CYCOGNITO

SOLUTION BRIEF

CyCognito + Splunk

The Challenge

You're faced with adapting to a dynamic threat landscape, evolving adversary tactics, advanced threats and evolving business demands — and your existing security technologies can't keep up.

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. Security teams can more quickly detect, investigate, and respond to attacks when all their machine data is centralized and utilized.

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 Splunk empower companies to take control of external risk and attack surface management by identifying critical security risks and correlating them with events seen within the Splunk platform. With CyCognito's attacker's perspective combined with features like Splunk's Risk-Based Alerting, security teams can detect and react to more threats while drastically reducing the number of false positives they experience.

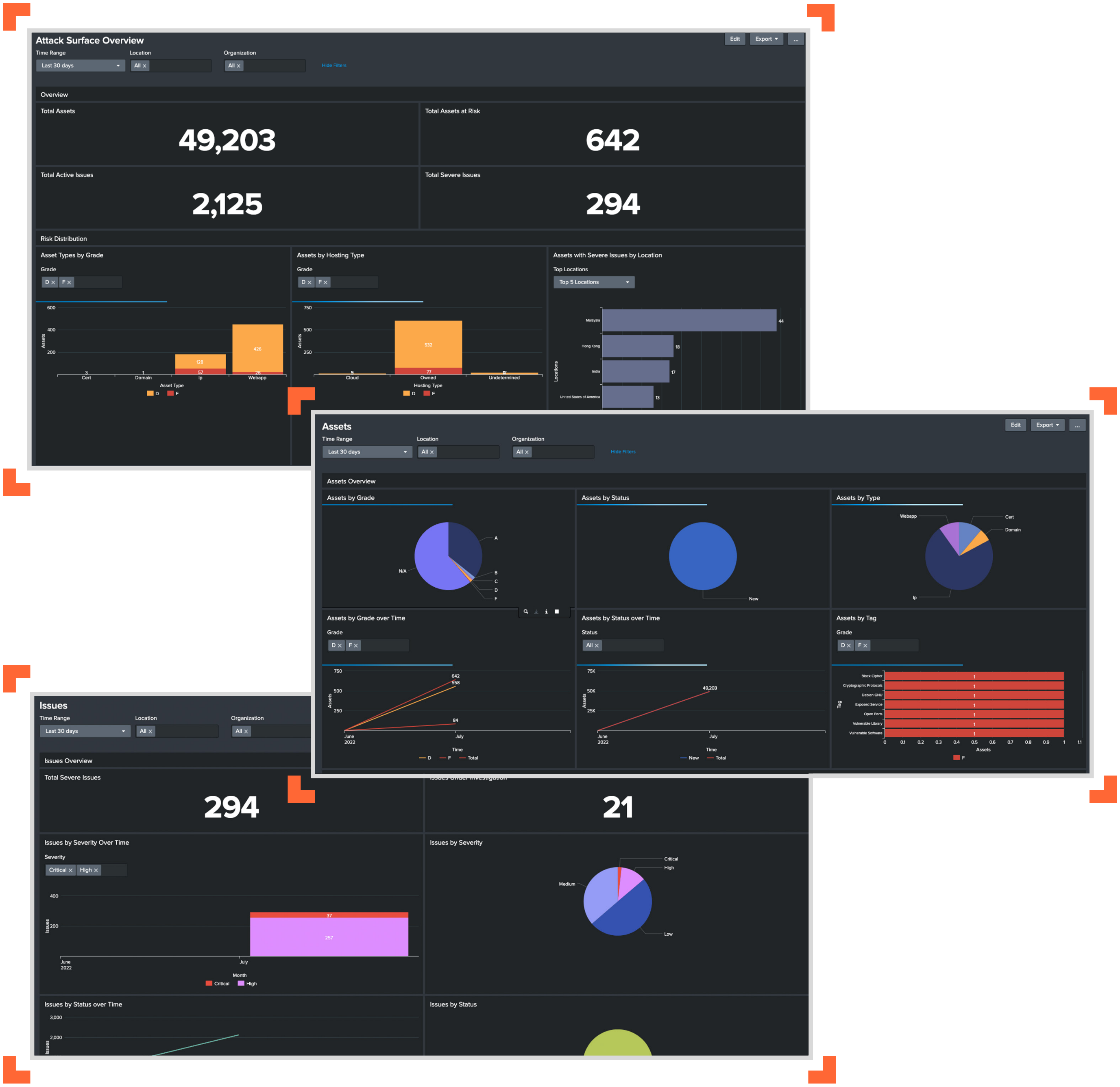
Integrating asset and vulnerability data from CyCognito into Splunk automatically sends the highest risk issues to the Splunk SIEM. Dashboards provide security teams across the organization visibility into external risks they may not have otherwise known existed. Security Operations teams can easily 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 Use Cases for Splunk Enterprise and Splunk Cloud

- **IT business operations** – Splunk provides real-time monitoring, event management and alerting, and visibility into the health of physical and virtual IT infrastructure. Splunk also provides monitoring of applications and business and IT services.
- **Security and compliance** – Splunk speeds security investigations through real-time monitoring, historical analysis, and visualization of massive datasets. Security teams can perform comprehensive incident investigations and create ad hoc reports in minutes.
- **Business analytics** – Splunk opens a window into complex business processes, customer behavior, product usage, and digital marketing campaigns. Businesses seeking to drive more revenue through their websites or mobile apps can gain timely and relevant business insights.
- **IoT and industrial data** – Splunk enables you to monitor operations, analyze usage, and integrate insights into an end-to-end view of business operations. Splunk accomplishes this feat by using data that is generated by connected devices, control systems, sensors, supervisory control and data acquisition (SCADA) systems, and more.



Joint Solution Benefits

- **Tightly integrated solution** feeds relevant, context rich data into Splunk Enterprise, using features like risk-based alerting to provide faster, more precise threat detection and response
- **Pre-built dashboards** provide visibility and access to your externally facing assets and vulnerabilities
- **Advanced search features** help to pinpoint issues contributing to organizational risk and exposure
- **Contextualized, enhanced alerts** for external assets
- **Automated workflows** using Splunk alerts can be triggered from changes to your external attack surface

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 Splunk

Splunk is the world's first Data-to-Everything Platform designed to remove the barriers between data and action, so that everyone thrives in the Data Age. Splunk empowers IT, DevOps and security teams to transform their organizations with data from any source and on any timescale.

Ready to learn more about how Splunk 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