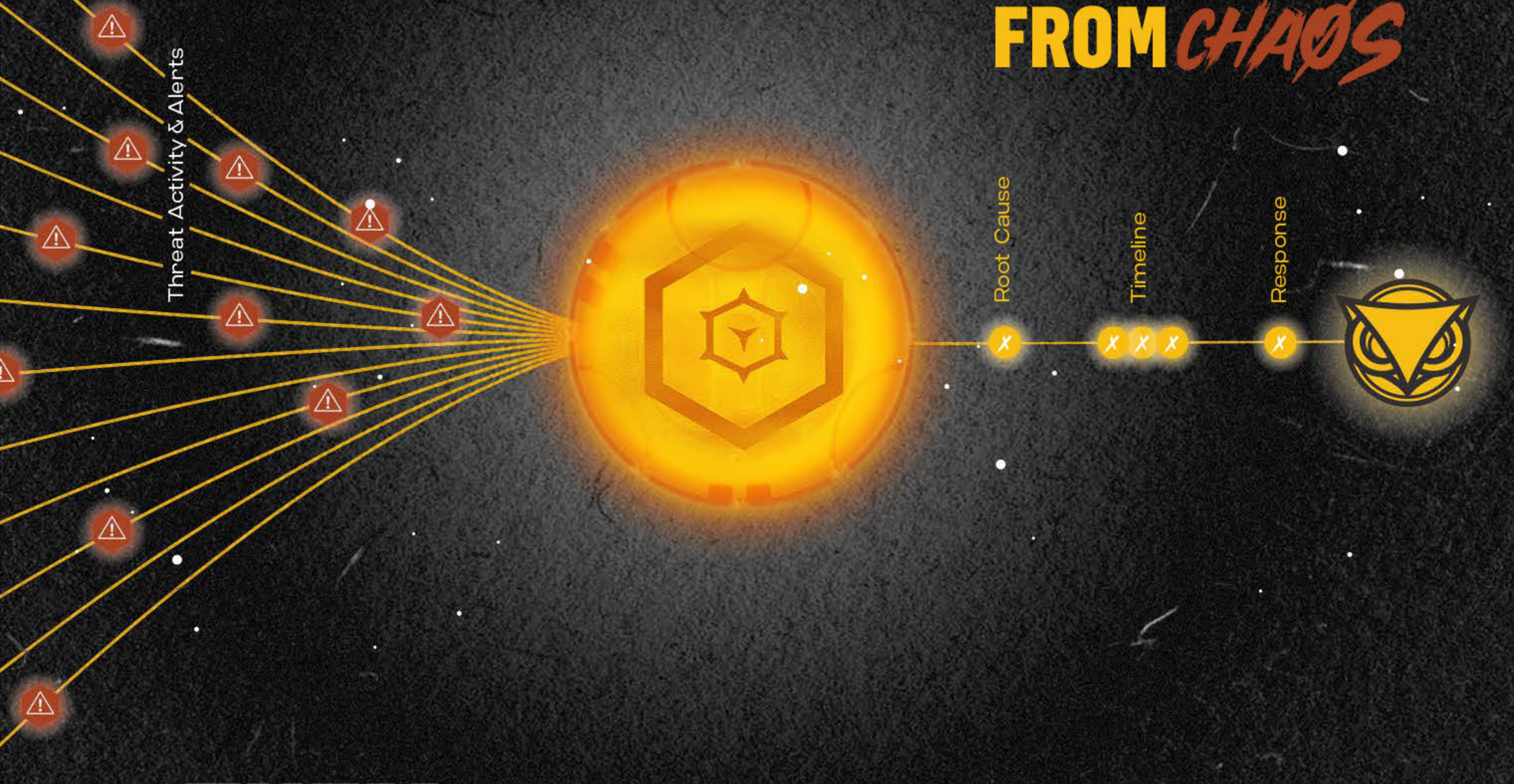
THE MALOP™

Cybereason's primary differentiator is the ability to consolidate alerts into a single operation. Cybereason makes sense of complex data relationships and behaviors to stitch together the separate components of an attack, including all users, devices, identities, and network connections into an operation-centric view we call The MalOp™.

CREATE ORDER FROM CHAOS



THEM

ALERT DOZENS OF TIMES
for a single intrusion, creating unnecessary noise

GENERATE FALSE POSITIVES,
overwhelming teams

BURDEN WITH SLOW MANUAL PROCESSES,
lengthening MTTR

CYBEREASON

DRIVE UNPARALLELED EFFICIENCY WITH THE MALOP™

ALERT CONSOLIDATION

Cybereason's operation-centric approach means the full attack story from A-Z is contained in a single screen, including all impacted users and devices. Our unique understanding of data relationships means full context accompanies every detection within the MalOp™.

HIGH FIDELITY DETECTIONS

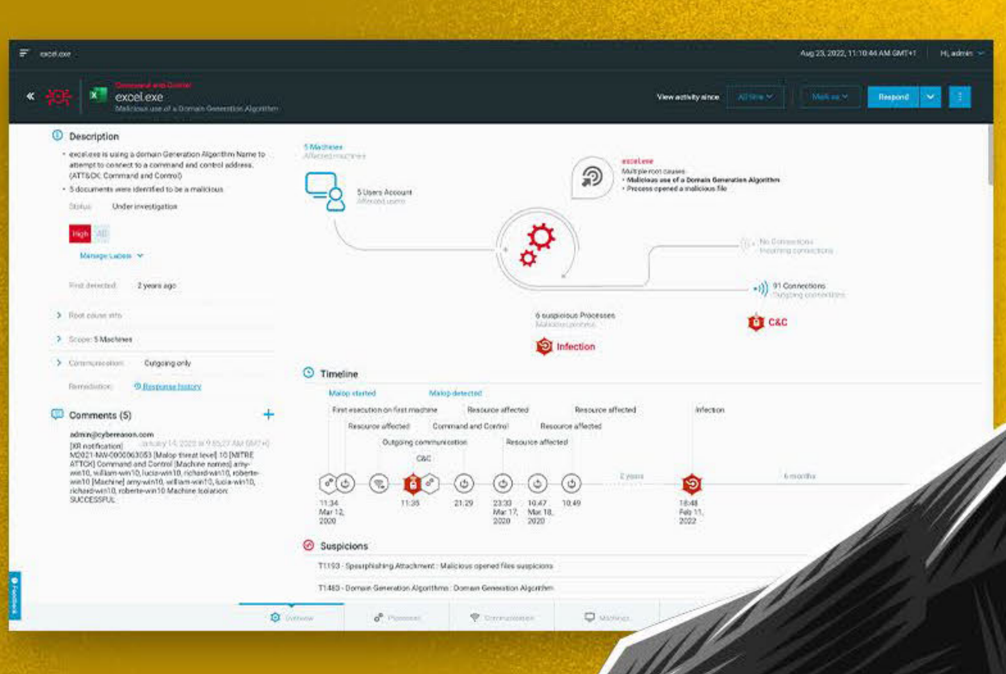
Cybereason builds detections based on chains of behaviors that are convicted into a MalOp™ after the level of maliciousness rises to become a verified alert, dramatically reducing the burden of false positives

AUTOMATION

Orchestrate and automate response to all impacted users and endpoints. Automation means reduced MTTR and extra bandwidth for security analysts.

cybereason®

Every MalOp™ contains root cause, attack timeline, scope of the operation, inbound and outbound connections, tools used by the attacker, threat intelligence, and tailored response playbooks.



MALOP™ CAPABILITIES

MALOP™ DETECTION ENGINE

The MalOp™ Detection Engine is the industry's leading data analysis engine. We process data on a planetary scale and stitch together all varying components of an intrusion by applying machine learning, behavior-based detection, and a host of other techniques to uncover advanced adversaries and the full scope of their operation.

THREAT INTELLIGENCE

Every detection is enriched with Nocturnus insights, embedded intelligence from a host of sources, MITRE ATT&CK tagging, and the ability to integrate 3rd party threat intelligence feeds to create additional context for rapid decision making.

DIGESTIBLE UI

Junior security analysts are immediately upleveled via our intuitive UI. Small teams can do the work of large teams, and historically complex tasks like DFIR, Threat Hunting, and Investigation are made available to Tier I analysts, with more advanced modules available to Tier III when needed.

XDR ENRICHMENTS

Enrich detections with relevant data from identity sources, workspace solutions, SaaS applications, cloud sources and more. Create a single point of visibility, detection and response across the enterprise.

DEEP DIVE OPTIONS

Pivot the investigation any which way and dive deep into nearly any aspect of the MalOp™ for a detailed view of all data that went into the conviction of a MalOp™.

AUTOMATED RESPONSE

The MalOp™ sees the full picture of the attack, and we take it a step further and populate tailored response playbooks that remediate the complete intrusion in one fell swoop. Orchestrate and automate response in-platform.

BENEFITS

QUICKLY UNDERSTAND & REMEDIATE AN INTRUSION

BOOST OPERATIONAL EFFICIENCIES BY 10X

INCREASE ANALYST BANDWIDTH & PRODUCTIVITY
in order to spend cycles on other tasks

AUTOMATE AWAY REPETITIVE & MUNDANE TASKS
& use human intervention only for critical decisions

LEVERAGE THE MOST EFFECTIVE DETECTION SOLUTION
in the history of MITRE ATT&CK results to leave no stone unturned

LEARN MORE ABOUT THE MALOP™

Request A Demo

ABOUT CYBEREASON

Cybereason is the champion for today's cyber defenders with future-ready attack protection that extends from the endpoint to the enterprise, to everywhere. While every other security solution is alert-centric, Cybereason is operation-centric. We empower defenders to instantly visualize MalOps from root cause to every affected endpoint with real-time, multi-stage displays of all attack details. This gives you the power to end attacks with a single click.
Learn more at cybereason.com/why-cybereason

cybereason®