

Unlock the power of your data... Give them a voice!

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



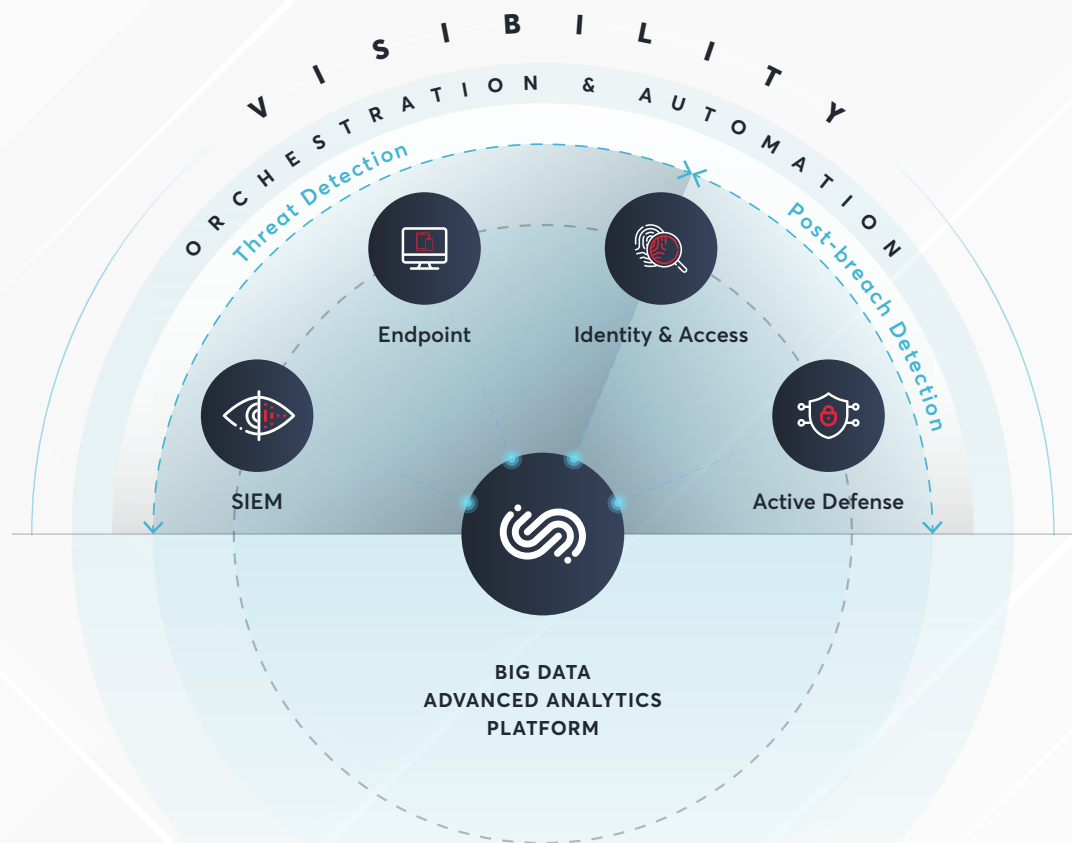
PLATFORM

Optimize your SecOps Investigation & Response against Sophisticated Attacks

The increasing complexity of and dependency on the IT ecosystem gives rise to previously unknown Digital Risks as well as new kinds of threats.

The need to build Security and Resilience into your SecOps from the ground up has never been greater.

ClearSkies™ offers fast, robust, flexible, scalable and cost-effective cloud-based products and services that deliver real-time visibility over your security posture.



WHAT YOU GAIN

Combine
ClearSkies™
cloud-based
products and
services to
minimize your
digital risk



SIEM

Gain Real-Time
Visibility of your
Security Posture



Endpoint

Detect & Respond
to Malware & Insider
Threats Before it is
too Late



**Active
Defense**

Lure and Trap
Threat-Actors Post-
Breach



**Identity &
Access**

Stay on Top of your
User Base



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

SIEM

Unravel Real-Time Visibility

ClearSkies™ Cloud SIEM provides real-time in-depth Intelligent Analysis and Correlation of log and event data collected from heterogeneous data sources combined with evidence-based knowledge of emerging threats and vulnerabilities to produce actionable information.

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). At the same time, it safeguards the Confidentiality, Integrity and Availability of sensitive information found within log and event data.

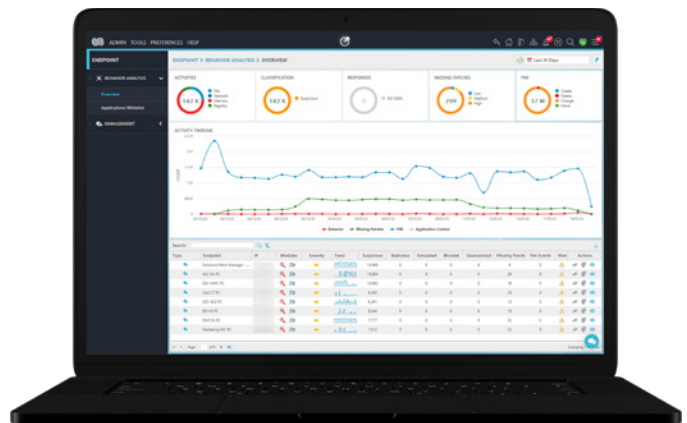


ENDPOINT

Detect and Respond to threats as they emerge

ClearSkies™ Endpoint Detection and Response (EDR) complements the detection and prevention of never-before-seen targeted attacks and insider threats with the use of Behavioral Monitoring and Analysis (BMA) and by leveraging Advanced Security Analytics complemented by Threat Intelligence and signature-based detection.

- ✓ 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



ACTIVE DEFENSE

Hunting the Attackers, not the Attacks

ClearSkies™ Active Defense deceives cybercriminals into thinking they have discovered a way to escalate their privileges, perform lateral movement, and/or access sensitive information/data towards achieving their goals.

If threat-actors attempts any probing or access any fake information, you get an alert notification with attack-vector information for further analysis before an incident is escalated. Attack-Vector information provides you with valuable intelligence as to how cybercriminals interact with assets, including their methods, purpose and source.

By occupying cybercriminals for as long as possible with decoys and traps, you can delay them from achieving their real purpose, thus gaining valuable time to take necessary defensive actions.

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 delivers vital and comprehensive visibility and tracking of precisely what users are authorized to access on your organizational critical systems and resources. Such a powerful user auditing capability also helps ensure compliance with corporate policies and regulatory frameworks.

- ✓ 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.



MSSP PLATFORM

An Intelligent Cloud-Based Managed Security Operations Platform

Cloud-based **ClearSkies™ Cloud MSSP Platform**, together with its support and MSS training scheme, empowers you to provide top-quality Managed Security Services (MSS) that place your organization ahead of the competition.

Provide top-quality and cost-effective Managed Security Services (MSS) to your customers, positioning you as their only sensible choice.

Get peace of mind knowing that the Platform by which you offer your MSS remain constantly maintained, is continuously fed with Threat Intelligence, and remains compliant with relevant regulatory frameworks.

Stand out from the competition with your own multitenancy MSSP Platform backed by world-class cybersecurity expertise. Here's how:

- ✓ Brand your own white-label Managed Security Services (MSS)
- ✓ Provide top-notch competitive Managed Security Services (MSS)
- ✓ Reduce your operating costs through our cost-efficient licensing program
- ✓ Pay as you grow with a scalable and flexible service delivery model
- ✓ Get expert ongoing support, including onboarding, generous resources and continuous partner training

PROFESSIONAL SERVICES

Make the most out of your ClearSkies™

ClearSkies™ Professional Services provide a complete set of services revolving around the ClearSkies™ Big Data Advanced Analytics Platform.

These services help you to successfully implement and improve your organizational security posture while using ClearSkies™ products. Specifically, with ClearSkies™ Professional Services, our experts help with the design, implementation, configuration, optimization and training needed to get the most out of ClearSkies™ products.

Implementation	Configuration	Optimization	Training
<ul style="list-style-type: none">• Installation and Initial Configuration• Onboarding of In-Scope Assets	<ul style="list-style-type: none">• Implementation of Incident Escalation Process and Flows	<ul style="list-style-type: none">• Effectiveness Assessment• Endpoint Policy Configuration• Log & Event Collection Optimization• Security Use Case Modelling and Adoption	<ul style="list-style-type: none">• Endpoint Policy Configuration• Security Analyst

A well-rounded set of ServiceModules



Threat Intelligence

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



Compliance

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



Dashboards

An overview of your security alerts status, performance, availability, user behavior, and other metrics that are more relevant to you.



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.



Vulnerability Management

A consolidation of various vulnerability tools used during your analysis and correlation process to further minimize false-positive alerts.

SERVICE DELIVERY MODEL

Take full control over your security budgets

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

Package	ClearSkies™ Cloud SIEM	ClearSkies™ Cloud SIEM on Azure	MS/MDR	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 5 with the option for add-on	Built-in 5 with the option for add-on	Built-in 5 with the option for add-on	Built-in 5 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

WHY CLEARKIES

Why our customers keep choosing ClearSkies™

ClearSkies™ cloud-based products and services offer an array of unique innovative features based on our expertise and experience, which reflect our understanding and ability to anticipate the Information Security and Risk Management landscape. This allows us to develop innovation-driven products with a customer-focused approach and flexibility to reflect customer's evolving needs and budget.



Get Real Value and Usable Results

Unlocking the power of data by extracting actionable information out of vast volumes of otherwise meaningless data to identify patterns of suspicious/malicious behavior that would otherwise go unnoticed.



Lower your Security Investment and Costs

Uncompromising subscription-based products that lower your cost of ownership, since no initial investment is needed while maintenance and administration are included.



Benefit from our Customer-Focused Approach

Yielding much faster response times to your support enquiries, and more overall support value. ClearSkies™ customers have a voice, and their concerns are heard.



Adapt ClearSkies™ to your Environment and Needs

Flexible architecture that allows for a firm adaptation to any organization of any size or complexity. A scalable service delivery model allows full control over your security budgets.

What our clients say



ClearSkies™ products have helped us to significantly improve the speed at which we detect and respond to suspicious behaviors inside and outside of our networks.

Newsphone, Greece



The efficiency and power of ClearSkies™ [...] are provided by world-class professionals who prove to us daily that we can rest assured knowing that our cybersecurity is in good hands.

Investment Bank of Greece



ClearSkies™ gives our Board a comprehensive bird's-eye view, with drilldown capabilities, of what is happening in our digital environment at all times.

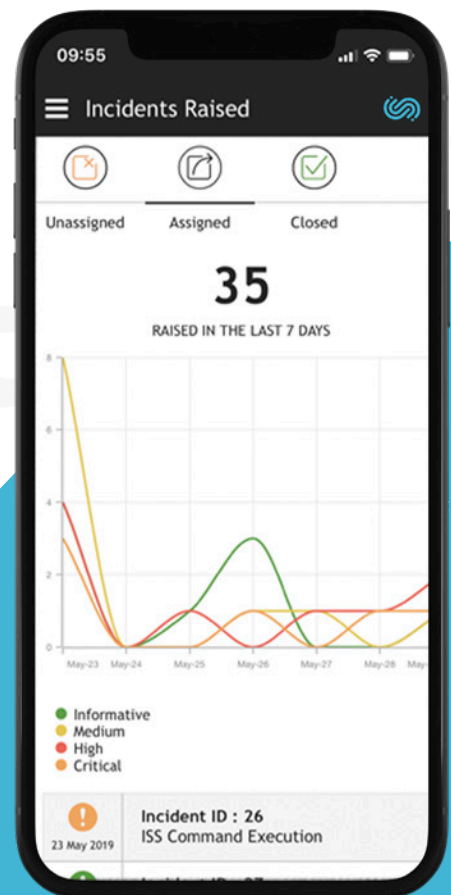
Marlow Navigation, Cyprus

Unlock the power of your data...
Give them a voice
Unlock the power of your data...
Give them a voice
Unlock the power of your data...
Give them a voice

MOBILE APP

Real-time visibility while on the go

ClearSkies™ Mobile App's friendly intuitive interface brings your SIEM's user experience to your smart device to help you stay ahead of information-threats as they emerge, anywhere, anytime.



Contact Us

Cyprus (Headquarters)

1 Lefkos Anastasiades Str. 2012
Strovolos, Nicosia

T +357 22 463600

E info@clearskiessa.com

www.clearskiessa.com



OFFICES CYPRUS | GREECE | USA | UK | KSA

© 2021 Odyssey Consultants LTD.

All rights reserved. This product and related documentation are protected by copyright law and are distributed under licensing restricting the copy, distribution, and reverse-engineering. No part of this product or related documentation may be reproduced in any form or by any means without prior written permission from Odyssey Consultants LTD.

Trademarks © 2021 Odyssey Cybersecurity™, ClearSkies™, iCollector™ and IthacaLabs™ are all registered trademarks of Odyssey Consultants LTD. All other marks mentioned herein are trademarks of their respective companies.