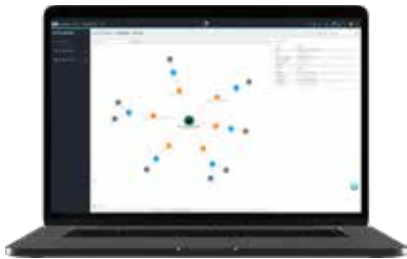Data enrichment via Third-Party Integrations

Since we started using ClearSkies™ products, we have improved our strategic decision-making due to the crucial security context found in the information they provide.

Nesma & Partners, Kingdom of Saudi Arabia

ACTIVE DEFENSE
Identify, lure, deceive and stop threat actors that have penetrated your network

ClearSkies™ Active Defense, is a post-breach detection technology which deceives cybercriminals into thinking they have discovered a way to escalate their privileges, perform lateral movement, or access sensitive information /data towards achieving their goals.

- ✓ Lay traps to catch attackers in the event of a breach.
- ✓ Lure and deceive attackers into revealing information about them.
- ✓ Buy valuable time by delaying and misdirecting attackers in your network.

IDENTITY & ACCESS
Spot Who did What from Where and When

ClearSkies™ Identity & Access provides audit and monitoring capabilities that aggregate log and event data relating to users' identity and access. It feeds log and event data into ClearSkies™'s UEBA and advanced security analytics engine, which extracts context and delivers intuitive visualizations together with audit information of "who did what from where and when".

- ✓ Keep user account statuses in check.
- ✓ Easily spot suspicious or vulnerable user accounts.
- ✓ Drastically improve the auditing and insider threat detection capabilities with minimal effort.

ENDPOINT DETECTION & RESPONSE
Detect and Respond to threats as they emerge

ClearSkies™ Endpoint Detection and Response (EDR) is a comprehensive Endpoint Protection solution, fully integrated with ClearSkies™ to complement the detection and response of cyber, insider and third-party threats by utilizing Behavioral Monitoring and Analysis (BMA) which leverages ClearSkies™ advanced security analytics, and Threat Intelligence.

- ⊘ Get real-time visibility for faster response
- ⊘ Automate and orchestrate response actions
- ⊘ Prevent data leakage
- ⊘ Simplify Incident Investigation and Threat Hunting
- ⊘ Identify users' suspicious/malicious behaviors by using UEBA
- ⊘ Enhance and simplify compliance and auditing requirements

VULNERABILITY MANAGEMENT
Manage Threats & Configuration Weakness to minimize your attack surface

Associate vulnerabilities and configuration weakness with threats targeting your organization to prioritize your actions and minimize the impact of a materialized threat.

- ⊘ Assess, prioritize, act and manage the outcome of a vulnerability assessment exercise.
- ⊘ Prioritize vulnerabilities based on their classification & impact.
- ⊘ Associate threats with corresponding vulnerabilities as they emerge to orchestrate and automate response actions.
- ⊘ Drastically reduce false-positive alerts (up to 95% reduction), saving valuable time and resources that would otherwise be diverted from focusing on actual threats.

MARKETPLACE
Enrich your data

ClearSkies™ Marketplace data enrichment provides seamless integration of disparate 3rd-party technologies for broader and deeper real-time visibility and analysis of what transpires in your networks and systems. Integrate 3rd-party technologies into your Security Information and Event Management process for enriched analysis and investigation processes.

Data enrichment adds more log and event data, as well as contextual information, to your Security Information and Event Management. With an enhanced ability to derive meaningful insights, you are empowered with broader visibility, threat intelligence, and other actionable information that supports reduction of false positives, and more confident responses.

Improved analysis, detection, investigation and response capabilities, and expanding your data sources, provide contextual information vital for situational awareness when evaluating your security posture.

With more refined and complete data, your SIEM operations earn greater usability and value.

SUPPLEMENT YOUR VISIBILITY WITH MORE DATA AND CONTEXT

- Log integrations
- SOAR
- Threat Intelligence
- Ticketing
- ClearSkies™ Premium Add-ons

MAKE THE MOST OUT OF YOUR CLEARSKIES™

ClearSkies™ Services provide you with the knowledge and expertise to optimize your use of the ClearSkies™ Threat & Vulnerability Management Platform.

Support Services grant you the knowledge necessary to successfully deploy and optimize ClearSkies™ in your environment.

Professional Services go over and above to enhance your user experience and expand your capabilities in improving your organizational security posture with ClearSkies™ products.

▼ SUPPORT SERVICES

IMPLEMENTATION
- Installation and Initial Configuration
- Onboarding of In-Scope Assets

CONFIGURATION
- Implementation of Incident Escalation Process and Flows

▼ PROFESSIONAL SERVICES

OPTIMIZATION
- Effectiveness Assessment
- Endpoint Policy Configuration
- Log & Event Collection Optimization
- Security Use Case Modelling and Adoption

TRAINING
- Endpoint Policy Configuration
- Security Analyst

REAL-TIME VISIBILITY FOR YOUR CLOUD ENVIRONMENT

For Microsoft Azure and Oracle Cloud network environments

The ClearSkies™ Threat & Vulnerability Management Platform products can be seamlessly deployed on Microsoft Azure and Oracle Cloud network infrastructures. ClearSkies™ brings to your Azure and Oracle cloud networks and systems the unique benefits of the intelligent and innovative ClearSkies™ products and addons. These include real-time broad and deep visibility, enhanced detection and response, automation and orchestration of response actions, identity and access management, post-breach detection and response, and vulnerability management.

Licensing

ClearSkies™ products on Microsoft Azure and Oracle use the Bring-Your-Own-License (BYOL) delivery model, providing a cutting-edge Security-as-a-Service (SaaS) solution, which addresses the cybersecurity and compliance needs of your organization, regardless of size, infrastructure complexity or industry.

FLEXIBLE & SCALABLE SERVICE DELIVERY MODEL

Considering the varying sizes, needs, complexity, internal capabilities, budget constraints and cybersecurity management maturity levels of different organizations, ClearSkies™ SIEM is a flexible and scalable service delivery model offered as follows: ClearSkies™ SIEM, MS/MDR and Hybrid.

PACKAGE	CLEARSKIES™ SIEM	CLEARSKIES™ SIEM ON AZURE	MS/DR	HYBRID
Log and Event Data collected daily	1, 3, 5, 10... GB	1, 3, 5, 10... GB	1, 3, 5, 10... GB	1, 3, 5, 10... GB
Real-Time Analysis	4 weeks – 12 weeks	4 weeks	4 weeks – 12 weeks	4 weeks – 12 weeks
Online Log and Event Data retention period	3 months – 12 months	3 months	3 months – 12 months	3 months – 12 months
Offline Log and Event Data retention period	Unlimited	Unlimited	Unlimited	Unlimited
Number of Secure Web Portal (SWP) users	Built-in 3 with the option for add-on	Built-in 3 with the option for add-on	Built-in 3 with the option for add-on	Built-in 3 with the option for add-on
Minimum license period	12 months	3 months	12 months	12 months
Endpoint Agent Free	Unlimited	Unlimited	Unlimited	Unlimited
Endpoint Detection & Response Agent	5 included additional can be purchased	5 included additional can be purchased	5 included additional can be purchased	5 included additional can be purchased

A VALUE-SHARING PARTNERSHIP FOUNDED ON TRUST

The ClearSkies™ Partners Program is a value-adding reseller program that drives your business growth by developing your sales capabilities, as well as your technical expertise in successfully promoting and delivering ClearSkies™ products and services.

As a ClearSkies™ Partner, you enjoy a package of incentives, sales tools, resources and benefits, which kickstart your business growth while empowering your customers to gain cross-layered visibility of their digital infrastructure and security posture.

WHY PARTNER WITH US

- Stand out from your competition with innovative world-class offerings
- Access resources that help kickstart your business growth and profitability
- Enhance your technical and sales know-how and skills through in-depth training from world class experts
- Rest assured throughout your business development initiatives with us by your side, every step of the way
- Demonstrate your credibility through world-class training and certifications
- Receive sales leads based on your region and partner status

WHY CLEARKIES™
INNOVATIVE.
TWO STEPS AHEAD.

ClearSkies™ offers an array of unique innovative advantages that empower you in achieving and maintaining cyber resilience in a rapidly changing world. With ClearSkies™, you can rest assured that you have the capability to associate threats with corresponding vulnerabilities as they emerge, this way safeguarding your valuable assets in an expanding threat landscape.

INTELLIGENT
Identify patterns of suspicious/malicious behavior that would otherwise go unnoticed.

INNOVATIVE
We constantly develop our product aiming always to unlock the intelligence of data with new innovative features and add-ons

SCALABLE
A simple and scalable service delivery model allows full control over your security budgets.

CUSTOMIZABLE
A flexible architecture that allows us to adapt to customer environment and needs regardless of the size or complexity.

EASY DEPLOYMENT
Up and running in a matter of a few days with immediate results.

NO COST OF OWNERSHIP
Uncompromising subscription-based products with zero initial investment needed, and ongoing maintenance and administration included.

20+
Years of experience
& expertice

32+
Countries with
trusted customers

150+
Highly skilled
professionals

4
Offices in Cyprus (HQ),
Greece, MENA, UK

3
Intelligent Security
Operation Centres
Worldwide

WE ARE ODYSSEY
YOUR ONE STRATEGIC PARTNER IN CYBERSECURITY

Odyssey is a leader in Cybersecurity, supporting organizations around the globe in their cyber resilient journey.

For more than two decades, Odyssey empowers customers to build an effective and applicable Cybersecurity Strategy, to effectively anticipate, respond, swiftly recover, and adapt to the destructive threats of a dynamically expanding threat landscape.

Odyssey's holistic approach combines five pillars of solutions, services and products: Advisory Services (GRC), Integrated Solutions, Cloud Security, ClearSkies™ Threat & Vulnerability Management Platform and Managed Security / Detection & Response Services (MSDR). Each of the five pillars, both separately or combined, enable organizations to adhere to compliance requirements and effectively manage their digital risks, in all operational aspects of their organization: People, Process and Technology.

Odyssey is ISO 27001, ISO 9001 and ISO 22301 certified, SOC 2® Type 2 attested, and accredited by the Payment Card Industry Security Standards Council (PCI SSC) as a Qualified Security Assessor (QSA). Odyssey has received numerous global awards and recognitions, such as its inclusion in Gartner's Magic Quadrant for Security Information and Event Management for its ClearSkies™ SIEM. Additionally, the company has been certified as a Great Place to Work® for three consecutive years.

ClearSkies™

CYPRUS (HQ) | GREECE | MENA | UK

www.clearskiessa.com