Top 5 Security Highlights From Splunk .conf21

Why is fall our favorite season? At Splunk, we're quick to answer: because of .conf (obviously).

This past October, Splunkers from across the globe tuned into our annual user conference. We assembled an incredible collection of sessions and welcomed more attendees than ever before. Better yet, customers, partners and Splunkers came together from the safety and comfort of their own homes — hoodies optional — and shared in the myriad of ways Splunk has helped them level-up their security practice.

In our security super session, Splunk Vice President of Security Product Jane Wong looked at the future of security, and the challenges organizations are likely to face — including cloud complexity, data fragmentation and nebulous regulatory requirements. We also looked at how we can help our customers tackle and solve these problems.

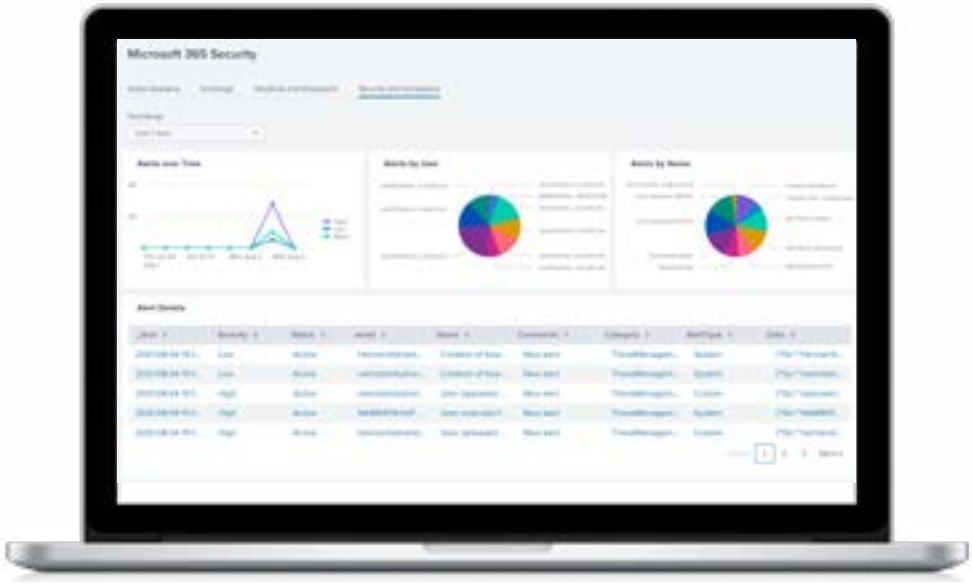
If you missed it, never fear. We've put together our top five takeaways, including some of the newest offerings from across Splunk's security solutions.

1. Cloud complexity is on the rise (and a top security concern)
2. Risk-based alerting can help you take back control of your SOC
3. Automation is easier to manage and more accessible than ever
4. Intelligence management is the secret sauce of security
5. For a simpler, more unified response, consolidate your tools and data security analytics

Cloud complexity is on the rise (and a top security concern)

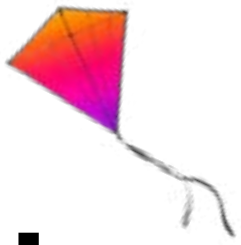
In the time of large-scale cloud migrations and remote work, security has never been more important. Cloud environments introduce new attack vectors due to new data streams, workloads, applications and services. These challenges were only exacerbated during the pandemic, with much of our global workforce becoming remote.

That's why we've been hard at work developing solutions to better secure your cloud journey, unify security operations and improve analyst productivity. In the upcoming release of Splunk Enterprise Security (ES) cloud, we continue to evolve cloud security monitoring, making it even easier to detect and respond to threats across hybrid, cloud and multicloud environments. Many of our customers run workloads in Microsoft Azure, Google Cloud Platform (GCP) or Amazon Web Services (AWS), and we've found establishing a holistic view to be crucial to identifying new and emerging threats.



We've also developed more sophisticated detection rules for cloud attacks thanks to our automated security content, which can help teams stay current on the latest threat detection techniques courtesy of the Splunk Threat Research Team.

At the end of the day, the collective move to the cloud is essential. It presents endless benefits, including increased agility, reduced costs and decreased time to market. And as you embark on your migration journey, we're here to equip you with the right tools so you can do it seamlessly and securely.



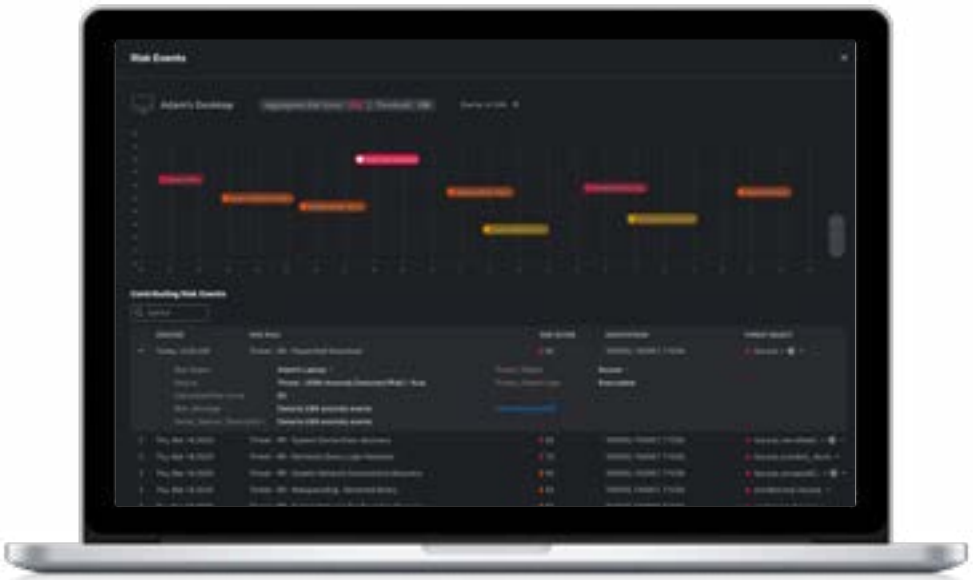
Risk-based alerting can help you take back control of your SOC

Security teams are spending too much time investigating low-value alerts with too little context. Alert fatigue continues to plague unwitting analysts on a daily basis. Incidents based on narrowly defined detections can lead to a high volume of false positives and a lot of extra noise, quickly overwhelming and overburdening anyone on the front lines.

To help tackle this, we introduced risk-based alerting (RBA) — forever changing how customers manage their security operations. This approach works by attributing risk to users and entities, subsequently triggering an alert once certain risk and behavioral thresholds are exceeded.

This helps security operations centers (SOCs) optimize threat hunting by reducing the volume of alerts — thereby increasing true positives — while surfacing more sophisticated threats like low and slow attacks that most correlation searches traditionally miss. This frees up time and resources to home in on actual (often complex) threats and align operations to industry-standard cybersecurity frameworks.

Enhanced capabilities for RBA can be found within the incident review dashboard in Splunk Enterprise Security 6.6. With just a single click, you'll see a new RBA event timeline visualization that gives you a bird's eye view of all the contributing risk events. This provides an analyst with a more comprehensive view of the overall activities associated with a threat actor, making easy work for security teams.



All in all, risk-based alerting will transform your threat investigation and response, dramatically increasing your productivity. And who wouldn't want that?

Automation is easier to manage and more accessible than ever

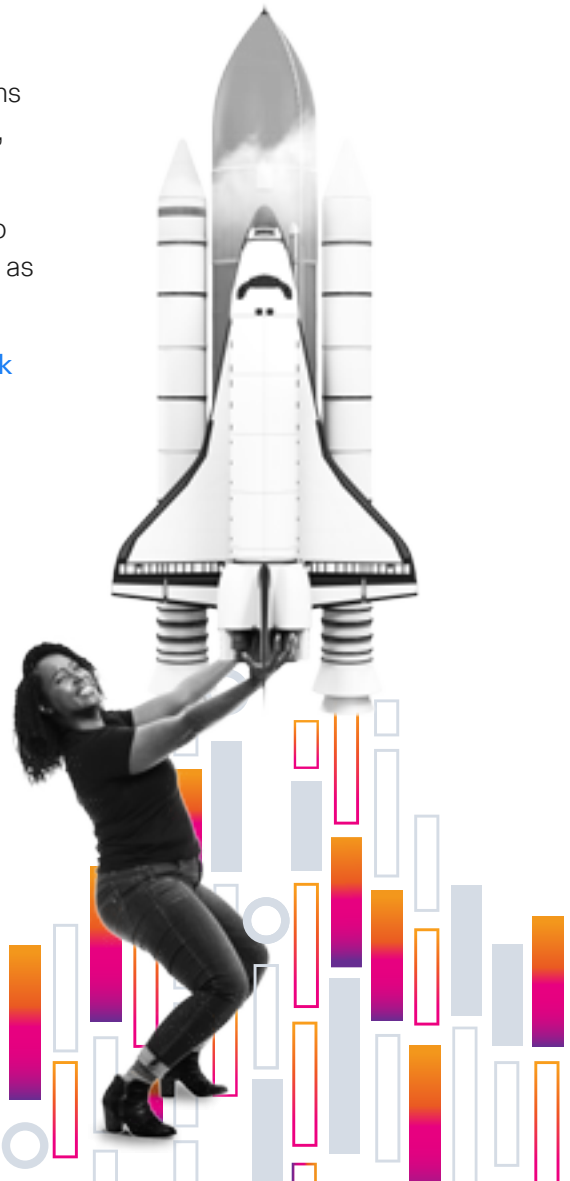
Some security tasks are just too big for teams to process manually. Not to mention, manual investigation and response can be incredibly tedious. Analysts often experience burn out performing the same set of tasks, while more pressing threats go unnoticed. In order to maximize productivity, efficiency and speed — and to not risk anyone's sanity — the only way forward is automation.

Enter Splunk SOAR (formerly known as Splunk Phantom). Our security operations, automation and response (SOAR) solution helps security teams eliminate analyst grunt work and resolve security incidents in record time, cutting their response from minutes (or hours) to mere seconds.

However, we didn't want to stop there. We decided to take things one step further by making automation even more accessible for our customers — as well as easier to deploy, implement and scale across an organization.

To lower the barrier to entry for less technical users, we introduced Splunk SOAR Cloud. With this cloud-based technology, teams benefit from more efficient installation, configuration and scaling of their SOAR technology. Cloud software updates will be continuous and automatic, with no need for manual updates, so customers can spend more time protecting their organization (and less time on infrastructure management).

The updated Splunk SOAR Visual Playbook Editor also makes it easier than ever to create, edit, implement and scale automated playbooks, so you can automate simple security tasks regardless of your level of expertise, and use them as part of a larger investigation for a more modular approach to automation.



4

Intelligence management is the secret sauce of security

Even with the best security incident and event management (SIEM) or security analytics solution, one of the biggest challenges organizations face is maintaining and evolving their security program's rules to better detect and respond to evolving threats. With so many disparate sources — in addition to varying data structures and formats — leveraging the necessary intelligence can be tedious and time-consuming. Especially when security teams are short on time and resources, with little-to-no bandwidth to create all the necessary detections and playbooks.

Fortunately, there's now a solution for customers to integrate and automate intelligence into every stage of the incident response process and across an ecosystem of teams, tools, peers and partners. How? With none other than Splunk Intelligence Management (formerly known as TruSTAR).

Splunk Intelligence Management brings our rapidly growing intelligence marketplace — featuring all types of open, commercial and community intelligence sources — to users everywhere, so they can create complex pipelines without ever having to worry about writing or maintaining scripts. We also launched SURGe, a rapid-response security program for high-profile threats (think Kaseya or the SolarWinds hacks). SURGe provides blue teams with the latest technical guidance and contextual awareness — including who's behind the attack, what their techniques are and how they're implementing the attack.

Finally, if your security team is short on time and resources, then curated in-product security content (e.g., use cases, detection searches and playbooks) can help you hit the ground running. Access detection searches and analytic stories via Splunk Enterprise Security — or more specifically, Splunk Enterprise Security Content Updates (ESCU). Security teams can also take advantage of out-of-the-box content in Splunk SOAR thanks to "playbooks" — also known as in-product guides that provide analysts with step-by-step guidance on how to investigate or respond to an alert.

For a simpler, more unified response, consolidate your tools and data

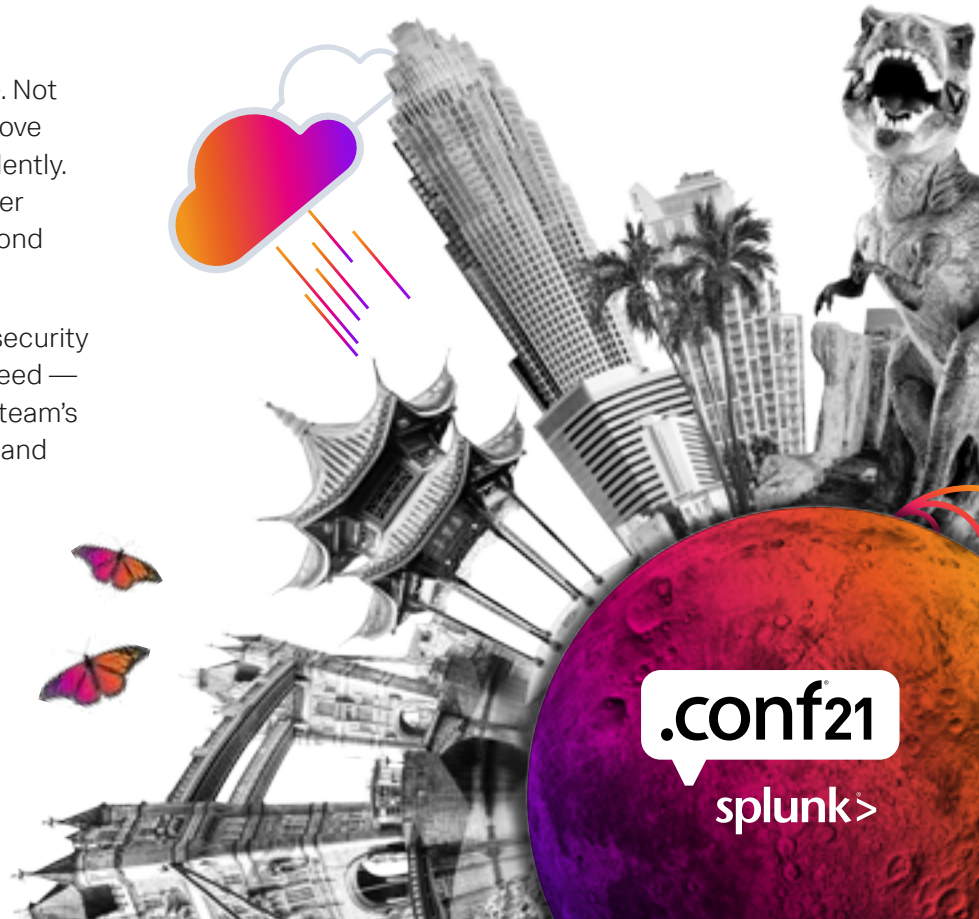
Security should be simple, right? But more often than not, security operations are disparate and unnecessarily complex, involving a patchwork of security tools that are only meant to solve one or two problems. This means that various security functions are divided across a number of security products, resulting in a total lack of visibility and integration.

Security teams are then forced to do "swivel-chair security," constantly pivoting between multiple security product management consoles to do their job. As a result, threat detection, investigation and response are slower, inefficient and much more prone to error. This creates gaps in your defenses that attackers can exploit.

At the Security Super Session, we said goodbye to "swivel-chair security" and hello to Splunkbase — our marketplace for all solutions that plug into Splunk, allowing teams to integrate their preferred security tools along with their respective capabilities for centralized visibility and control across their security stack and systems.

With over 2,400 technology integrations in Splunkbase, there's something for everyone. Not to mention, each solution provides value above and beyond what each tool offers independently. Now, all your security tools can work together seamlessly, so you can investigate and respond to threats without issue.

Gone are the days of pivoting back to your security tools' interface to get the information you need — you can stay within Splunk, increasing your team's productivity and efficiency when detecting and responding to incidents.



Couldn't attend .conf?

We've got you covered! Grab your favorite Splunk T-shirt and tune into our free, on-demand security sessions today