

Mandiant and Splunk for Security

Formidable Defense Against Attackers

The security landscape is ever-changing, intensified by more sophisticated threats, and an increasing number of employees working from home leading to an expanding attack surface. Security professionals are tasked with maintaining a secure environment against a plethora of threats, manifested in thousands of alerts and events that are generated by security controls every day.

As a security team, are you confident your security tools are up-to-date and configured to prevent and respond to these new attacks? When a new threat actor comes onto the scene, are you ready to respond? Most likely, these challenges won't subside — and will continue to escalate — as more businesses undergo digital transformation.

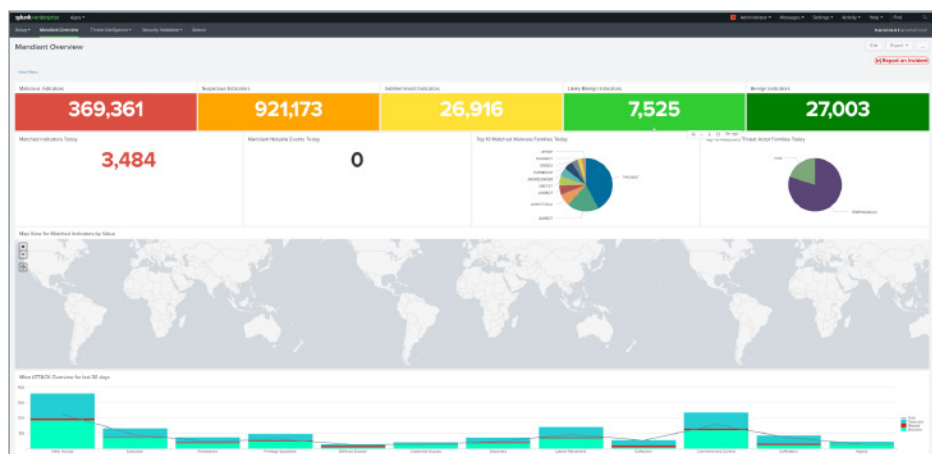
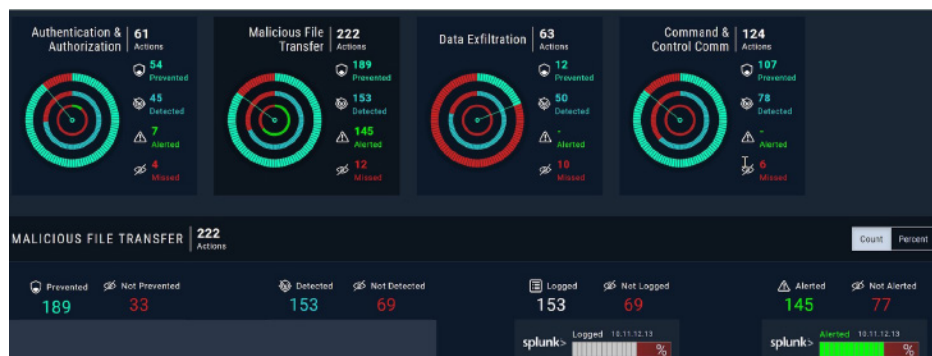
Enter the strategic partnership of Splunk and Mandiant. While Mandiant provides threat intelligence and security validation data, Splunk ingests that information and analyzes it, empowering security teams to rapidly detect and respond to attacks.

The Mandiant Advantage App for Splunk

The [Mandiant Advantage Platform](#) allows you to automate Mandiant expertise, intelligence and technology so you can prioritize and accelerate efforts to detect and respond to attacks.

The Mandiant Advantage App for Splunk incorporates three key Mandiant offerings:

1. Mandiant Threat Intelligence
2. Mandiant Security Validation
3. Mandiant Incident Response



Mandiant Threat Intelligence

Mandiant Threat Intelligence, coupled with Splunk Enterprise and Splunk Enterprise Security, provides direct access to authentic and active threat data, allowing your security teams to quickly identify and understand real-time adversary activity. Mandiant Threat Intelligence provides visibility into the adversary landscape and arms your team with the knowledge of what threats matter most to your organization. This intelligence empowers organizations to better understand attackers and their tactics so you can make informed decisions and take decisive action. Mandiant Threat Intelligence feeds provide insights into well-known malicious actors, top malware families, and maps to the [MITRE ATT&CK Framework](#).

Mandiant Security Validation

Mandiant Security Validation, integrated with [Splunk Enterprise](#) and [Splunk Enterprise Security](#), allows customers to gain confidence in their cyber readiness to withstand attacks. While Mandiant tests the efficacy of security controls to detect or block attacks, it also validates that event information is being sent to Splunk Enterprise, and triggering alerts in Splunk Enterprise Security. With Mandiant and Splunk, customers can continuously validate the effectiveness of their security controls and gain quantitative data to optimize their defenses and make data-driven decisions on the right investments for the future.

Mandiant Incident Response

In the face of a suspected or active breach, customers can use the integration between Mandiant and Splunk to engage with Mandiant incident response experts and report an incident, with the click of a button. This allows customers to investigate, contain and respond to active breaches with confidence; increase the speed, scale and efficiency of their incident response capabilities; and bolster their security operations to detect and respond to attacks in the future.

Get Started with Splunk and Mandiant

To get started, download the Mandiant Advantage App from [Splunkbase](#) and then enter your Mandiant API keys for security validation or threat intelligence. You'll also have access to Mandiant's customer success team with your normal Mandiant threat intelligence subscription.

For more information on Splunk and Mandiant, head to our [Global Partner Page](#).



Learn more: www.splunk.com/asksales

www.splunk.com