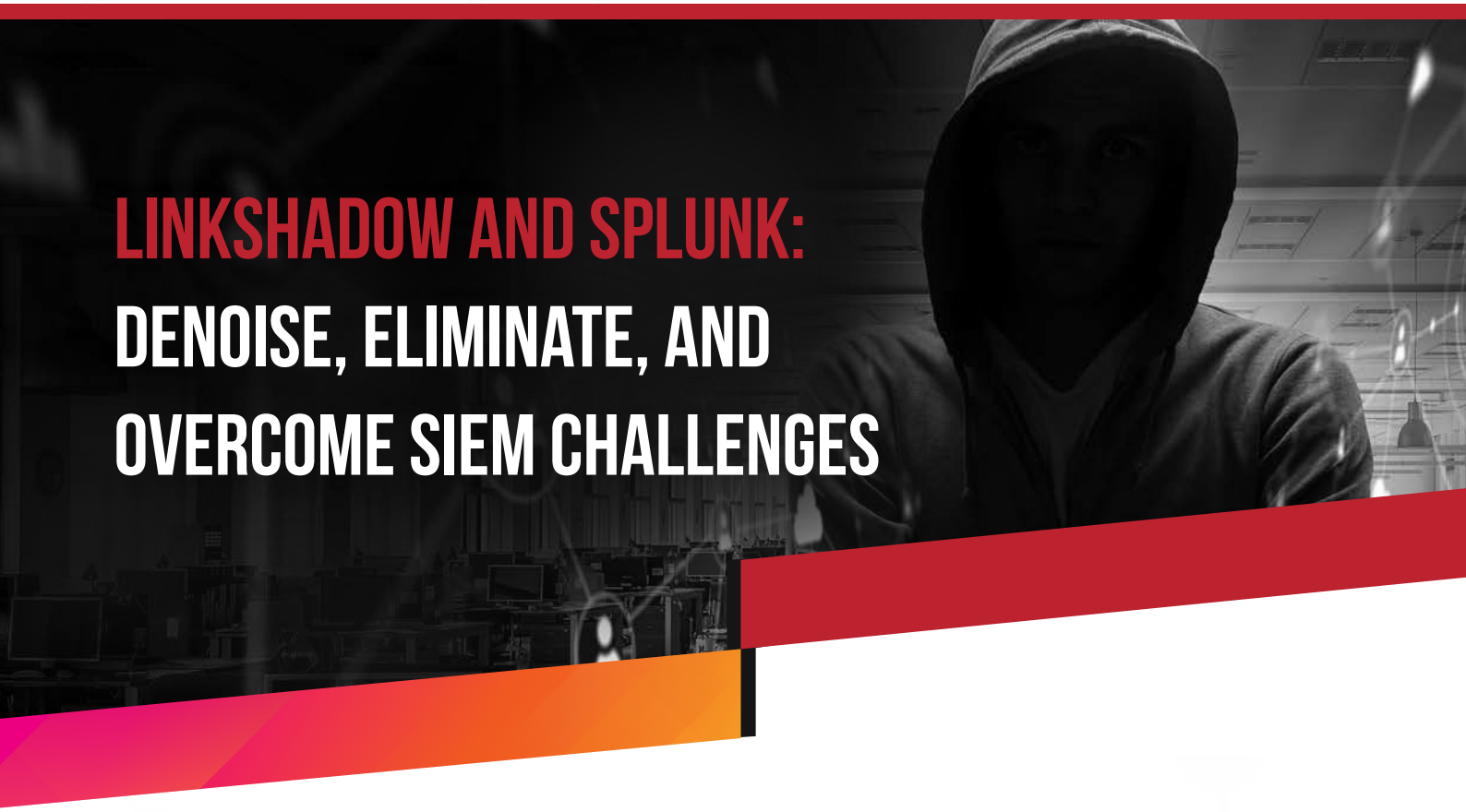

LINKSHADOW AND SPLUNK: DENOISE, ELIMINATE, AND OVERCOME SIEM CHALLENGES

Splunk Enterprise is the industry-leading platform for machine data. Machine data is one of the fastest growing, most complex areas of big data. It is also one of the most valuable, containing a categorical record of user transactions, customer activity, sensor readings, machine behavior, security threats, fraudulent activity and more.

Splunk Enterprise collects all your machine data from wherever it is generated, including physical, virtual and cloud environments. It enables you to search, monitor and analyze your data from one place in real time. Troubleshoot problems and investigate security incidents in minutes. Monitor your end-to-end infrastructure to avoid service degradation or outages. Gain Operational Intelligence with real-time visibility and critical insights into customer experience, transactions, and other key business metrics.

LinkShadow Integrates with Splunk to gather the logs from various log sources which are already connected to the Splunk as part of the Data Collection. Splunk feeds LinkShadow with the detections of the security devices that are fortifying the enterprise.

LinkShadow collects this intelligence and run it over the advanced machine learning algorithms in order to build various dashboards to show either the effectiveness and efficiency of the security devices, the return of investment of the security spending, visualize the attackscape, and more.

INTEGRATION STORY: LINKSHADOW - SPLUNK

LinkShadow integrates with the security tools in the organization to measure the weight of the attack detection and the performance of the security device using the BlockCount Ratio dashboard.

Splunk makes it easier to forward the logs from a single source of contact to minimize the configuration overhead, maximize the efficiency of the log collection, and ensure the full coverage of the organization's security devices.

CHALLENGES OVERCOME BY THE INTEGRATION

As a static rules-based solution any SIEM solution will fire from 100 to 150 alerts per day! If the organization is depending on the Out-of-Box rules, it is expected to reach more than 1000 alert per day. As SIEM rely on static based detection rules, it could not handle new, more advanced types of attacks and constant behavior changes.

LinkShadow uses the Advanced Machine Learning Algorithms to build dynamic Use-Cases that coup with the constant change of the User, Asset, and Network behavior Out-Of-Box with no human interaction or configuration.

www.splunk.com