CYCOGNITO

SOLUTION BRIEF

CyCognito + Cortex XSOAR

The Challenge

You're faced with adapting to a dynamic threat landscape, evolving adversary tactics, evolving business demands and an overwhelming volume of security tasks— and your existing security technologies can't keep up. Analysts waste time pivoting across consoles for data collection, determining false positives, and performing repetitive, manual tasks throughout the lifecycle of an incident.

To meet these new challenges and reduce mean-time-to-detect, modern security teams need data-driven capabilities, contextual business-centric insights, and timely and accurate threat detection techniques. As they face a growing skills shortage, security leaders deserve more time to make decisions that matter, rather than drown in reactive, piecemeal responses.

At CyCognito, we believe all cyber risk is business risk - we empower security teams to see their attack surface the way attackers do and work with partners that make identifying and fixing the most critical security issues seamless.

The Solution

Together, CyCognito and Cortex XSOAR empower companies to take control of external risk and attack surface management by unifying automation, case management, real-time collaboration, and threat intelligence management. Teams can manage alerts across all sources, standardize processes with playbooks, take action on threat intelligence, and automate response for any security use case.

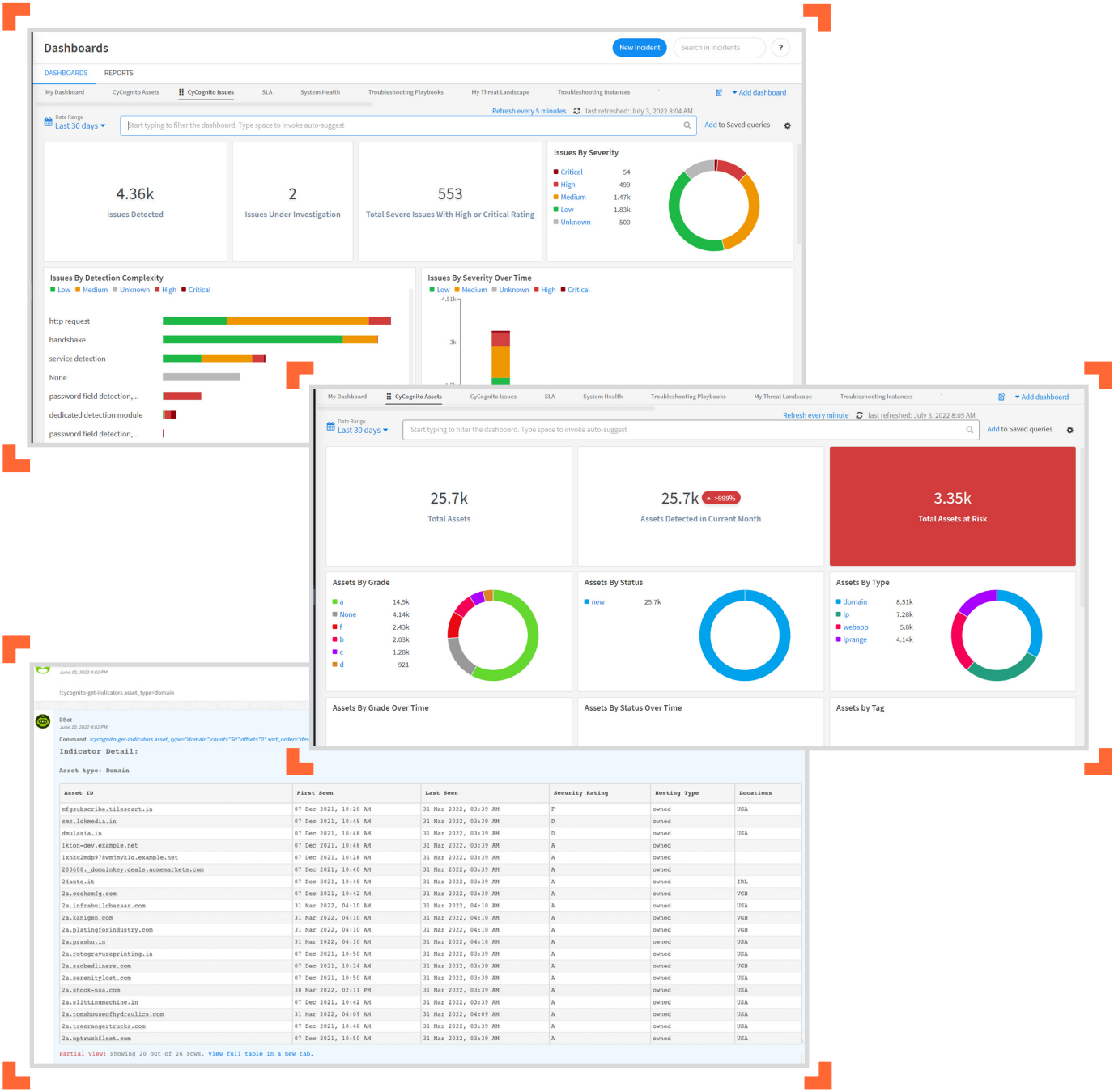
Integrating asset and vulnerability data from CyCognito into Cortex XSOAR allows security teams across the organization visibility into external assets and issues they may not have otherwise known existed. Security Operations teams can easily be alerted to these new threats – complete with step-by-step exploitation instructions to validate risk, safe sandbox to simulate attacks, and indicators of compromise (IOCs) – and use integrated features to decrease your MTTR, ensuring your enterprise is protected from future attacks

Key features of CyCognito External Risk Management

- **Graph business and asset relationships** – Find all of your exposed assets and easily determine which business unit or team owns them
- **Provide business context with evidence** – Evaluate risk by determining the business purpose and data residing in each asset, complete with automated comprehensive evidence empowering validation and satisfying auditor requirements
- **Continuous multi-factor security testing at scale** – Automatically detect risk and validate potential attack vectors across your entire external IT ecosystem: SaaS, subsidiaries, interconnected third-parties, and event IaaS
- **Security issue identification and prioritization** – Commercial-grade vulnerability scanning, pen test maneuvers, DAST (dynamic application security testing), weak credentials, authentication bypass, configuration issues and more identifies top issues and the path to remediating them
- **Faster remediation** – Close the window of attack in days versus months, which reduces breach likelihood

Key Benefits of Cortex XSOAR

- **Scalable, consistent incident response** – Speed up deployment with hundreds of out-of-the-box (OOTB) playbooks covering a wide range of security use cases (e.g., phishing prevention, IOC enrichment, cloud security) or use the powerful software development kit to build your own integrations.
- **Modular, customizable playbooks** – Address simple use cases and complex, custom workflows using a visual drag-and-drop playbook editor with thousands of executable actions. Playbook blocks/tasks can be nested and reused across playbooks. Real-time editing, a playground for testing playbooks, and YAML-based sharing make playbook creation quick and easy.
- **Perfect balance of automation and human response** – Maintain control over automated processes with manual approval tasks available as part of any playbook.
- **Orchestration across the product stack** – Automate incident enrichment and response across more than 500 integrations with data enrichment tools, threat intelligence feeds, SIEMs, firewalls, EDRs, sandboxes, forensic tools, messaging systems, and more.



Joint Solution Benefits

- **Tightly integrated solution** feeds relevant, context rich data into Cortex XSOAR for faster, more precise threat detection and response using new and existing playbooks
- **Pre-built dashboards** provide visibility and access to your externally facing assets and vulnerabilities
- **Supercharge investigations** with built-in, high-fidelity risk intelligence from the CyCognito platform
- **Boost collaboration and reveal critical threats** by layering CyCognito risk and threat intelligence with internal incidents to prioritize alerts and make smarter response decisions
- **Easily identify** asset owners and responsibility to remediate with CyCognito's fully contextualized attack surface map

About CyCognito

We are CyCognito, a revolutionary new approach to external cyber risk management driven to create positive business impact. Far deeper than external attack surface management, our platform helps organizations identify, understand and master their risk in profound new ways.

Fully-automated, highly scalable, and designed to function as promised, our platform uses advanced machine learning and natural language processing to allow for unprecedented reach, speed and accuracy. We can step into the shoes of potential attackers—which in turn helps us identify and secure gaps better than anyone. We help teams secure their attack surface by helping them determine true risks, where they need to focus and how they should invest. And then we use what we learn to help bridge cyber risk remediation across departments unlike ever before.

About Cortex XSOAR

Cortex XSOAR, a Palo Alto Networks company, is the only Security Orchestration, Automation, and Response (SOAR) platform that combines security orchestration, incident management, and interactive investigation to serve security teams across the incident lifecycle. With Cortex XSOAR, security teams can standardize processes, automate repeatable tasks, and manage incidents across their security product stack to improve response time and analyst productivity.

Ready to learn more about how Cortex XSOAR and CyCognito can help your security team gain the real-world experience and skills needed to manage your attack surface and defend against advanced cyber threats? Contact sales@cycognito.com.

To learn how the CyCognito platform uniquely helps you identify and prioritize the paths of least resistance into your IT ecosystem, so that you can eliminate them, visit **cycognito.com**.

CYCOGNITO