C.O.S.M.O

CYBER OPERATIONAL SECURITY MANAGEMENT OPTIMIZER

Cyber Threat Intelligence Planning and Analysis Platform

CYPHER LLC
cypher-llc.com
CEO: Joseph Anderson - janderson@cypher-llc.com
Sales Engineer: Ray Ally - rally@cypher-llc.com
44679 Endicott Drive, Suite 314
Ashburn, VA 20175
Phone: 571.206.1401

The Problem

Cyber threat actors take advantage of organizations that have poor cyber planning disciplines, disorganization, disjointed tools, employee turnover, weak processes, and mission complacency. The attackers conduct persistent campaigns against these organizations because the adversary has determined that the target can be exploited based on the vulnerabilities that exist and slow response times by the organization. The timeline below provides a real-world example of a cyber threat actor executing old and newer techniques with persistent campaigns versus the poor incident reaction times of cyber planners and analyst attempting to respond.

CYBER THREAT CAMPAIGN TIMELINE

APT 1 (China) - APT 29 (Russia) - APT 33 (Iran)

Cyber Planners and Analysts

MALICIOUS ACTIVITY

Threat Actors utilize TTPS, malware, vulnerability exploits, zero day, phishing, password attacks, bot nets, ransomware, man in the middle attacks, and more to gain access to critical information.

Cyber Analysts and Planners conduct extensive research and collaborate with cyber partners to create mitigation techniques, and plan for the cyber threat. This process can take anywhere from weeks to months while the threat actor is successfully gaining access to vulnerable information. Unsuccessful mitigations, lack of threat knowledge and historical data, and lengthy collaboration processes allow for threat actors to easily access sensitive data and compromise of critical infrastructure.

COMPROMISED DATA

Threat Actors will now take advantage of the extracted data and slow incident response times to adjust their techniques to conduct persistent attacks over the years. Efforts are doubled in attempt to gain access from previously failed efforts, and new techniques are deployed along with older techniques creating an overwhelming persistent attack.

MEANWHILE.....

MALICIOUS ACTIVITY WITH NEW TECHNIQUES

Cyber Planners and Analysts are still working on the previous attacks by manually searching for historical knowledge, conducting extensive meetings to discuss the attacks, researching multiple threat intelligence tools, and creating duplication of efforts along the way. The slow incident response times, mixed with the lack of proactive planning, creates a vulnerability in itself that allows a cyber threat actor to benefit from this disorganization.

MORE COMPROMISED DATA

Cyber threat actors continue to gain access to even more data due to planners and analysts maintaining poor incident cyber planning disciplines mixed with lengthy incident response times.

The Solution

COSMO was created with the sole focus on shifting the paradigm of the cyber operational environment from a reactive and disjointed approach to a proactive defensive tempo by providing a platform that follows an organized kill-chain process, integrates disparate cyber threat intelligence feeds, provides historical data, trends, attack patterns in one central location, and empowers the cyber analyst with courses of action to mitigate and halt threat penetration.

COSMO is the new force multiplier that introduces an enhanced visibility of the Cyber Intelligence Preparation of the Battlefield (CIPB) through its predictive capabilities utilizing AI and Machine Learning. **COSMO** enables the analyst to plan against future attacks thus improving the response time during zero day attacks. Additionally, **COSMO** eliminates stove pipe mission partnerships and encourages collaboration and communication across an enterprise which is critical to defend against the adversary.

WITHOUT COSMO

Resources and Processes Utilized:

- Multiple planners and analysts
- Multiple threat intelligence sources with varied information
- Manually created SharePoints
- Research from multiple threat sources discussing overlapping information
- Constant emails between cyber partners and agencies
- Paper flow charts to determine risk assessment
- Multiple cyber conferences and meetings to collaborate and discuss incident response and mitigation strategy
- Paper flow charts to determine risk assessment
- IOCs and technique sharing through text or pdf files via email
- IOC blocking that does not prevent the enemy from pivoting their strategy

WITH COSMO

Resources and Processes Created:

- Cyber planners and analysts access one unified platform that contains aggregated intelligence
- Historical information prevents overlap and research duplication efforts
- Multiple conferences, emails, and phone calls are eliminated with easy to share dashboards and centralized playbooks
- Reduced incident response times with quickly discovered TTPs and recommended courses of action
- 2D/3D visuals how a threat moves through a victims network
- Initial risk scoring to determine threat level
- Easy IOC and mitigation technique sharing
- Predictive Analysis, AI, and Machine Learning to help determine early warning signs of an attack

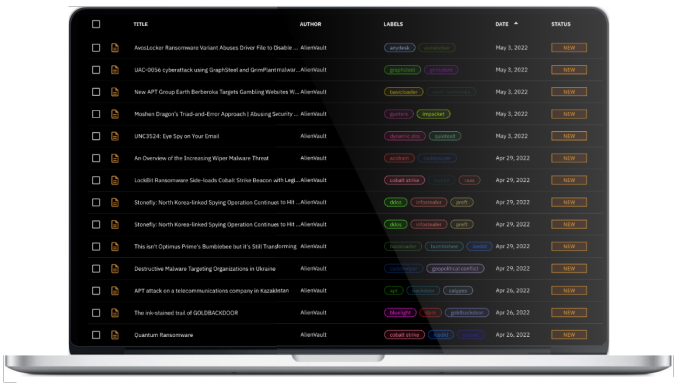
COSMO is a **"one-stop" cyber threat intelligence platform** created to provide detailed information on cyber threats, and compare them to their current network security posture. We use Artificial Intelligence and Machine Learning (AI/ML) to characterize a threat, recommended courses of action and provide initial risk assessments while predicting possible future attacks. **COSMO** has common operating dashboards that can be shared throughout an enterprise environment which allows users to view one common operating picture and view cyber threat statistics.

Threat Ingestion

COSMO automatically ingests reports from various sources such as Mandiant (FireEYE), Crowd Strike, Alien Vault, and Record Future.

Users can manually create their own reports utilizing threat information captured from emails, PDFs, sensor or network data, and text files. Ingested information is presented with easy to read dashboards displaying various captured threat information statistics.

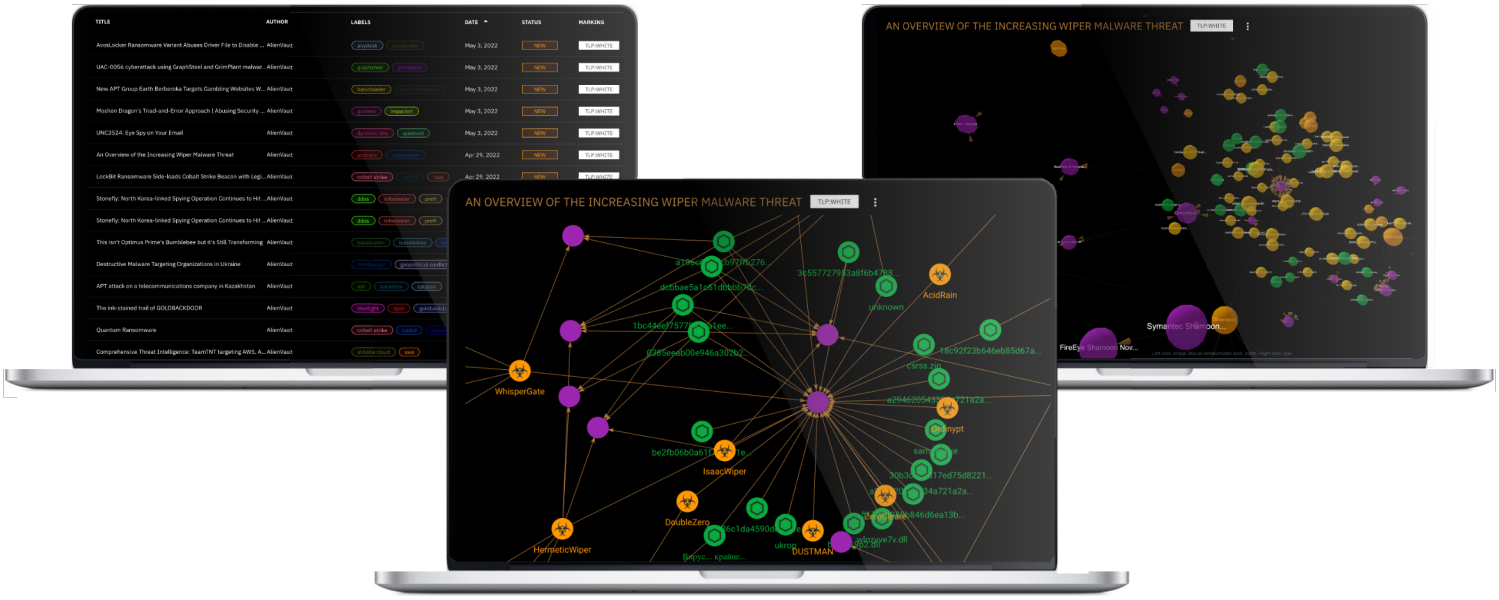
COSMO uses industry standards such as MITRE ATT&CK, STIX II, YARA, and TAXII to characterize and share threat indicators throughout automatically ingested reports, sensor or log data, or information manually ingested by users. Characterized information is displayed with easy to read tags as you review analyzed reports or cyber threat playbooks along with quick risk identification tools.



MITRE ATT&CK STIX TAXII YARA

Analyze

COSMO analyzes all ingested information, and creates a visual workflow for user review. Information is displayed utilizing cyber threat overviews/definitions, indicators, TTPs, malware kits, kill chain phases, campaign timelines, and much more. 2D and 3D graphs, and MITRE's threat matrix within **COSMO** help the user visualize how a threat actor moves through cyber space.

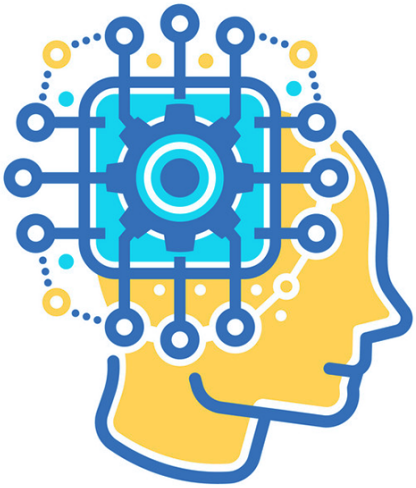


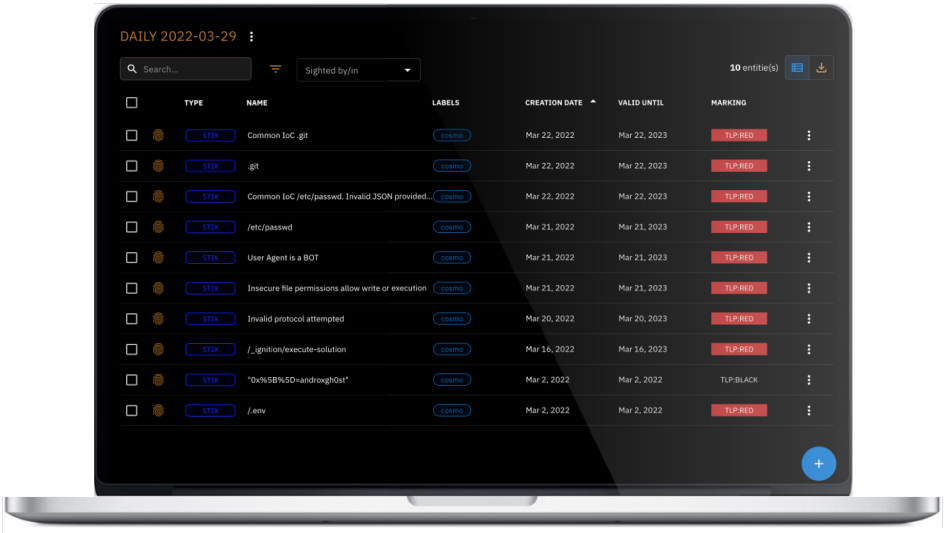
Mitigate

COSMO aggregates information into centrally located cyber playbooks containing detailed historical data on each threat actor. Playbook dashboards that are automatically created by **COSMO** can be easily shared through your enterprise allowing you to quickly share emerging threats and recommended courses of action. You can also export relevant threat statistics, indicators, and visual 2D/3D threat movement charts into pdfs, or text files.

Predictive Analysis (AI and Machine Learning)

COSMO utilizes proprietary predictive analysis tools along with Artificial Intelligence and Machine Learning to continuously monitor your network traffic and identify potential cyber threats. Daily reports will be delivered providing users with a list of analyzed threat indicators or malicious activity enabling your enterprise to take immediate recommended mitigation steps.





For more information, contact us at....
Joseph Anderson: janderson@cypher-llc.com
Ray Ally: rally@cypher-llc.com.

Visit our youtube link to see a quick demonstration of **COSMO** in action.

YouTube https://www.youtube.com/watch?v=7d2K9UpmKFU