



Enterprise Continuous Monitoring & Cyber Risk Management Solution

© 2021

www.marssuite.com

Phone: +1-256-513-9535 Email: contact@marssuite.com



Table of Contents

Introduction to MARS Suite	2
MARS Suite Components	3
Dashboard	3
Vulnerability Scanner	4
Threat Repositories and Alerting	4
Reporting	5
Incident Manager	6
Playbook Orchestration	7
Case Management	8
Network Traffic Discovery Sensors	8
Full Packet Capture	9
Network Security Monitoring Sensors	9
Network Intrusion Detection System (NIDS)	9
Analysis Tools	10
Asset Discovery and Inventory Management	11
MARS Suite for CMMC	12
MARS Suite Standards and Certifications	13
The MARS Suite Team	14
Mission Innovate: Home of the MARS Suite Team	14
All Points	14
Mission Multiplier	14



Introduction to MARS Suite

MARS Suite is a proven Enterprise Continuous Monitoring and Cyber Risk Management solution. It leverages legacy infrastructure and solutions, delivers comprehensive real-time situational awareness, manages cyber incidents, provides asset visibility, combats dynamic threats, and mitigates vulnerabilities. MARS Suite is NSA National Information Assurance Partnership (NIAP) tested and approved. It is also certified for operational use on the Approved Products List by the Department of Defense Joint Interoperability Test Command (JITC).

MARS Suite enables organizations to combat potential threats and adversaries by ingesting data from disparate IT sensors and scanners, tracking asset criticality, cross-referencing interrelated data, summarizing it, generating data driven risk scores, developing configurable reports and data visualizations on mission-relevant findings from various software and hardware perspectives. Additionally, this data is organized and prioritized in an intuitive manner with tools and affordances specifically designed to provide situational awareness for the leadership and actionable intelligence for the operators and analysts.

On the situational awareness front, the MARS Suite dashboard delivers a single pane of glass view that provides an enterprise-wide Common Operating Picture (COP) of the cybersecurity posture of the organization and its components. This allows decision makers to gauge the current state of operations, identify the organizational cyber risk and its trends over time, and determine the sources of potential vulnerabilities and exposure to the enterprise down to a specific device or user. These unique insights empower the leadership to optimally target their resources where they are most needed and leverage their existing infrastructure and teams more efficiently. This enables the organization to deal with ever changing cybersecurity challenges in real time and makes the operations significantly more cost effective.

Operators and analysts are provided actionable intelligence through powerful, yet easy to use tools that seamlessly correlate dynamic threat data with real time vulnerability scans, organizational directives, mission risks and organizational asset criticality. This unique approach to data driven risk management based on continuous monitoring enables the cybersecurity teams to effectively prioritize and optimize their operations. MARS Suite provides cybersecurity professionals the ability to quickly drill down from aggregated views and trending data to actionable specifics utilizing attribute-based access controls. It also seamlessly organizes operational and remediation information to simplify the reporting of status and management of resources. This feature reduces the administrative workload making the lives of operators and analysts significantly easier and freeing them up to focus on tangible cybersecurity analysis, remediation, and hunting functions.

Conventional SIEM solutions provide mechanisms to continuously identify events and inform operators and leadership. As a result, cybersecurity professionals are perpetually flooded with alerts and events of varying severity impacting assets and systems at all levels of criticality. This traditional incident and alert management focused approach makes task assignments and resource allocation progressively difficult and inefficient, due to the relentless influx of incidents and events with no discernable way to prioritize and manage them.

MARS Suite totally transforms this paradigm by empowering cybersecurity professionals to easily identify and focus on the highest organizational risk from the most dangerous cyber threats that expose and leverage vulnerabilities on assets that are most critical to an enterprise. By leveraging behavioral science and gamification technology, MARS Suite incentivizes the identification and pursuit of such targets. This unique approach simplifies, prioritizes, and optimizes an organization's cybersecurity posture, and operational effectiveness.

MARS Suite Components

MARS Suite is comprised of the following stack of technical components:

- Dashboard – Common Operating Picture for organizational situational awareness and risk management
- Vulnerability Scanner – for identifying infrastructural and system vulnerabilities
- Threat Repositories and Alerting – for correlating threat feeds and delivering alerts
- Incident Manager – for identifying, Analyzing and Managing cybersecurity incidents
- Network Traffic Discovery Sensors – for assessing network traffic in motion
- Analysis Tools – for conducting aggregated cyber analytics
- Asset Discovery and Inventory Management – for comprehensive infrastructure visibility

The following sections provide further details regarding the MARS Suite components and how they address specific cybersecurity requirements.

Dashboard

The MARS Suite Dashboard component Commander View is shown in Figure 1. Data collected through continuous monitoring scanners and sensors utilizing all MARS Suite components, as well as legacy network devices, can be easily aggregated, viewed, and used to prioritize information, actions and responsibilities for the most important and critical assets. MARS Suite computes a risk score based on asset criticality, threat proliferation and vulnerability severity across organizational domains in an intuitive letter grade.

The MARS Suite dashboard is extensible and can be configured to consume data ingested from diverse MARS Suite components as well as legacy systems, such as Tenable Nessus, Big Fix, Splunk, etc. Even when ingested from multiple systems, the information is displayed in a simple intuitive cross-correlated, structured fashion.

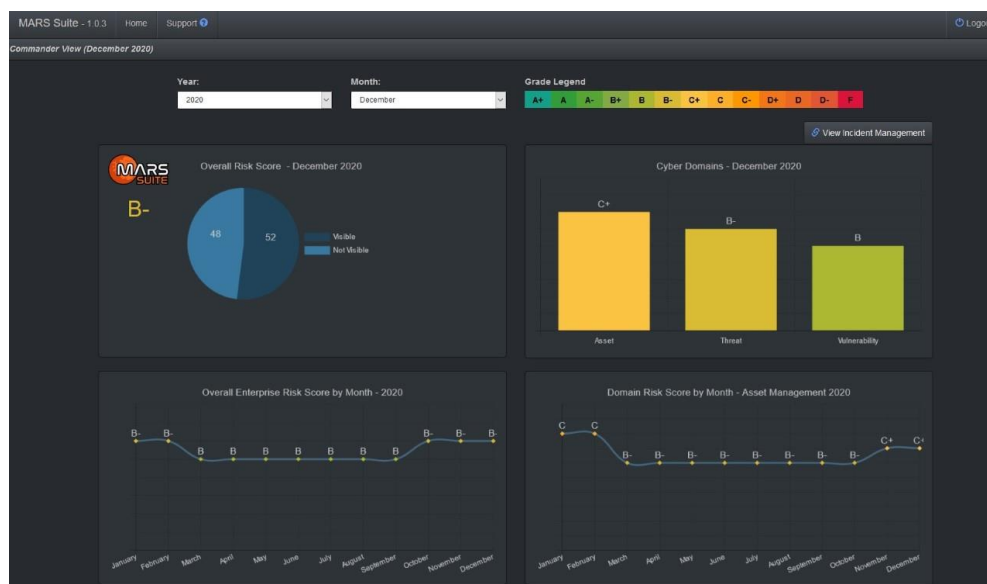


Figure 1: MARS Suite Dashboard Commander View

Vulnerability Scanner

The MARS Suite Vulnerability Scanner component, as depicted in Figure 2, is a full featured network scanner powered by Greenbone vulnerability manager. It can be configured to scan the organization's network for vulnerabilities, anomalies, system deficiencies, and configuration flaws both at pre-determined schedules and manually, as needed. If required, the scan sensors can work alongside other deployed toolsets to minimize network load.



Figure 2: MARS Suite Vulnerability Scanner

Threat Repositories and Alerting

MARS Suite utilizes threat information from the National Vulnerability Databases (NVD), including data from the Network Vulnerability Tool (NVT), Common Vulnerabilities and Exposures (CVEs), the Common Platform Enumeration (CPE) Dictionary, Community Emergency Response Team (CERT) Advisories, and the Security Content Automation Protocol (SCAP), as shown in Figure 3.

The Threat Repositories views displays a table that contains:

1. Threat Source – CVE ID of Threat along with a link to get more details.
2. Description of the Vulnerability
3. Severity of the Vulnerability (Critical, High, Medium, Low, None)
4. Asset Count showing number of assets impacted by Threat

Along with the count of assets impacted by Threat the Asset Count column contains an information icon that when clicked displays a dialog showing the details of the threat for all the impacted assets (shown below):

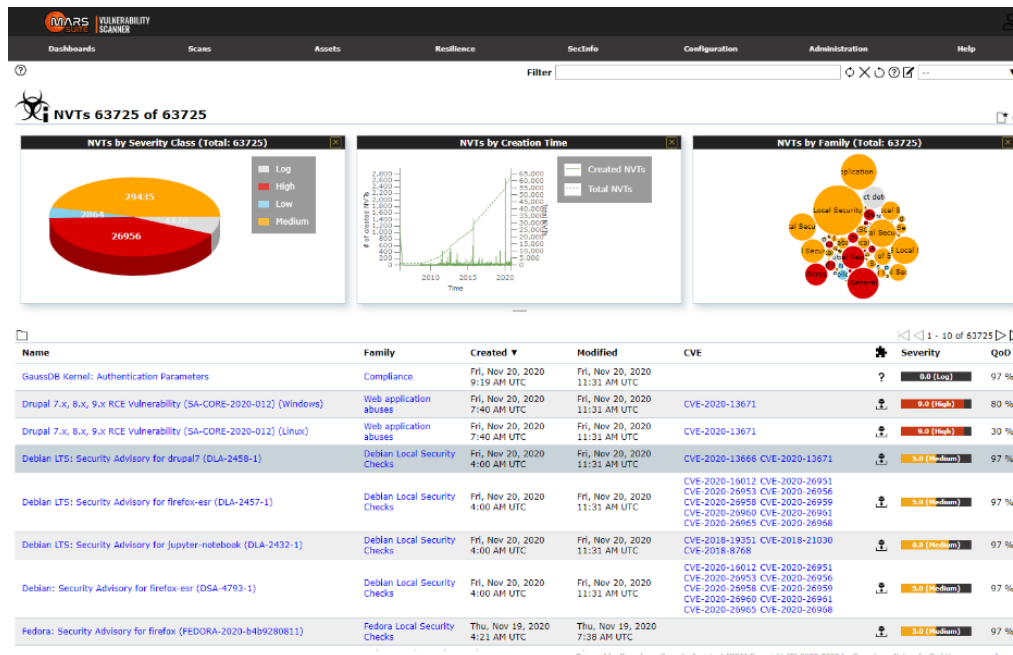


Figure 3: MARS Suite Threat Repositories & Sources

Reporting

MARS Suite Vulnerability Scanner & Sensors produce reports (that are emailed to authorized staff) and other required information to assist administrators in mitigating or fixing discovered anomalies, vulnerabilities, and system flaws. The scan reports also include instructions and links to download patches and firmware updates.

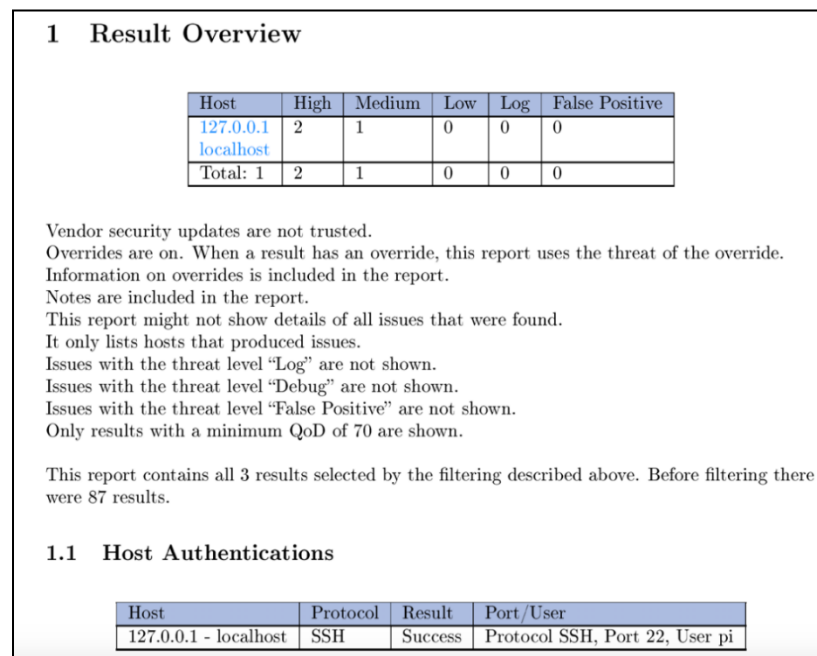


Figure 4: MARS Suite Emailed Scan Reports

Incident Manager

The MARS Suite Incident Manager component leverages the Security Onion toolkit and a variety of internal toolsets along with vetted best of breed opensource solutions as well as any existing customer legacy solutions. MARS Suite not only provides industry leading cybersecurity incident management capabilities, but it also correlates comprehensive network monitoring, threat identification, response management to develop an organizational risk profile that reflects the effectiveness of the enterprise cybersecurity posture.

MARS Suite Incident Manager provides both active hunting as well as passive forensic capabilities. The hunting capabilities are geared towards identifying adversary tactics, techniques, and procedures (TTPs), approach heuristics, attack vectors and associated analytics for Data in Motion (DiM) as well as Data at Rest (D@R). On the forensics front, MARS Suite provides detailed logs, correlated, aggregated, and normalized data for comprehensive System Performance Monitoring (See Figure 5) and detailed forensic analytics.



Figure 5: MARS Suite Incident Manager System Performance Monitor

The MARS Suite Incident Manager capability prioritizes incidents by focusing in on the risk from the most dangerous threats that expose and leverage vulnerabilities on assets that are most critical to an enterprise. Additionally, it provides functionality and affordances to respond, mitigate and remediate the risks being identified. Figure 6 below provides a sampling of some of the incident management capabilities.

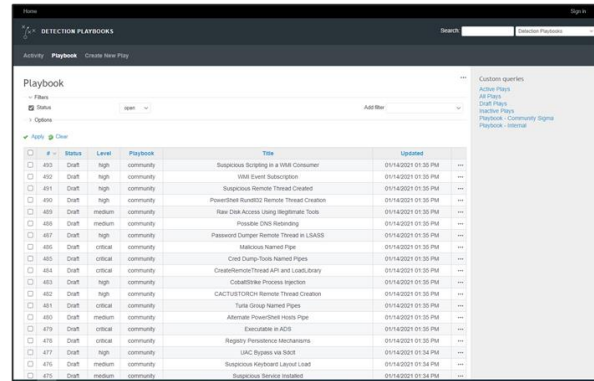
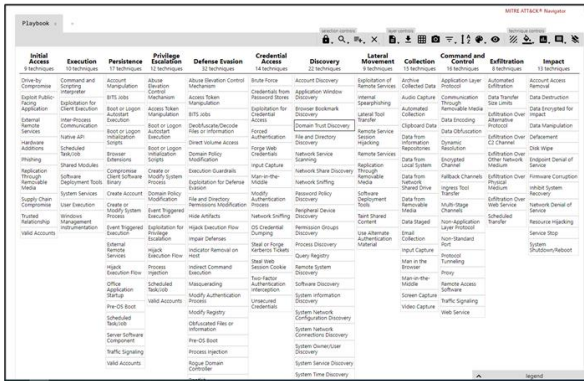
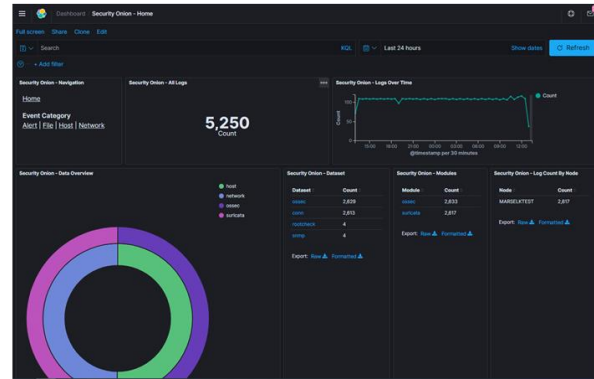
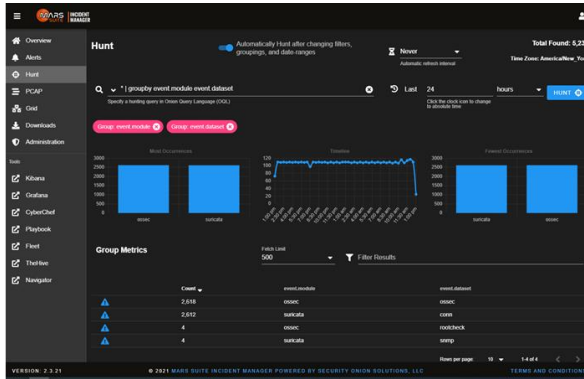


Figure 6: A sampling of MARS Suite Incident Manager screens

Playbook Orchestration

MARS Suite provides over 500 pre-defined “plays” that are collections of actionable orchestration steps derived from industry best practices System Security Plans (SSPs). The Playbook Orchestration component of MARS Suite Incident Manager provides a detailed dashboard for user defined plays and configurable alerts and reports.

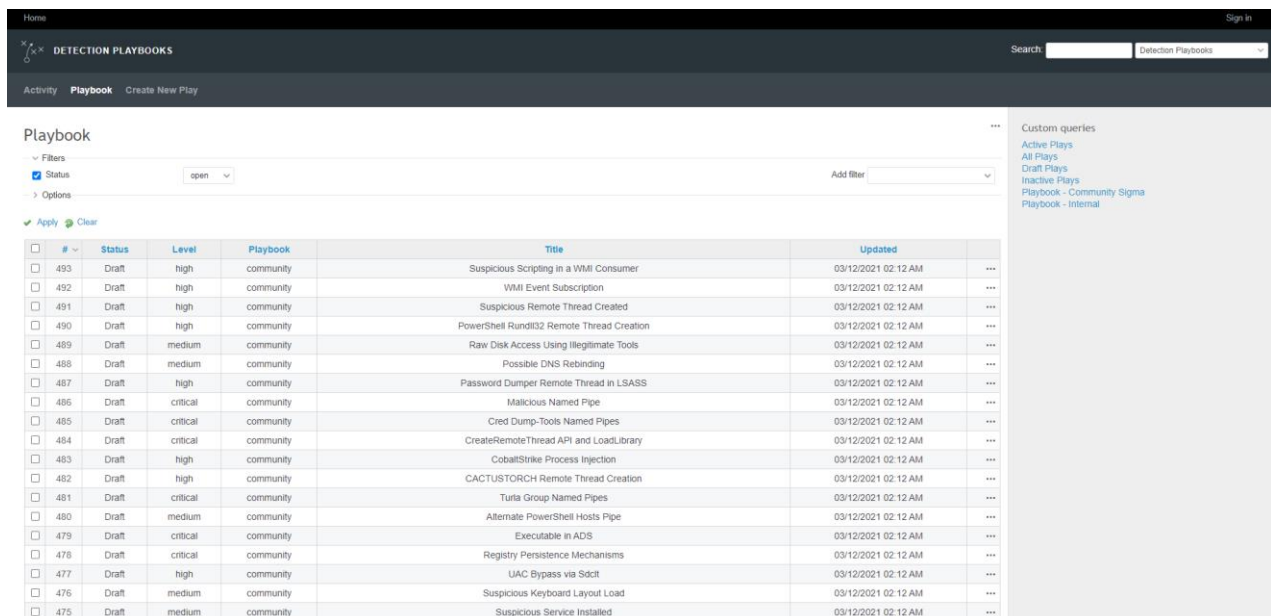
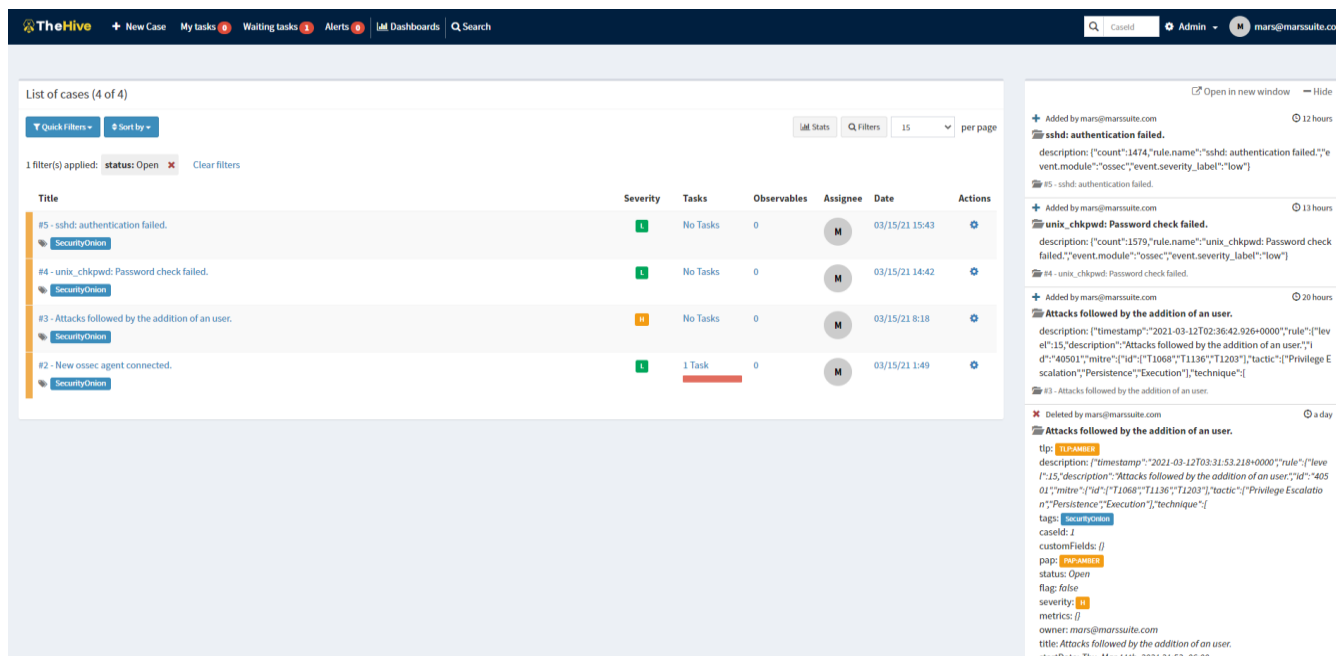


Figure 7: MARS Suite Incident Manager Playbook Orchestration

Case Management

MARS Suite Incident Manager provides a powerful Case Management solution. Analysts and operators can create, escalate, review, assign, and manage cases and alerts based on events and incidents as they occur in real time or in retrospect for the purpose of forensic analytics. Figure x shows a Case Management screen.



Title	Severity	Tasks	Observables	Assignee	Date	Actions
#5 - sshd: authentication failed.	L	No Tasks	0	M	03/15/21 15:43	
#4 - unix_chkpwd: Password check failed.	L	No Tasks	0	M	03/15/21 14:42	
#3 - Attacks followed by the addition of an user.	H	No Tasks	0	M	03/15/21 8:18	
#2 - New ossec agent connected.	L	1 Task	0	M	03/15/21 1:49	

Added by mars@marssuite.com 12 hours

sshd: authentication failed.

description: {"count":1474,"rule.name":"sshd: authentication failed","event.module":"ossec","event.severity_label":"low"}

#5 - sshd: authentication failed.

Added by mars@marssuite.com 13 hours

unix_chkpwd: Password check failed.

description: {"count":1579,"rule.name":"unix_chkpwd: Password check failed","event.module":"ossec","event.severity_label":"low"}

#4 - unix_chkpwd: Password check failed.

Added by mars@marssuite.com 20 hours

Attacks followed by the addition of an user.

description: {"timestamp":"2021-03-12T02:36:42.926+0000","rule":{"level":15,"description":"Attacks followed by the addition of an user","id":"40501","mitre":{"id":["T1068","T1136","T1203"],"tactic":["Privilege Escalation"],"persistence":["Execution"],"technique":[""]}}

#3 - Attacks followed by the addition of an user.

Deleted by mars@marssuite.com 1 day

Attacks followed by the addition of an user.

tip: **EXPLOITER**

description: {"timestamp":"2021-03-12T03:31:53.218+0000","rule":{"level":15,"description":"Attacks followed by the addition of an user","id":"40501","mitre":{"id":["T1068","T1136","T1203"],"tactic":["Privilege Escalation"],"persistence":["Execution"],"technique":[""]}}

tags: SecurityOnion

CaseId: 1

customFields: {}

app: EXPLOITER

status: Open

flag: false

severity: H

metrics: {}

owner: mars@marssuite.com

title: Attacks followed by the addition of an user.

startDate: Thu, Mar 11th, 2021 21:53 -06:00

Figure 8: MARS Suite Incident Manager Case Management Solution

Network Traffic Discovery Sensors

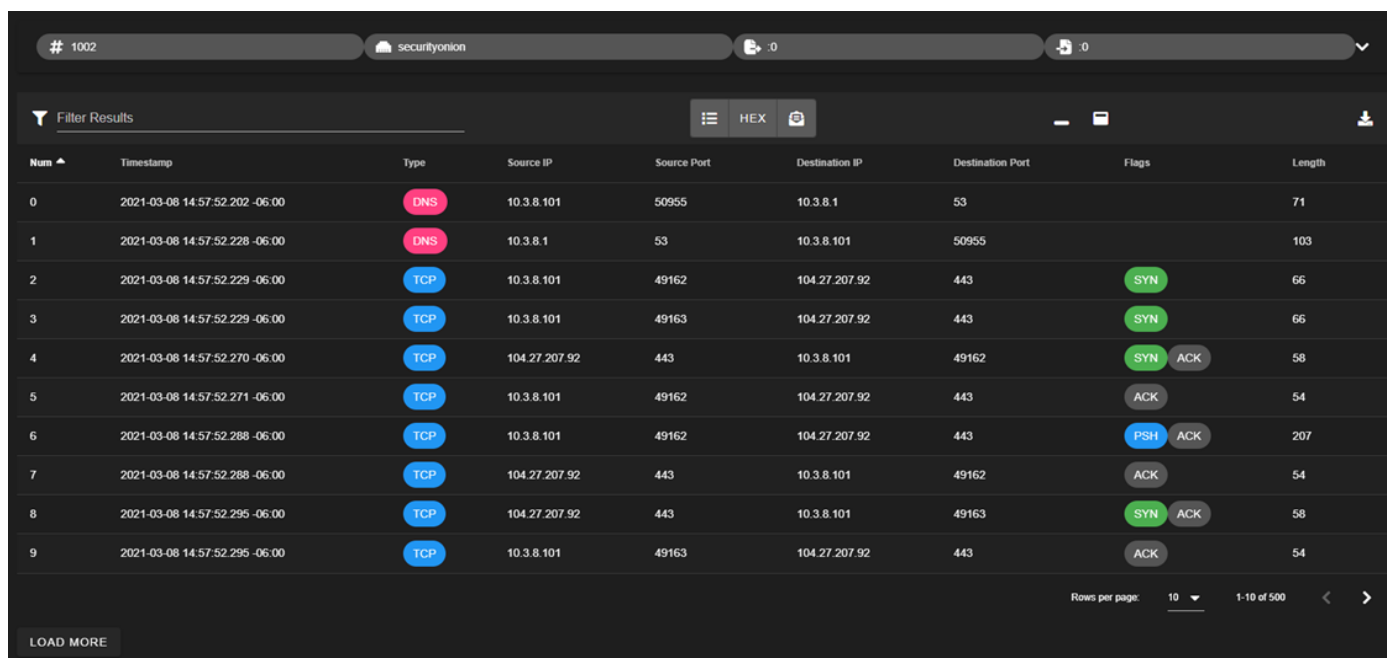
The MARS Suite Network Traffic and Intrusion Detection Sensors components powered by Security Onion leverage internal toolsets along with vetted best of breed opensource as well as any existing customer legacy solutions to provide comprehensive network status and analytical data for review and prioritization.

Network Security Monitoring (NSM) is, put simply, monitoring the network for security related events. It might be proactive, when used to identify vulnerabilities or expiring SSL certificates, or it might be reactive, such as in incident response and network forensics. Whether tracking an adversary or trying to keep malware at bay, NSM provides context, intelligence, and situational awareness of your network. In addition to the compiled high-level dashboards, network traffic and incidents can be viewed using the web user interfaces on each respective toolset, as depicted in the descriptions and figures below.

Data can be collected and analyzed, but not all malicious activity looks malicious at first glance. While automation and correlation can enhance intelligence and assist in the process of sorting through false positives and malicious indicators, there is no replacement for human intelligence and awareness. MARS Suite provides visibility into network traffic, and context around alerts and anomalous events to empower cyber analysts.

Full Packet Capture

Full Packet Capture leverages capabilities and functionality from tools such as Stenographer and netsniff-ng, which captures real time traffic via the MARS Suite Vulnerability Scanners and sensors. Full packet capture tracks and logs network incidents, such as exploit payloads, phishing emails, file exfiltration activities, etc.



Num	Timestamp	Type	Source IP	Source Port	Destination IP	Destination Port	Flags	Length
0	2021-03-08 14:57:52.202 -06:00	DNS	10.3.8.101	50955	10.3.8.1	53		71
1	2021-03-08 14:57:52.228 -06:00	DNS	10.3.8.1	53	10.3.8.101	50955		103
2	2021-03-08 14:57:52.229 -06:00	TCP	10.3.8.101	49162	104.27.207.92	443	SYN	66
3	2021-03-08 14:57:52.229 -06:00	TCP	10.3.8.101	49163	104.27.207.92	443	SYN	66
4	2021-03-08 14:57:52.270 -06:00	TCP	104.27.207.92	443	10.3.8.101	49162	SYN ACK	58
5	2021-03-08 14:57:52.271 -06:00	TCP	10.3.8.101	49162	104.27.207.92	443	ACK	54
6	2021-03-08 14:57:52.288 -06:00	TCP	10.3.8.101	49162	104.27.207.92	443	PSH ACK	207
7	2021-03-08 14:57:52.288 -06:00	TCP	104.27.207.92	443	10.3.8.101	49162	ACK	54
8	2021-03-08 14:57:52.295 -06:00	TCP	104.27.207.92	443	10.3.8.101	49163	SYN ACK	58
9	2021-03-08 14:57:52.295 -06:00	TCP	10.3.8.101	49163	104.27.207.92	443	ACK	54

Figure 9: MARS Suite Network Traffic Events

Network Security Monitoring Sensors

The NSM sensors also include network-based and host-based intrusion detection systems (IDS) which analyze network traffic or host systems and provide log and alert data for detected events and activity. The following types of intrusion detection systems are available using the MARS Suite NSM sensors:

Network Intrusion Detection System (NIDS)

MARS Suite Incident Manager leverages Security Onion powered toolsets and a variety of internal and vetted best of breed open source tools. These rule-based network intrusion detection systems (NIDS) analyze traffic to discover fingerprints and identifiers that match known malicious, anomalous, or otherwise suspicious traffic.

MARS Suite also includes analysis-driven NIDS that, unlike rules-based systems, analyze large volumes of data. MARS Suite monitors network activity and logs session connections, DNS requests, network services and software, SSL certificates, and HTTP, FTP, IRC, SMTP, SSH, SSL, and syslog activity that is seen by the sensor, providing a real depth and visibility into the context of data and events. Additionally, MARS Suite includes analyzers for many common protocols and has the capacity to check MD5 sums for HTTP file downloads against Malware Hash Registry projects. This toolkit also provides real-time correlation of network activity with up-to-date community intelligence feeds, alerting when users access known malicious systems or websites. The file analysis framework provides protocol independent file analysis, allowing for the ability to capture files as they

pass through the network, then automatically pass them to a sandbox or a file share for antivirus scanning.

Analysis Tools

With full packet capture, logs, alerts and Network Intrusion data, there is an incredible amount of data available for analysis. MARS Suite Incident Manager powered by Security Onion integrates and correlates the data into a powerful dashboard that can also be used to prioritize work towards the organization's most critical assets first.

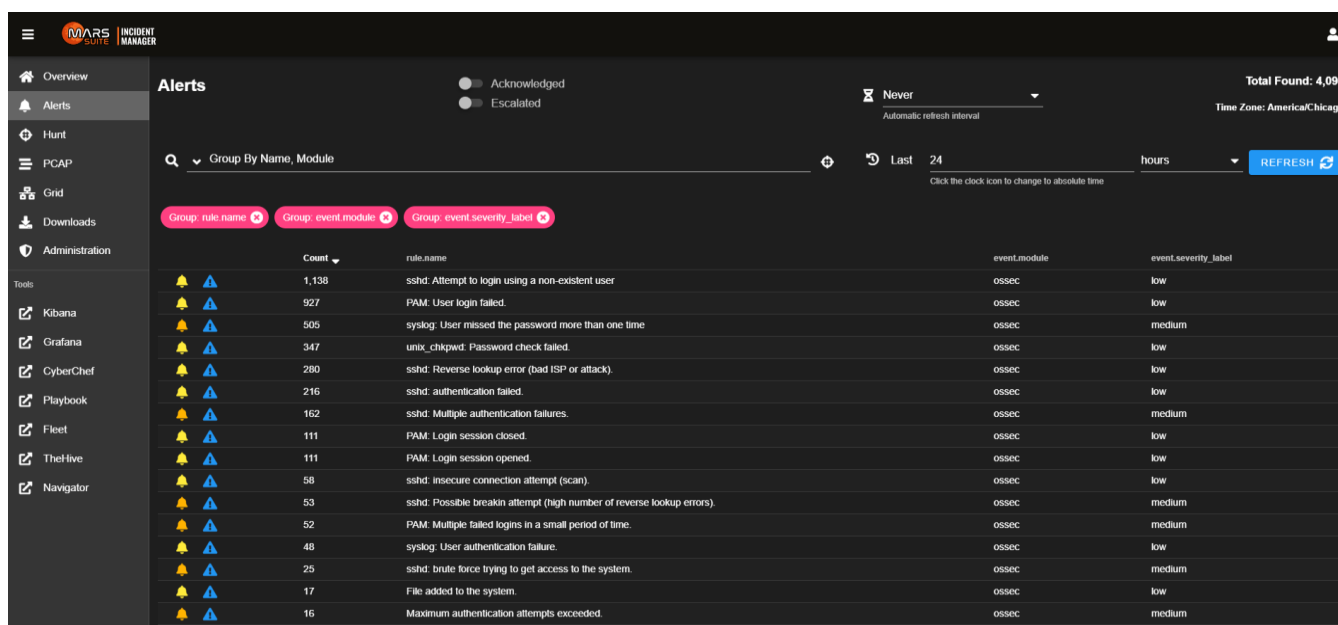


Figure 11: MARS Suite Analysis Tools

Asset Discovery and Inventory Management

The asset management capabilities of MARS Suite include the ability to auto discover and map network assets using network discovery scans. Asset management allows administrators to aggregate their systems and pull relevant information such as operating system versions, installed application and service information (including version and build numbers), as well as end of life notifications for operating systems and software packages.

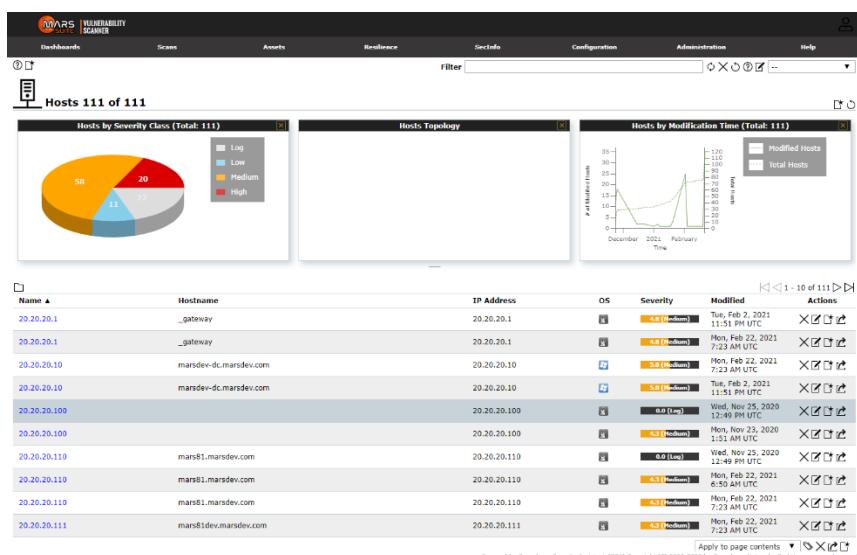


Figure 12: MARS Suite Vulnerability Scanner Asset List and Network Map



Figure 13: MARS Suite Asset Domain and Organizational Units Risk Grading



MARS Suite for CMMC

MARS Suite provides significant compliance coverage required by the DoD's Cybersecurity Maturity Model Certification (CMMC) for Levels 2 and higher. Table 1 below, provides a description of the Domains, Capabilities, Practices and certification levels addressed by MARS Suite, correlated to the currently drafted version of CMMC.

Level	Domain	Practice	Capability
2	Audit & Accountability (AU)	AU.2.042	Perform auditing
2	Audit & Accountability (AU)	AU.2.043	Perform auditing
2	Audit & Accountability (AU)	AU.2.044	Review and manage audit logs
2	Incident Response (IR)	IR.2.092	Plan incident response
2	Incident Response (IR)	IR.2.093	Detect and report events
2	Incident Response (IR)	IR.2.094	Detect and report events
2	Incident Response (IR)	IR.2.096	Develop and implement a response to a declared event
2	Incident Response (IR)	IR.2.097	Perform post incident reviews
2	Risk Management (RM)	RM.2.141	Identify and evaluate risk
2	Risk Management (RM)	RM.2.142	Identify and evaluate risk
2	Risk Management (RM)	RM.2.143	Manage risk
2	Security Assessment (CA)	CA.2.159	Define and manage controls
2	System & Info. Integrity (SI)	SI.2.216	Perform network and system monitoring
2	System & Info. Integrity (SI)	SI.2.217	Perform network and system monitoring
3	Audit & Accountability (AU)	AU.3.045	Define audit requirements
3	Audit & Accountability (AU)	AU.3.046	Define audit requirements
3	Audit & Accountability (AU)	AU.3.048	Perform auditing
3	Audit & Accountability (AU)	AU.3.049	Identify and protect audit information
3	Audit & Accountability (AU)	AU.3.050	Identify and protect audit information
3	Audit & Accountability (AU)	AU.3.051	Review and manage audit logs
3	Audit & Accountability (AU)	AU.3.052	Review and manage audit logs
3	Incident Response (IR)	IR.3.098	Develop and implement a response to a declared event
3	Incident Response (IR)	IR.3.099	Test incident response
3	Risk Management (RM)	RM.3.144	Identify and evaluate risk
3	Risk Management (RM)	RM.3.146	Manage risk
3	Situational Awareness (SA)	SA.3.169	Implement threat monitoring
4	Asset Management (AM)	AM.4.226	Manage asset inventory
4	Audit & Accountability (AU)	AU.4.053	Review and manage audit logs
4	Audit & Accountability (AU)	AU.4.054	Review and manage audit logs
4	Incident Response (IR)	IR.4.100	Plan incident response
4	Risk Management (RM)	RM.4.149	Identify and evaluate risk
4	Risk Management (RM)	RM.4.150	Identify and evaluate risk
4	Risk Management (RM)	RM.4.151	Identify and evaluate risk
4	Situational Awareness (SA)	SA.4.171	Implement threat monitoring
4	System & Info. Integrity (SI)	SI.4.221	Identify and manage information system flaws
5	Audit & Accountability (AU)	AU.5.055	Perform auditing
5	Incident Response (IR)	IR.5.106	Plan incident response
5	Incident Response (IR)	IR.5.102	Develop and implement a response to a declared event
5	Risk Management (RM)	RM.5.152	Manage risk
5	Risk Management (RM)	RM.5.155	Manage risk

Table 1: CMMC Framework Controls Addressed by MARS Suite

MARS Suite Standards and Certifications

MARS Suite is a COTS product deployed in commercial and government environments and in compliance with requisite standards, certifications, and accreditation requirements. The functionality, controls and affordances provided in MARS Suite enable compliance coverage for many industry standards requirements including:

FIPS 140-2	DoD Cybersecurity Maturity Model Certification – CMMC
NIST 800-53	DISA Security Technical Implementation Guide – STIG
NIST 800-171	NIST Security Content Automation Protocol – SCAP
NIST CIS v7.1.x	Federal Information Security Management Act – FISMA
NIST CSF v1.1	CERT Resilience Management Model – RMM v1.2

Table 2: Industry Standards supported by MARS Suite capabilities

The operating processes and quality standards of the MARS Suite Team are ISO 9001 (AS 9100) certified. The software development, operations, and management of the MARS Suite Team are also assessed and certified at a Capability Maturity Model Integration (CMMI DEV 3) level.

MARS Suite is built utilizing a proven Holistic All Points Product Innovation Process that leverages Human Centered Design (HCD), Double Helix Methodology (DHM) and Collaborative Innovation Sessions (CIS).

MARS Suite has been subjected to the most stringent government testing, certification, and accreditation procedures, including the Federal Information Processing Standards (FIPS). MARS Suite has also been tested by the National Information Assurance Partnership (NIAP), a joint security testing effort between the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA).

MARS Suite is a Department of Defense Joint Interoperability Test Command (JITC) Approved Certified Cyber Security Product and is currently available on the DoD Approved Products List (DoD APL).



CMMI DEV / 3SM
Exp. 2020-12-22 / Appraisal #30935



The MARS Suite Team

Mission Innovate: Home of the MARS Suite Team

Mission Innovate is a HUBZone-certified small business offering leading-edge cybersecurity and information technology solutions. Headquartered in Huntsville, Alabama and formed through a joint venture between All Points and Mission Multiplier, we bring access to our state-of-the-art cyber lab where we develop leading-edge cybersecurity products and solutions to help federal and commercial clients secure their missions. Mission Innovate is comprised of cybersecurity and IT thought leaders who create innovative and custom solutions to help our clients more effectively manage cybersecurity risk and IT systems. We conduct extensive research and development to create cutting-edge cybersecurity tools and solutions like MARS Suite to address continually evolving cybersecurity challenges. Additional information can be found at www.missioninnovate.com

All Points

Established nearly 25 years ago as a Merritt Island, Florida based Service-Disabled Veteran Owned Small Business (SDVOSB), All Points today has operations in 18 states and has grown into a leading solution provider to a diverse array of Government and Commercial customers. All Points has built an excellent reputation in solution development and systems integration in strategic, high risk, security sensitive, mission critical domains such as Aerospace, Intelligence, Defense and Cyber, while also providing consistent, low risk, cost effective and reliable products and services to a wide variety of customers in the civilian and commercial sectors. The dedicated and diverse team at All Points has award winning expertise in Engineering, Software Development, IT Management, Product Delivery, InfoSec Monitoring, Cyber Operations, Critical Infrastructure, Export Control, Integrated Logistics, and Program Management. Additional information can be found at www.allpointslc.com

Mission Multiplier

Mission Multiplier is a Huntsville-based, HUBZone small business specializing in cybersecurity solution development and is a recognized DoD asset at the forefront of cybersecurity and information assurance innovation. Mission Multiplier is a participant in the DoD Mentor-Protégé program (with All Points as the Mentor) and maintains a Defense Security Service (DSS) recognized Top Secret facility clearance. Mission Multiplier delivers tailored, highly innovative cyber solutions focused on enabling and protecting client missions. Mission Multiplier is comprised of subject matter experts and cyber developers in the areas of cybersecurity assessment, governance, engineering, operations, and research & development. Mission Multiplier was recently awarded the "2019 Small Business of Year" in the government contracting technology category by the Huntsville Alabama Chamber of Commerce. Additional information can be found at www.missionmultiplier.com

Contact the MARS Suite Team

Email: contact@marssuite.com

Phone: (256) 513-9535

Web: www.marssuite.com