MANDIANT

MANDIANT ADVANTAGE
SOLUTION BRIEF

Building A Formidable Cyber Defense

Highlights

- Stay ahead of attackers and today's evolving threats by pulling industry-leading Mandiant threat intelligence, expertise and controls-agnostic technology directly into Splunk.
- Understand the adversary and their tactics with Mandiant Threat Intelligence, make informed decisions and take decisive action.
- Prepare for an attack by validating the effectiveness of security controls, ensure that event information is flowing properly and trigger the creation of notable events in Splunk Enterprise Security.
- Click a button to engage with Mandiant Incident Response experts from within the Splunk console.
- Reduce software and cloud risk with faster response and remediation through automated identification of asset exposures, misconfiguration and vulnerabilities.
- See into the deepest, darkest corners of the Internet to identify impending threats and uncover unknown data and credential leaks.

Simplifying security effectiveness with Mandiant and Splunk

The security landscape is increasingly dangerous and ever-changing, with an expanding attack surface brought about in part due to the increasing number of employees working from home. 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, you must be confident that your security tools are up-to-date and configured to prevent and respond to new attacks. When a new threat actor comes onto the scene, you must be ready to respond. Organizational challenges will continue to escalate as more businesses undergo digital transformation.

Enter the integration between Splunk and Mandiant. While Mandiant provides threat intelligence and security validation data, Splunk ingests that intelligence 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 five essential Mandiant offerings into Splunk Enterprise and Splunk Enterprise Security:

Mandiant Advantage Threat Intelligence

Mandiant Advantage Attack Surface Management

Mandiant Advantage Security Validation

Mandiant Advantage Digital Threat Monitoring

Mandiant Incident Response

splunk>

Mandiant Advantage Threat Intelligence

Threat Intelligence provides direct access to authentic and active threat data, allowing your security team to quickly identify and understand real-time adversary activity. 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 wellknown malicious actors, top malware families, and maps to the MITRE ATT&CK Framework.

Mandiant Advantage Attack Surface Management

Attack Surface Management enables comprehensive visibility of the extended enterprise and security teams to proactively mitigate real-world threats. Attack Surface Management scans corporate assets and cloud resources daily and identifies application and service technologies. Using over 250 data sources—including Mandiant Threat Intelligence, the solution identifies risks to the organization, assigns severity and provides information the security team can use within Splunk to remediate risk.

Mandiant Advantage Security Validation

Security Validation enables 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 Advantage Digital Threat Monitoring

Digital Threat Monitoring delivers customized alerts on potential targeting, as well as data or credential leaks. Triggered alerts from monitoring the open, deep and dark web can be viewed in the Splunk visualization tool using several preconfigured charts. This high-level overview brings what matters most to the forefront.

Mandiant Incident Response

During a suspected or active breach, customers can use the integration between Mandiant Incident Response and Splunk to engage with Mandiant incident response experts with the click of a button. These experts can help customers build incident response capabilities, respond to active breaches and bolster security operations to detect and respond to future attacks.

FIGURE 1. Integrated dashboards for Mandiant Advantage App for Splunk.

Get Started with Splunk and Mandiant

To get started, download the Mandiant Advantage App from Splunkbase and then enter your Mandiant Advantage API keys for Threat Intelligence, Digital Threat Monitoring, Attack Surface Management and Security Validation. You'll also have access to the Mandiant customer success team with your normal Mandiant Threat Intelligence subscription.

About Splunk

Splunk turns data into doing helping organizations unlock innovation, improve security and drive resilience through their leading data platform that supports shared data across any environment so that all teams in an organization can get end-to-end visibility with context for every interaction and business process.

Learn more at **www.mandiant.com**

Mandiant
11951 Freedom Dr, 6th Fl, Reston, VA 20190
(703) 935-1700
833.3MANDIANT (362.6342)
info@mandiant.com

About Mandiant
Since 2004, Mandiant® has been a trusted partner to security-conscious organizations. Today, industry-leading Mandiant threat intelligence and expertise drive dynamic solutions that help organizations develop more effective programs and instill confidence in their cyber readiness.

MANDIANT
YOUR CYBERSECURITY ADVANTAGE