ANOMALI®

Partner Data Sheet

CYBERSPONSE
ADAPTIVE SECURITY

CyberSponse, Inc.

INDUSTRY
Security Orchestration & Automated Response (SOAR)

WEBSITE
https://CyberSponse.com/

COMPANY OVERVIEW
CyberSponse is the leading provider of automated incident response and enterprise incident management for cybersecurity threat management. The CyberSponse patented technology platform dramatically improves the efficiency of daily SecOps team's response and remediation against cyber-attacks. The platform provides a centralized technology for managing, monitoring, mitigating, reporting, and analyzing an organization's entire incident response process.

PRODUCT OVERVIEW
The CyberSponse platform easily integrates with all cybersecurity tools and stays up-to-date with the latest technology (malware analysis, threat intelligence, IDS, IPS, End Point, SIEM, etc.). The CyberSponse platform has the ability to easily connect all security technologies (via connector store) into a single centralized platform, acting as an interpreter and orchestrator to assign tasks for the team to complete and generate API based actions or instructions for cybersecurity tools to perform automatically.

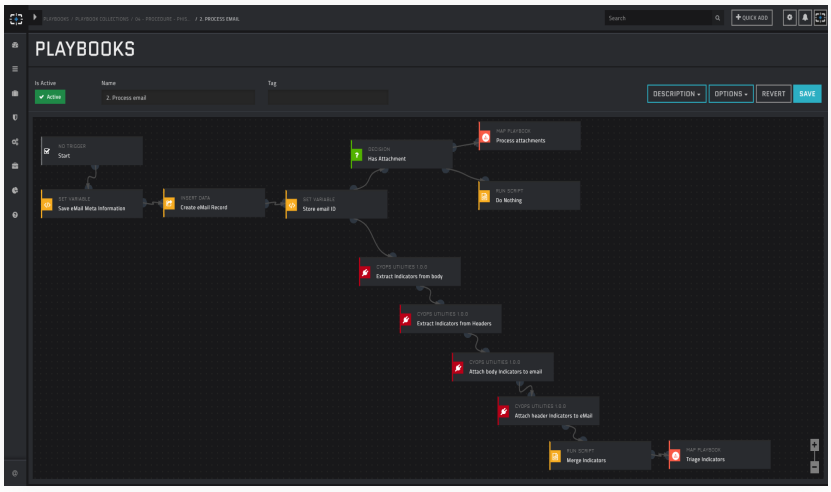
SOLUTION HIGHLIGHTS
- Automated Incident Response
- Enterprise Case Management
- Vulnerability Management
- Reporting and Metrics

The Need for Adaptive Security

Organizations today face an unmanageable level of known and unknown threats, all of which are evolving at an unprecedented rate. Security operators looking to identify which threats require immediate remediation are quickly inundated with an overwhelming number of alerts. Organizations need adaptable security solutions and processes that will help them rapidly assess, understand, and respond to evolving threats.

Solution

The CyberSponse platform provides users with automated playbooks tailored to their specific cybersecurity tools and environments. Through easy drag and drop integrations with existing cybersecurity solutions, CyberSponse aggregates alerts and contextualizes these alerts with external threat intelligence from the Anomali ThreatStream® platform. This unique combination provides analysts with an effective means to prioritize alerts, assign tasks and properly track all alerts and incidents. Analysts can easily research the highest priority alerts in ThreatStream to further refine their understanding of the threats, equipping them with new intelligence to develop automated and semi-automated response actions within the CyberSponse platform. As organizations continue to utilize the platforms in tandem, newly generated intelligence will empower security teams with improved responses.



Both the CyberSponse and Anomali ThreatStream platforms are modular and designed to grow and mature with evolving security programs. As additional tools are acquired, these platforms can be quickly integrated into existing workflows and playbooks to ensure immediate value on investment. Out of the box threat feeds from Anomali and playbooks from CyberSponse enable users to instantly research and respond to threats.

808 Winslow Street, Redwood City, CA 94063 USA
1-844-4-THREATS | info@anomali.com | www.anomali.com

BENEFITS OF ANOMALI

- Easy-to-use interface to view threat information received through STIX/TAXII feeds
- Analyze and correlate data into actionable information: SIEM rules, reports, and dashboards
- Pinpoint IOCs – quickly search for a specific indicator, search for an indicator type over a time range, and drill-down into details
- Eliminate unnecessary, duplicative and irrelevant indicators – before they enter your infrastructure
- Identify and prioritize the events that matter now – without DIY scripting
- Machine learning algorithms scale to accommodate thousands of IOCs per minute across your environment

BENEFITS OF CYBERSPONSE

- Save thousands of labor-hours and expensive budgets on incident response and remediation efforts
- Tool-agnostic, enabling security operations centers to integrate and orchestrate all their current tools without displacing or requiring any new tool purchases
- The only security orchestration and automation platform offering that is part of the Incident Response Consortium, a non-profit community of incident responders collaborating and offering open source playbooks, runbooks, connectors and incident response plans
- Communicate and collaborate promptly and effectively even when significant infrastructure components such as power or the Internet are compromised
- Keep senior management and executives informed of current incidents with customizable reports

Benefits of the joint offering

Threat Intelligence coupled with Security Orchestration & Automation provides an enterprise platform for security operators to confidently automate workflows and playbooks and orchestrate incident response efforts. This integrated combination allows operators to take action and prioritize security alerts at a fraction of the conventional time previously required with manual efforts.

Improved Response

Enriched contextual data can be constructed into mature incident response plans and playbooks. No more analyst burn-out or false positives, no more hassles with "too many alerts, not enough time." These advanced plans and playbooks drastically reduce time from alert to resolution and mitigate a major problem in security today - time and resources.

Integrated Workflows

Data from disparate sources is combined into a single comprehensive format and quickly passed between tools with little human intervention. This eliminates repetitive actions across platforms and promotes automation of playbooks for high speed incident response.

About Anomali

Anomali® detects adversaries and tells you who they are. Organizations rely on the Anomali Threat Platform to detect threats, understand adversaries, and respond effectively. Anomali arms security teams with machine learning optimized threat intelligence and identifies hidden threats targeting their environments. The platform enables organizations to collaborate and share threat information among trusted communities and is the most widely adopted platform for ISACs and leading enterprises worldwide. For more information, visit us at www.anomali.com and follow us on Twitter @Anomali.

About CyberSponse

CyberSponse is the only patented automated incident response platform that fills the gap between automation-only and human dependent security organizations. The CyberSponse Operations Platform permits the automation of hundreds of security tools within a single incident management, case management and analysis console for easy use and rapid remediation. CyberSponse is backed by a team of self-made entrepreneurs looking to disrupt the security industry with true grit, hard work, hustle and precision execution. For more information visit www.CyberSponse.com or follow us on Twitter @CyberSponse.

ANOMALI®
808 Winslow Street, Redwood City, CA 94063 USA
1-844-4-THREATS | info@anomali.com | www.anomali.com