C.O.S.M.O

BRINGING ORDER TO CYBER OPERATIONS

WHITE PAPER

TECHNICAL DOCUMENTATION FOR CYPHER'S
NEXT GENERATION AI/PREDICTIVE ANALYSIS
THREAT INTELLIGENCE PLATFORM

CYPHER

www.cypher-llc.com

CONTENTS

3 INTRODUCTION

4 ABOUT

5 ARCHITECTURE & DEPLOYMENT

7 DETECTING THE THREAT

8 INTEGRATION

9 BENEFITS

10 REALWORLD

12 CONCLUSION

13 GLOSSARY

14 INTERFACE

C.O.S.M.O

CYBER
OPERATIONAL
SECURITY
MANAGEMENT
OPTIMIZER

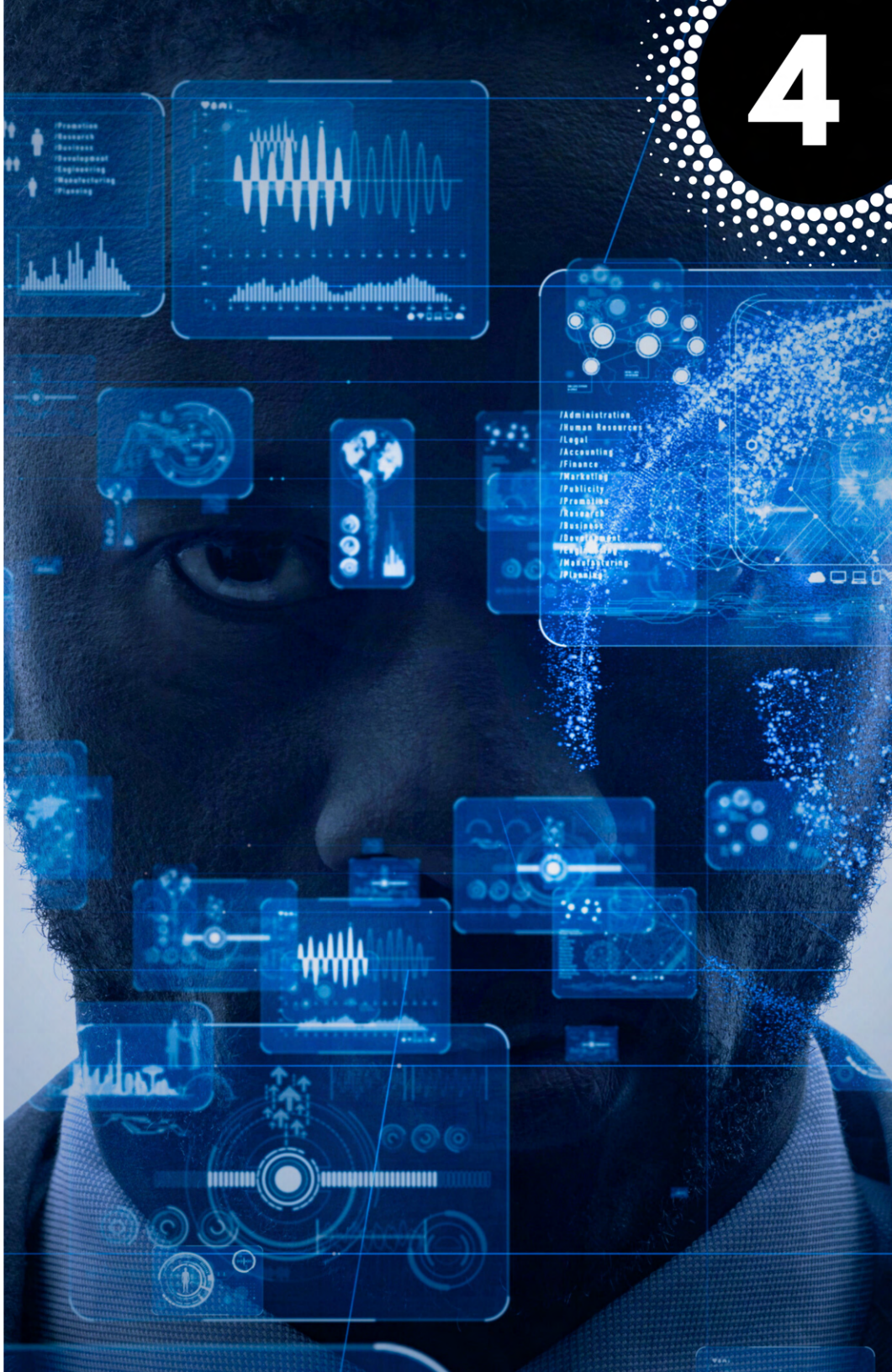
INTRODUCTION

"In today's digital landscape, cybersecurity threats are becoming increasingly sophisticated, requiring advanced tools for effective detection and mitigation. C.O.S.M.O addresses these challenges by integrating AI-driven analysis, predictive capabilities, and comprehensive threat intelligence into a cohesive platform that enhances cybersecurity operations."

ABOUT

C.O.S.M.O (Cyber Operational Security Management Optimizer) is an advanced cyber threat intelligence platform designed to enhance your organization's cybersecurity defenses.

C.O.S.M.O leverages AI, predictive analysis, and a custom built log ingestion tool for document formatting into STIX II format to provide real-time threat detection and comprehensive threat intelligence. C.O.S.M.O offers unparalleled accuracy, proactive risk management, and actionable insights, ensuring your organization stays ahead of cybercriminals.



ARCHITECTURE & DEPLOYMENT

> **C.O.S.M.O's** architecture consists of several key components that work together seamlessly to deliver robust threat intelligence and predictive analysis.

Proprietary AI and Predictive Analysis

GraphQL: Used for querying and manipulating data.

ElasticSearch: For powerful search and data analytics capabilities.

Redis: In-memory data structure store for caching.

RabbitMQ: For message brokering.

Node.js: For server-side scripting.

React: For building user interfaces.

TypeScript: For scalable and robust development.

Hardware Requirements

The hardware needed for deployment scales based on customer requirements and the amount of data being ingested. This flexibility ensures that C.O.S.M.O can be effectively deployed in various organizational contexts, from small enterprises to large corporations.

Hardware Requirements

C.O.S.M.O integrates seamlessly with existing cybersecurity infrastructure, enhancing overall security posture without requiring significant changes to current systems.

User Training and Support

User training and support are provided to ensure users can effectively utilize C.O.S.M.O's capabilities, maximizing the tool's impact on cybersecurity operations.

> C.O.S.M.O offers flexible deployment options, including on-premises, cloud-based, and hybrid solutions, catering to diverse organizational needs. These deployments can occur in both unclassified and classified environments, ensuring the tool meets a wide range of security requirements.

DETECTING THE THREAT

AI Predictive Analysis Model

The AI model is designed to detect potential cyber threats by analyzing vast amounts of data in real-time.

C.O.S.M.O ingests network logs, system events, and threat feeds, analyzing this data to identify patterns, anomalies, and emerging threats.

Predictive analysis provides alerts based on log data and user-set thresholds, helping anticipate and mitigate potential risks before they escalate.

Threat Campaigns offer insights into potential threat campaigns by observing threats over time, allowing for proactive threat management and strategy adjustments.

Contextualization

Threat Intelligence Sources: Each threat intelligence source connected via API is contextualized with STIX II and MITRE ATT&CK frameworks, ensuring comprehensive and standardized threat data.

Enhanced Analysis: This contextualization enhances analysis by providing a structured approach to understanding and mitigating threats based on recognized standards.

“Harness the Power of AI to Predict and Preempt Cyber Threats.”

INTEGRATION

Integration and Operation

The integration of various components ensures smooth operation and effective threat intelligence gathering. This involves synchronizing the backend system, log ingestion tool, and AI model to work together efficiently

STIX II Formatting

The Structured Threat Information Expression (STIX II) standard is utilized for efficient threat data exchange and interoperability. The custom ingestion tool converts raw documents into STIX II format, enabling clear and standardized threat information communication.

AI Model Development

The AI model is trained using extensive datasets, including network traffic, logs, and user behavior data. Advanced machine learning algorithms and neural networks are utilized to detect threats with high accuracy. Effectiveness is demonstrated through performance metrics such as detection accuracy, false positive rates, and response times."

“C.O.S.M.O integrates effortlessly with existing systems, providing enhanced cybersecurity without disrupting your operations.”

9

BENEFITS

Enhanced Threat Detection

C.O.S.M.O significantly improves threat detection capabilities by analyzing vast amounts of data in real-time, identifying patterns and anomalies that traditional methods might miss.

Efficiency and Accuracy

The platform ensures efficient data ingestion and analysis, providing accurate threat intelligence and reducing the cognitive load on human analysts.

Scalability

C.O.S.M.O is designed to scale with the growing volume of threat data, ensuring continuous protection as your organization expands.

Automation and Intelligence

Automation through AI-driven analysis reduces the need for manual monitoring, allowing cybersecurity teams to focus on more strategic tasks.

Customizable Dashboard

C.O.S.M.O features a customizable dashboard that integrates various data points into a cohesive interface for quick assessments and informed decision-making.

Data Sharing

Data can be easily shared across the enterprise via JSON format, Excel, or TXT/CSV, ensuring accessibility and flexibility in handling threat intelligence.

REAL WORLD

Financial Sector

In the financial sector, where the stakes are extraordinarily high, C.O.S.M.O's advanced capabilities are critical. It processes data from network logs, emails, PDFs, and other formats, converting them into a standardized structure that ensures seamless communication and analysis.

This enables financial institutions to detect potential threats early, manage risks proactively, and protect sensitive financial data from breaches and cyberattacks.

With features like predictive analysis alerts and insights into threat campaigns, C.O.S.M.O helps financial firms stay ahead of cybercriminals, safeguarding both their assets and reputation.

Government Agencies

Government agencies, which handle sensitive and classified information, face unique security challenges. C.O.S.M.O's real-time threat detection and comprehensive threat intelligence significantly bolster their defenses.

By integrating AI predictive analysis and utilizing the MITRE ATT&CK framework for contextualizing threat intelligence, C.O.S.M.O provides actionable insights into potential threat campaigns.

This proactive approach allows government agencies to anticipate and mitigate risks before they escalate, ensuring the security and integrity of critical national infrastructure. The customizable dashboard enables quick assessments and informed decision-making, enhancing overall security posture.

Health Care

Healthcare organizations face unique challenges in protecting patient data and ensuring compliance with regulations like HIPAA. C.O.S.M.O addresses these challenges by providing robust threat detection and intelligence capabilities.

Its AI-driven analysis and predictive capabilities enable healthcare providers to identify patterns and anomalies in vast amounts of data, ensuring early detection of malware intrusions and phishing attempts.

The customizable dashboard integrates various data points, allowing for quick assessments and informed decision-making, ultimately protecting patient data and maintaining trust in healthcare services.

Educational Institutions

Educational institutions are increasingly targeted by cyber threats, putting student data and institutional research at risk.

C.O.S.M.O addresses these challenges by offering robust threat detection and intelligence capabilities. Its AI-driven analysis detects malware, phishing attempts, and network anomalies, while the custom log ingestion tool ensures data from various sources is processed efficiently.

> **C.O.S.M.O's** architecture consists of several key components that work together seamlessly to deliver robust threat intelligence and predictive analysis.

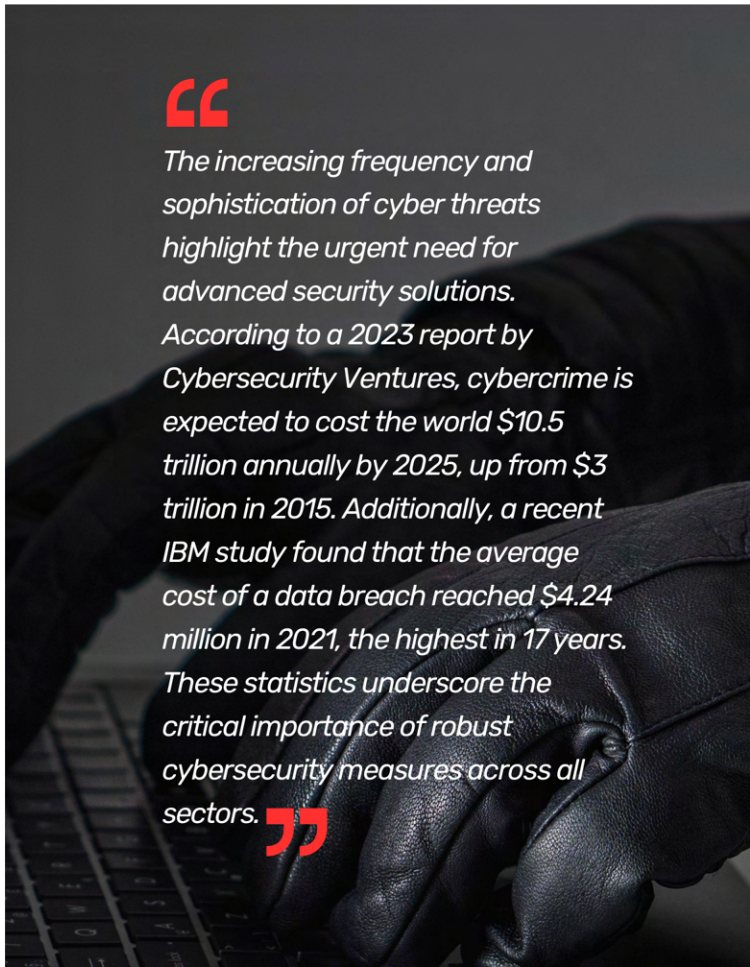
Critical Infrastrucure

Critical infrastructure, such as national power grids, is a prime target for cyberattacks due to the potential for widespread disruption and chaos. Imagine a coordinated attack on a power grid using advanced persistent threats (APTs). C.O.S.M.O's real-time threat detection and AI-driven predictive analysis identify unusual patterns early, allowing for swift action.

As the attack unfolds, C.O.S.M.O enables the cybersecurity team to deploy countermeasures quickly, isolating affected network segments and neutralizing threats before significant damage occurs.

By contextualizing threats with the MITRE ATT&CK framework, C.O.S.M.O helps the team understand the attackers' tactics, improving defense strategies and future preparedness.

This proactive risk management ensures the continuous protection of critical infrastructure, safeguarding national security and maintaining public trust.



> *The increasing frequency and sophistication of cyber threats highlight the urgent need for advanced security solutions. According to a 2023 report by Cybersecurity Ventures, cybercrime is expected to cost the world $10.5 trillion annually by 2025, up from $3 trillion in 2015. Additionally, a recent IBM study found that the average cost of a data breach reached $4.24 million in 2021, the highest in 17 years. These statistics underscore the critical importance of robust cybersecurity measures across all sectors.*

CONCLUSION

C.O.S.M.O is a transformative cybersecurity and AI platform that addresses the growing and sophisticated cyber threats faced by various sectors, including finance, government, education, and healthcare.

By leveraging real-time threat detection, AI-driven predictive analysis, and comprehensive threat intelligence, C.O.S.M.O ensures that organizations can proactively manage risks and safeguard their sensitive data.

The platform's ability to process diverse data sources into the standardized STIX II format ensures clear and actionable threat intelligence, enhancing interoperability and communication.

C.O.S.M.O's robust capabilities enable organizations to detect potential threats early, understand emerging threat patterns, and make informed decisions quickly.

In a landscape where cybercrime costs are projected to reach $10.5 trillion annually by 2025, and the average cost of a data breach continues to rise, C.O.S.M.O provides the necessary edge to stay ahead of cybercriminals.

By integrating advanced AI models and offering a customizable dashboard for quick assessments, C.O.S.M.O empowers cybersecurity teams to focus on strategic initiatives and enhance overall security posture.

In summary, C.O.S.M.O not only fortifies an organization's defenses against evolving cyber threats but also ensures continuous protection and regulatory compliance, making it an indispensable tool in today's digital age.

> *"C.O.S.M.O's AI-driven analysis empowers organizations to detect threats in real-time, proactively manage risks, and safeguard sensitive data, ensuring robust protection against evolving cyber threats."*

13

GLOSSARY

AI (Artificial Intelligence): Technology enabling systems to perform tasks that typically require human intelligence.

STIX II (Structured Threat Information Expression): A standard for sharing cyber threat intelligence.

Log Ingestion Tool: A tool for collecting and processing log data from various sources.

Predictive Analysis: The use of data, statistical algorithms, and machine learning techniques to identify the likelihood of future outcomes based on historical data.

Threat Intelligence: Information that helps organizations understand the risks associated with potential or current threats.

MITRE ATT&CK: A globally accessible knowledge base of adversary tactics and techniques based on real-world observations.

GraphQL: A query language for APIs and a runtime for executing those queries.

ElasticSearch: A search engine based on the Lucene library, used for searching and analyzing data in real-time.

Redis: An in-memory data structure store used for caching.

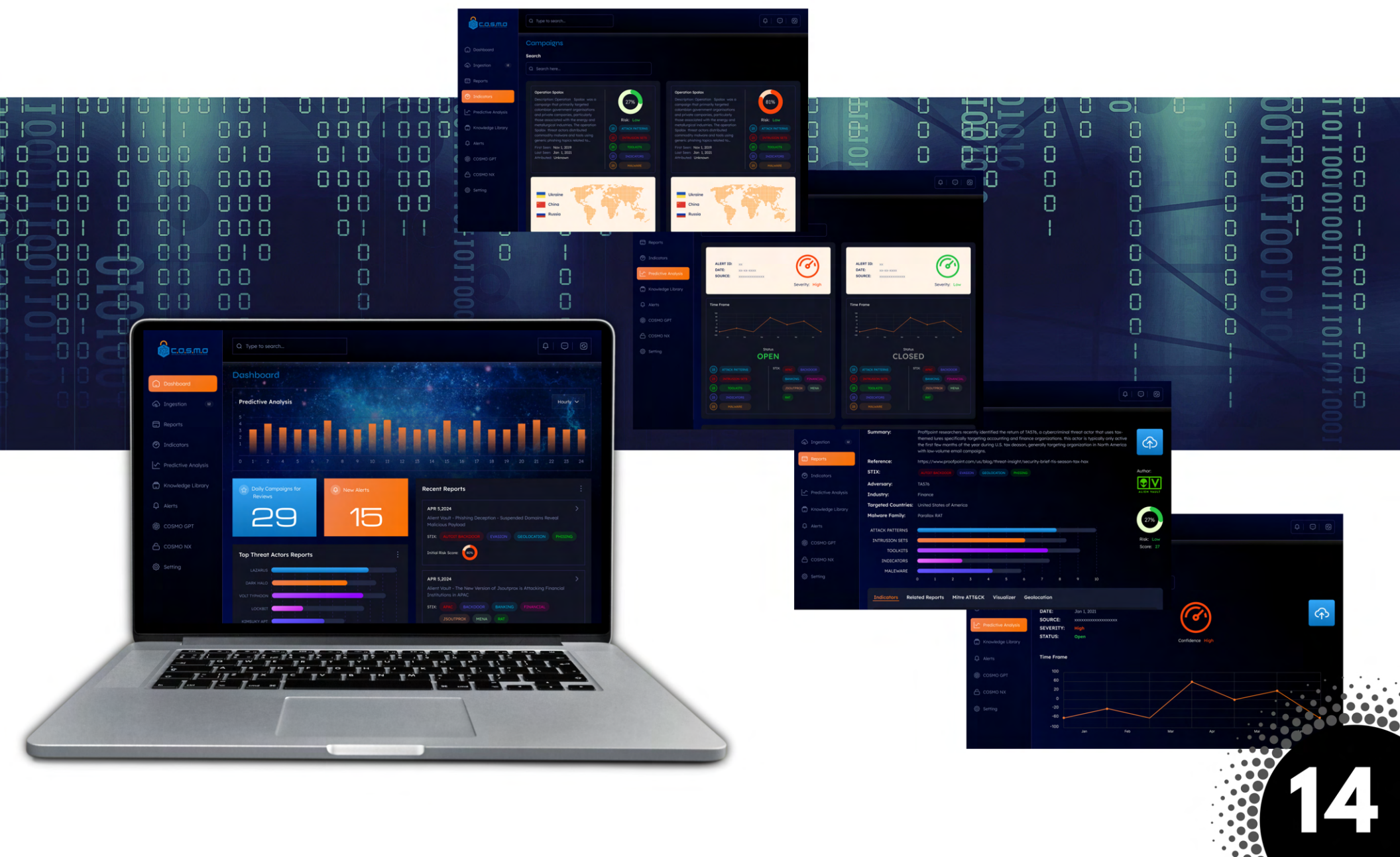
RabbitMQ: A message broker that enables applications to communicate with each other.

Node.js: A JavaScript runtime built on Chrome's V8 JavaScript engine.

React: A JavaScript library for building user interfaces.

TypeScript: A strongly typed programming language that builds on JavaScript.

INTERFACE


c.o.s.m.o
Campaigns
Search
Operation Spalax
Ukraine
China
Russia
Predictive Analysis
ALERT ID:
DATE:
SOURCE:
Severity: High
Severity: Low
Time Frame
Status
OPEN
CLOSED
Dashboard
Ingestion
Reports
Indicators
Knowledge Library
Alerts
COSMO GPT
COSMO NX
Setting
Hourly
Daily Campaigns for Reviews
29
New Alerts
15
Recent Reports
APR 5,2024
Alient Vault - Phishing Deception - Suspended Domains Reveal Malicious Payload
Top Threat Actors Reports
LAZARUS
DARK HALO
VOLT TYPHOON
LOCKBIT
Summary:
Reference:
STIX:
Adversary:
TA576
Industry:
Finance
Targeted Countries:
United States of America
Malware Family:
Parallax RAT
ATTACK PATTERNS
INTRUSION SETS
TOOLKITS
INDICATORS
MALWARE
Indicators
Related Reports
Mitre ATT&CK
Visualizer
Geolocation
Author:
Risk:
Score:
DATE:
SOURCE:
SEVERITY:
STATUS:
Confidence
Time Frame

For more information, contact:
CEO: Joseph Anderson - janderson@cypher-llc.com
COO: Lisa Anderson - landerson@cypher-llc.com
CTO: John Izquierdo - jizquierdo@cypher-llc.com

LEARN MORE AT
cypher-llc.com