C.O.S.M.O

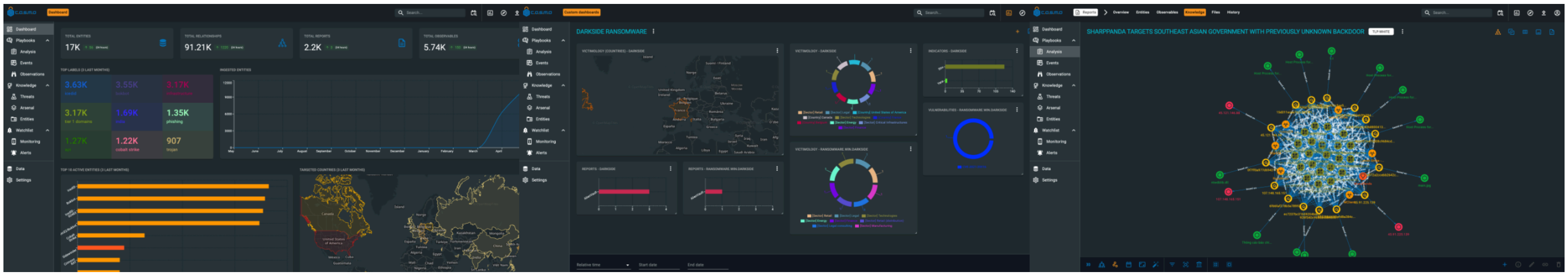
BRINGING ORDER TO CYBER OPERATIONS

WHAT IS COSMO?

A NEXT GENERATION CYBER THREAT INTELLIGENCE PLATFORM BUILT WITH THE CYBER PLANNER IN MIND!

COSMO is an end-to-end threat intelligence platform created to provide cyber planners with detailed information on cyber threats and comparing that to their current network security posture. COSMO does this by utilizing industry standards such as MITRE ATT&CK and STIX to identify a threat with as much detail as possible. Various Threat Intelligence feeds are aggregated into COSMO allowing a single location to view threat information from any threat intelligence source the user chooses to subscribe to. This information allows a cyber planner to take all the information about the threat and create mitigation techniques on their network to prevent a potential attack or stop one currently in progress.

COSMO's Artificial Intelligence and Machine Learning quickly assists with the characterization of a threat by providing the best courses of actions while also providing risk assessments and predicting possible future attacks. COSMO provides all of the collected and assessed threat information in the form of a live playbook which can be shared. As an easy-to-use end-to end solution, COSMO also provides common operating dashboards which can be shared throughout an enterprise environment. Additional functions built into the dashboard allow users to collaborate and task each other with actions or research needed to defend their networks.



Cypher | UNLOCKING SOLUTIONS

CASE STUDY

SOLAR WINDS HACK: At the end of 2020, the biggest news in the Cyber World was the Solar Winds hack where Nation State Actors gained access to networks, systems, and data of thousands of SolarWinds customers. Over 30,000 customers utilized Solar Wind's "Orion" Network Management tool. This allowed Threat Actors to leverage a backdoor to deliver malware through an update to Orion. Unfortunately most of the malware on partners systems such as FireEye, Microsoft, Intel, Cisco and Deloitte were discovered too late. Specifically, Microsoft's own system was being used to further the attack. Even with a "Kill Switch" in place developed by the partner companies, the Threat Actors showed continued persistence with the hack.

HOW COSMO COULD HAVE HELPED!

In the scenario provided, there were known Nation State Threat Actors that utilized malware to disrupt operations and steal data from Solar Wind's customers. There was also a long timeline of events that has taken DoD and DHS months to determine the extent of damage to their cyber mission partners. COSMO's Artificial Intelligence and Machine Learning could have helped in detecting variations of malware early, predicting a threat actors persistence by identifying their TTPs, and predict critical infrastructure vulnerable to persistent attacks, and create a course of action for cyber planners on how to combat the threat early to disrupt their operation. COSMO provides this information within seconds to enable a Cyber Planner to react quickly to identify gaps in security controls along with providing solutions to Offensive and Defensive Cyber Teams.

> *"COSMO IS AN END TO END SOLUTION DESIGNED TO HELP A CYBER PLANNER WITH FAST COLLECTION OF THREAT INTELLIGENCE TO RAPID RESPONSE REDUCING INCIDENT RESPONSE TIME IN A LARGE ENTERPRISE ENVIRONMENT."*

FAST THREAT IDENTIFICATION

DETAILED THREAT ANALYSIS

REDUCED INCIDENT RESPONSE TIME

ARTIFICIAL INTELLIGENCE AT IT'S BEST

THE 5 STEP PROCESS

1

THREAT INGESTION

Use custom APIs from your favorite intelligence feeds, network scans, sensor logs & data, and upload custom threat intelligence documents such as emails, pdf, etc.

2

IDENTIFY AND CHARACTERIZE

Identify and profile threats easily using MITRE ATT&CK framework, STIX II object characterization, custom onsite IOCs, and Threat Actors targeted by your organization.

3

ANALYZE

Analyze and contextualize IOCs, Malware, Threat Actors, Threat Vectors, and Risk Assessments. Create live cyber playbooks detailed with information on the threat and its campaigns along with receiving rapid response options or courses of action.

4

MITIGATE

Create common operating dashboards that can be shared enterprise wide. Use built-in tasking and collaboration capabilities to share live playbook information to any user in your organization for corrective action or research.

5

PREDICT, PROTECT, RESILIENCY

Allow COSMO's proprietary AI and Machine Learning engine to continuously monitor your organization's cybersecurity program by utilizing the NIST Cybersecurity Framework model to determine your organizational 800-53 Rev 5 compliance in relation to security controls and overall security readiness. COSMO’s continuous monitoring process allows for discovery of potential future attacks.

THE COSMO FACTOR

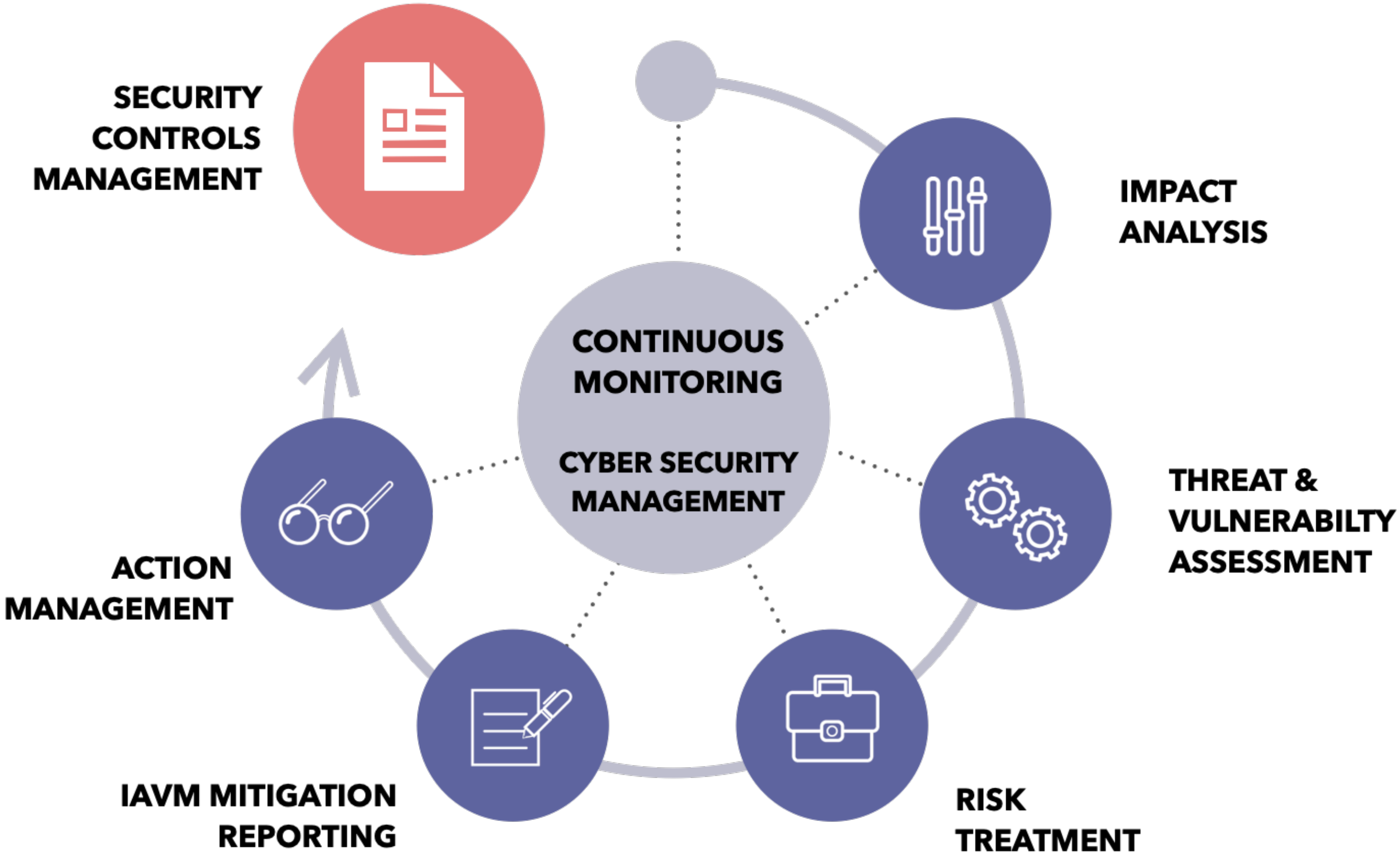
Most Cyber Threat Intelligence Platforms carry a few functions that identify and characterize cyber threats; however, they do not function as an end-to-end solution providing Cyber Planners with the flexible response options or recommended follow up actions once the cyber threats are characterized.

For example, Cyber Planning throughout the DoD consist of manual documentation of cyber threats. The use of paper flow charts to determine what type of threat is occurring mixed with the excessive collaboration through email, phone, and numerous meetings continues to prevent the Defensive and Offensive Cyber Operators from receiving information in a timely manner. This leads to lengthy incident response times.

COSMO provides that end-to-end solution that allows a cyber planner to reduce their response time of collecting threat intelligence all the way to mitigation and protection. COSMO compiles threat information in the form of easy to understand live playbooks with information such as IOCs, Threat Characteristics, TTPs, Campaigns, and known mitigations. This information is easy to share through the use of COSMOs collaboration tools and live playbook sharing capability. COSMO users receive detailed reports on the threat in the form of a Threat Summary along with Rapid Response Options or Courses of Action. As an added bonus, COSMO's AI and Machine Learning leverages the NIST Cybersecurity Framework to learn and provide a snapshot of security control gaps throughout your enterprise.

CONTINUOUS MONITORING

COSMO'S Artificial Intelligence mixed with Cyber Security Management provides planners and analyst with a detailed report of gaps in security controls and IAVM compliance.


SECURITY CONTROLS MANAGEMENT
IMPACT ANALYSIS
CONTINUOUS MONITORING
CYBER SECURITY MANAGEMENT
THREAT & VULNERABILTY ASSESSMENT
ACTION MANAGEMENT
IAVM MITIGATION REPORTING
RISK TREATMENT

DEVELOPMENT TIMELINE

CURRENT FEATURES

Threat Ingestion/Data Capture
Threat Dashboards
Rapid Response Playbooks
Threat Profile Identification
Threat TTPS
Geo Mapping Location of Threats
Live Threat Feeds
Advanced Persistent - Threat (APT) Network Visualization
Threat Analysis/Real-Time - IOC Events
Create Campaign Events
Collaboration
Rapid Response Options

2021 Q3

Q3 RELEASE

Risk Assessment and Management Module
Continuous Monitoring
DCO Targeting
Operational Deconfliction

2022 Q1

2022 Q1 RELEASE

ML and AI
Machine Analytics
Impact Assessments
Threat/ Intel Reports
Integration CTI Security Operations
Behavioral Analysis
Any New Customer Requirements