SURGe

Your trusted advisor for timely security research and guidance

SURGe is a team of Splunk security experts, threat researchers and advisors dedicated to researching, responding, and educating on the threats that impact the world. Our mission is to provide appropriate context and timely recommendations on the latest global breaking security news for organizations. Organizations may leverage SURGe's expertise and knowledge sharing to navigate security incidents with confidence.

We can be an extension of your team

SURGe empowers blue teams across the globe with timely contextual analysis of the security incident and appropriate recommendations to solve your most pressing security problems. We know that when a ransomware campaign is in flight, blue teams may not have the bandwidth to conduct comprehensive research around the adversary and their techniques. Security teams can lean on SURGe as their trusted partner by leveraging our analysis.

We can be your extra pair of eyes

SURGe provides step-by-step technical guidance that includes tested detections to help security teams increase visibility across their threat landscape. By utilizing the tested detections and out-of-the-box security content, organizations can monitor security incidents with ease.

We can be your knowledge hub

Aside from providing contextual analysis and technical guidance on the latest breaking security news, SURGe also shares trusted security research and threat intelligence that are essential for preventing successful cyberattacks. The team creates supporting materials such as security research papers, guides, blogs, datasets and conference presentations on various security topics to help your organization stay ahead of threats.

Many organizations often look to Splunk as their first tool to monitor and investigate security incidents. And as a trusted partner and advisor, SURGe further supports security teams during an initial incident review with technical response guides and contextual analyses. Check out our latest security research or sign up for alerts at www.splunk.com/surge.