MANDIANT ADVANTAGE

AUTOMATED DEFENSE

Power Your Security Team with Automated Monitoring and Triage

DATA SHEET

Benefits

- **Provides an open architecture allowing choice for best-of-breed technologies**
- **Delivers built-in intelligence that does not require playbooks, rules or scripts saving time and cost**
- **Automates monitoring, detection, triage and escalation of alerts**
- **Deploys in hours providing a quick time-to-value**
- **Integrates with the leading case management and SOAR products for quicker remediation and reduced attacker dwell time**
- **Powered by world-class Mandiant adversary intelligence**

The growth of security-related data coupled with the shortage of skilled security personnel leaves companies at risk. Security teams of all sizes are resource-constrained, filtering alerts to match analysis capacity of their staff. This means clues to potential threats may stay hidden and attackers can achieve longer dwell times in networks, increasing both the likelihood and impact of a security incident. Research shows that 45 percent of alerts are false positives[1] and a breach can cost $3.86 million on average.[2]

To address these issues, Mandiant Automated Defense, a critical component of extended detection and response (XDR) and the Mandiant Advantage platform, intelligently connects disparate SOC evidence by applying patented, probabilistic mathematics and Integrated Reasoning™ to determine the likelihood that events are malicious, actionable and important enough to escalate to security personnel. Automated Defense augments security operations teams by significantly reducing the need to chase false positives, resulting in more time for threat hunting and other proactive security activities.

An Open Architecture

Automated Defense integrates with a broad range of vendors, telemetries and threat intelligence, so you can choose the most appropriate solutions to modernize your sensor grid. You can even keep your existing tools without the need to rip and replace them. Automated Defense works with over 65 vendor offerings across important categories such as endpoint detection and response (EDR), endpoint protection platforms (EPP), incident detection and prevention systems (IDS/IPS), web filtering, security information and event management (SIEM), vulnerability scanning, authentication, and more.

Automated Defense integrates directly with security orchestration automation and remediation (SOAR) platforms to reduce attacker dwell time. This solution saves you time and effort because you are not responding to false positives—only actionable incidents are escalated.

1. IDC Infobrief (January 2021). The Voice of the Analyst—Improving Security Operations Center Processes through Advanced Technologies.
2. Swinhoe (August 13, 2020). What Is the Cost of A Data Breach?

Automated Security Investigations

Using patented techniques and probabilistic mathematics, Automated Defense monitors security event streams and automates expert human analysis of security alerts, accurately culling false positives and escalating actionable, prioritized and well-articulated investigation results. It conducts the following security operations tasks:

- Monitors and evaluates every alert with consistency in real time
- Analyzes investigation results based on common attacker tactics, techniques and procedures (TTPs), then decides on the appropriate action to take based on context
- Prioritizes investigation results based on asset criticality, attack stage progression and likelihood of incident
- Provides detailed cases in an intuitive incident summary with all available evidence of malicious activity
- Learns from customer feedback and integrates with SIEM, big data, SOAR, ticketing and case management platforms to reduce attacker dwell time
- Maps incidents to the MITRE ATT&CK™ Framework
- Includes multi-tenancy capability for easy customer management for managed security service providers (MSSPs)
- Reveals the quantity of alerts that are monitored, analyzed and escalated, as well as false positives
- Provides insight into health of sensors and controls networks

Attack Tactics

- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Defense Evasion
- Credential Access
- Discovery
- Lateral Movement
- Collection
- Command & Control
- Exfiltration
- Impact
- Unknown

Speed, Scale and Consistency of Software

Automated Defense runs 24x7 and scales to the largest enterprises. It integrates with existing security infrastructure including SIEM and SOAR platforms, and removes the need to filter, tune-down or ignore security events to match the monitoring capacity of human analysis. Because Automated Defense automates decision-making, security analysts are enabled to go threat hunting instead of spending time chasing false positives.

Automated Defense processes millions of alerts in real-time, eliminating human bias or fatigue. Because it uses probability-based reasoning, Automated Defense significantly reduces the number of false positives that need to be investigated.

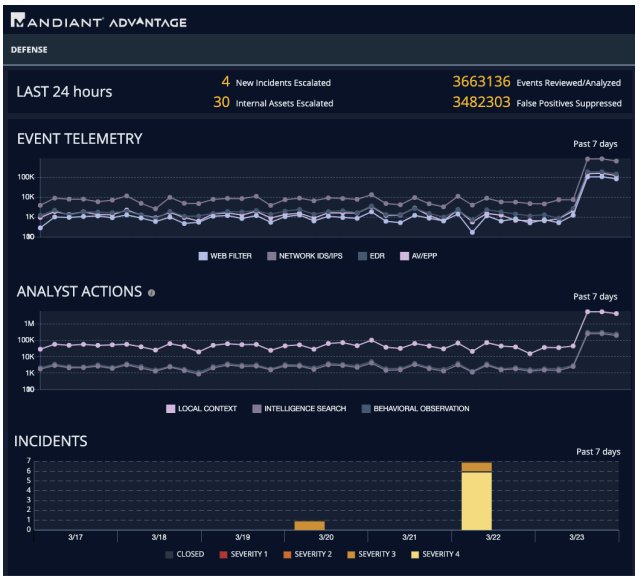

Figure 1. As new related information streams are evaluated, Automated Defense dynamically rescopes and reinterprets the attack tactic. If necessary, it reprioritizes the incident.

Figure 2. Automated Defense includes a complete checklist of security sensors in the environment.

Supported Technologies and Vendors - General Availability

Network Intrusion Detection and Prevention

- Check Point SmartDefense
- Cisco Firepower NGIPS (Sourcefire)
- Corelight Suricata IDS
- Fidelis Network
- FireEye Network Security (NX series)
- Fortinet FortiGate NIDS
- Gigamon Insight (ICEBERG)
- McAfee Network Security Platform
- Palo Alto Networks NGFW IPS
- Snort NIDS and IPS
- Trend Micro TippingPoint

Endpoint Detection and Response

- Crowdstrike Falcon Insight: EDR
- FireEye Endpoint Security (HX series)
- Microsoft Defender for Endpoint
- SentinelOne EDR
- Tanium Threat Response
- VMware Carbon Black EDR

Threat Intelligence Info

- IP Reputation, IP Anonymization (e.g. Public VPN & TOR Nodes), Geolocation, Known Bad Hashes

Industrial Control Systems

- Forescout eyeInspect

Context Integrations

- DHCP (Windows, UNIX, Fortigate, Infoblox)
- Microsoft AD
- Tanium Asset
- VMware Carbon Black Response
- Vulnerability Scanners (Tenable Nessus, Tenable Security Center, Qualys, Rapid7)

Endpoint Protection Platforms

- BlackBerry Protect (CylancePROTECT)
- Broadcom Symantec Endpoint Protection
- Crowdstrike Falcon Prevent: NGAV
- FireEye Endpoint Security (HX)
- Fortinet FortiClient NGEPP
- McAfee (Endpoint Security, VirusScan)
- Microsoft Defender for Endpoint
- Palo Alto (Networks Traps, Networks Cortex XDR)
- SenitnelOne EPP
- Sophos Endpoint Protection
- Tanium Threat Response
- Trend Micro (Apex One, OfficeScan, Deep Security)

Threat Intelligence Integrations

- DShield
- Maxmind
- Mandiant Threat Intelligence
- Open Threat Exchange (OTX)
- STIX/TAXII (Supporting most commercial vendors, e.g. Anomali and OASIS)
- VirusTotal
- WHOIS

Customer Info

- Critical Systems, IP space, DNS servers, critical accounts, internal/external safe list, malware importance, guest/unmonitored networks, filehash safel list, banned/suspicious countries, signature importance

URL/Web Filtering

- Broadcom Symantec Web Filter (Blue Coat ProxySG)
- Check Point URL Filtering
- Cisco (Firepower URL Filtering, Umbrella/Umbrella DNS WF)
- Forcepoint Web Security
- Fortinet (FortiGate Web Filtering, FortiClient Web Filtering)
- iBoss Secure Cloud Gateway
- McAfee Web Gateway
- Palo Alto Networks NGFW URL Filtering
- Zscaler Secure Web Gateways

Event Repository Integrations

- Amazon S3
- Apache Kafka
- Direct from security event product
- ELK, Hadoop
- Google Cloud Storage
- Microsoft Azure Event Hub
- Palo Alto Networks Cortex
- SIEM (e.g. AlienVault, ArcSight, Devo, QRadar, Splunk, Sumo Logic)

Operations Management

- Automated Communication Platforms (e.g. PagerDuty, Email)
- IBM Resilient SOAR
- Palo Alto Networks Cortex XSOAR (Demisto)
- ServiceNow
- Splunk Phantom

For more on Automated Defense, visit: **https://www.fireeye.com/mandiant/automated-defense.html**

MANDIANT ADVANTAGE

The cyber landscape continues to grow in complexity as adversaries become increasingly more sophisticated and rapidly morph their tactics. To proactively reduce business risk from motivated attackers, organizations need continuous validation technology powered by timely and relevant intelligence. Mandiant, a part of FireEye, brings together the world's leading Threat Intelligence and front-line incident response data with its continuous security validation platform to arm organizations with the tools needed to increase security effectiveness and reduce organizational risk, regardless of the technology deployed.

FireEye, Inc.
601 McCarthy Blvd. Milpitas, CA 95035
408.321.6500/877.FIREEYE (347.3393)
info@FireEye.com

AD-EXT-DS-US-EN-000346-01