SQUIRREL
COMPLIANCY SOLUTIONS

Squirrel Defender

Network STIG Automation

DEFENDER

Corporate Background

Founder

Size

Patents

Community

CISCO

DEVNET

Customers

DEFENSE INFORMATION SYSTEMS AGENCY

DEPARTMENT OF THE NAVY · UNITED STATES OF AMERICA

UNITED STATES ARMY

DEPARTMENT OF THE NAVY · UNITED STATES MARINE CORPS

ARMY NATIONAL GUARD

UNITED STATES NAVAL CRIMINAL INVESTIGATIVE SERVICE · VERITAS

THE DEPARTMENT OF THE TREASURY · 1789

SQUIRREL
COMPLIANCY SOLUTIONS

What’s the Pitch?

“Defender is a Network STIG Automation platform.”

Defender is a purpose-built platform of modernized engines for audit, analysis, and remediation of vulnerability findings.

Defender provides you with a curated STIG Automation Experience.

Defender is the only low-code/no-code GUI in industry with a workflow driven logic editor to achieve STIG compliancy.

Defender automation provides up to 80% in manpower reduction and 99% reduction in audit and remediation time of misconfigurations.

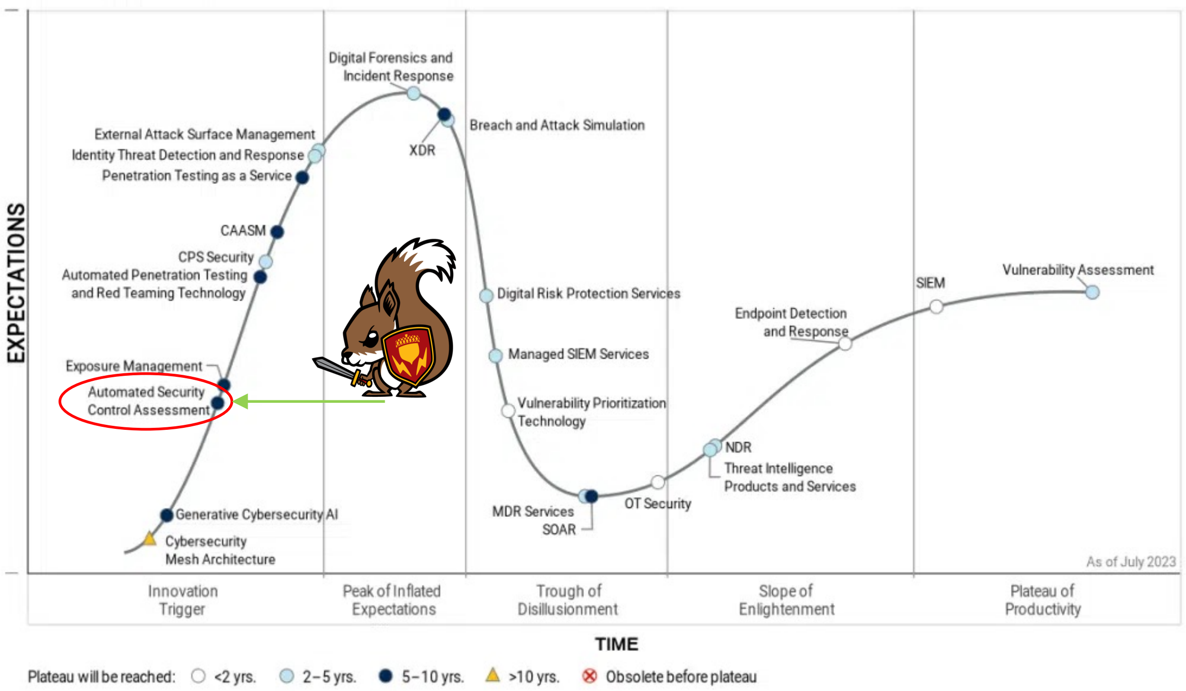
The DISA STIG is the only objective-based metric used across the DoD to measure operational readiness.

DEFENDER

Where Is Defender In Industry?

Gartner

Hype Cycle for Security Operations, 2023



Definition:

ASCA processes and technologies focus on the analysis and remediation of misconfigurations in security controls (e.g., endpoint protection, network firewall, identity, email security, and security information and event management), which improves enterprise security posture. ASCA can be a stand-alone tool or a capability of other security products, such as firewalls, identity threat detection and response, network security policy management, and cloud infrastructure entitlement management.

Gartner

SQUIRREL COMPLIANCY SOLUTIONS

DEFENDER

Salient Characteristics

Functions

- Layer 2 & 3 STIG Audit
- Layer 2 & 3 STIG Remediation
- Triggered Event Audit
- Scheduled Audit
- Low Code/No Code
- Embedded Logic GUI
- Moderated STIG Libraries

Compliancy

- DISA STIG
- CCRI/CCORI/CORA
- DoDI 8510.01 (CONMON)
- CPT Audit
- cATO
- DoDI 8420.01
- NIST 800-37/53/137

Features

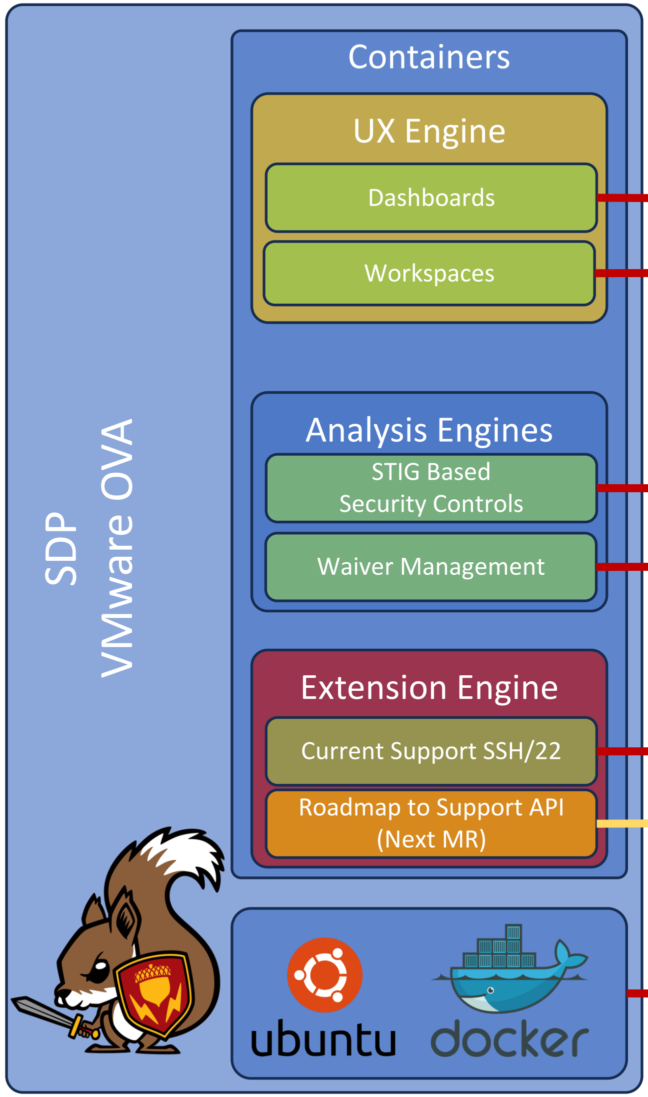
- Integrated STIG Viewer
- .CKL Artifacts & Export
- NSC Grading & Scoring
- Multi-Vendor Support
- Audit Over 900+ STIG Vulnerabilities
- Integrated Waiver Management System
- RBAC Management

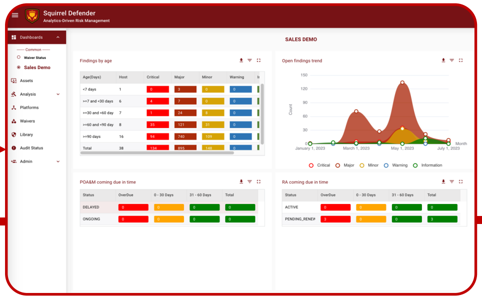
Currently Hold Active ATO
Approved for Operation in NIPR, SIPR, JWICS

SQUIRREL COMPLIANCY SOLUTIONS

DEFENDER

Platform Delivery & Architecture




Squirrel Defender
Analytics-Driven Risk Management

Dashboards
------- Common -------
Waiver Status
Sales Demo
Assets
Analysis
Platforms
Waivers
Library
Audit Status
Admin

SALES DEMO

Findings by age

Age(Days)	Host	Critical	Major	Minor	Warning
<7 days	1	0	3	0	0
>=7 and <30 days	6	4	7	0	0
>=30 and <60 day	7	1	24	8	0
>=60 and <90 day	8	35	121	31	0
>=90 days	16	94	740	109	0
Total	38	134	895	148	0

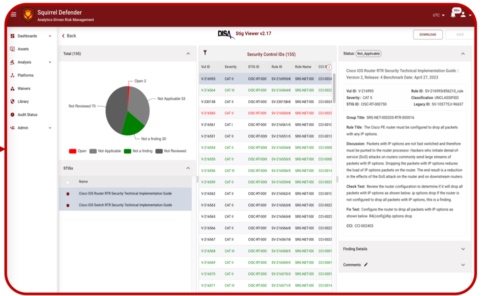
Open findings trend

POA&M coming due in time

Status	OverDue	0 - 30 Days	31 - 60 Days	Total
DELAYED	0	0	0	0
ONGOING	0	0	0	0

RA coming due in time

Status	OverDue	0 - 30 Days	31 - 60 Days	Total
ACTIVE	0	0	0	0
PENDING_RENEW	3	0	0	3


Squirrel Defender
Analytics-Driven Risk Management

UTC 99+

Dashboards
Assets
Analysis
Platforms
Waivers
Library
Audit Status
Admin

Back

DISA Stig Viewer v2.17

DOWNLOAD SAVE

Total (155)

STIGs

Name
Cisco IOS Router RTR Security Technical Implementation Guide
Cisco IOS Switch RTR Security Technical Implementation Guide

Security Control IDs (155)

Vul ID	Severity	STIG ID	Rule ID	Rule Name	CCI ID
V-216993	CAT II	CISC-RT-000	SV-216993r8	SRG-NET-00	CCI-0024
V-216564	CAT III	CISC-RT-000	SV-216564r8	SRG-NET-00	CCI-0023
V-230158	CAT II	CISC-RT-000	SV-230158r8	SRG-NET-00	CCI-0024
V-216560	CAT II	CISC-RT-000	SV-216560r8	SRG-NET-00	CCI-0023
V-216561	CAT I	CISC-RT-000	SV-216561r5	SRG-NET-00	CCI-0010
V-216551	CAT II	CISC-RT-000	SV-216551r5	SRG-NET-00	CCI-0013
V-216554	CAT II	CISC-RT-000	SV-216554r8	SRG-NET-00	CCI-0008
V-216555	CAT II	CISC-RT-000	SV-216555r5	SRG-NET-00	CCI-0008
V-216556	CAT III	CISC-RT-000	SV-216556r5	SRG-NET-00	CCI-0014
V-216559	CAT II	CISC-RT-000	SV-216559r8	SRG-NET-00	CCI-0023
V-216562	CAT II	CISC-RT-000	SV-216562r5	SRG-NET-00	CCI-0010
V-216563	CAT II	CISC-RT-000	SV-216563r8	SRG-NET-00	CCI-0023
V-216565	CAT II	CISC-RT-000	SV-216565r8	SRG-NET-00	CCI-0023
V-216566	CAT II	CISC-RT-000	SV-216566r8	SRG-NET-00	CCI-0023
V-216567	CAT II	CISC-RT-000	SV-216567r8	SRG-NET-00	CCI-0023
V-216568	CAT III	CISC-RT-000	SV-216568r5	SRG-NET-00	CCI-0001
V-216569	CAT II	CISC-RT-000	SV-216569r5	SRG-NET-00	CCI-0001
V-216570	CAT II	CISC-RT-000	SV-216570r5	SRG-NET-00	CCI-0001
V-216571	CAT III	CISC-RT-000	SV-216571r5	SRG-NET-00	CCI-0014

Status: Not_Applicable

Cisco IOS Router RTR Security Technical Implementation Guide :: Version 2, Release: 4 Benchmark Date: April 27, 2023

Vul ID: V-216993
Severity:: CAT II
STIG ID: CISC-RT-000750
Rule ID: SV-216993r856210_rule
Classification UNCLASSIFIED
Legacy ID: SV-105775,V-96637

Group Title: SRG-NET-000205-RTR-000016

Rule Title: The Cisco PE router must be configured to drop all packets with any IP options.

Discussion: Packets with IP options are not fast switched and therefore must be punted to the router processor. Hackers who initiate denial-of-service (DoS) attacks on routers commonly send large streams of packets with IP options. Dropping the packets with IP options reduces the load of IP options packets on the router. The end result is a reduction in the effects of the DoS attack on the router and on downstream routers.

Check Text: Review the router configuration to determine if it will drop all packets with IP options as shown below. ip options drop If the router is not configured to drop all packets with IP options, this is a finding.

Fix Text: Configure the router to drop all packets with IP options as shown below. R4(config)#ip options drop

CCI: CCI-002403

Finding Details

Comments

NIST National Institute of Standards and Technology

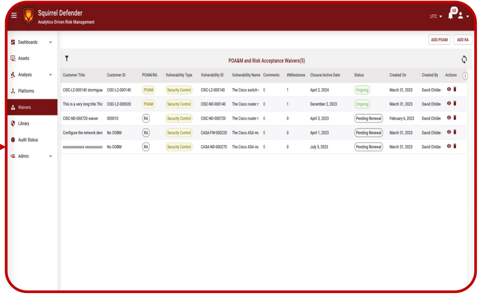
DISA

NIST SP 800-171

NIST Cybersecurity Framework

NIST SP 800-37 Risk Management Framework

NIST SP 800-53


Squirrel Defender
Analytics-Driven Risk Management

UTC 68

Dashboards
Assets
Analysis
Platforms
Waivers
Library
Audit Status
Admin

ADD POAM ADD RA

POA&M and Risk Acceptance Waivers(5)

Customer Title	Customer ID	POAM/RA	Vulnerability Type	Vulnerability ID	Vulnerability Name	Comments	#Milestones	Closure/Active Date	Status	Created On	Created By	Actions
CISC-L2-000140 stormguai	CISC-L2-000140	POAM	Security Control	CISC-L2-000140	The Cisco switch ı	0	1	April 2, 2024	Ongoing	March 31, 2023	David Childe	
This is a very long title This	CISC-L2-000020	POAM	Security Control	CISC-ND-000140	The Cisco router r	0	1	December 2, 2023	Ongoing	March 31, 2023	David Childe	
CISC-ND-000720 waiver	000010	RA	Security Control	CISC-ND-000720	The Cisco router r	0	0	April 3, 2023	Pending Renewal	February 6, 2023	David Childe	
Configure the network devi	No OOBM	RA	Security Control	CASA-FW-000220	The Cisco ASA mı	0	0	April 1, 2023	Pending Renewal	March 31, 2023	David Childe	
xxxxxxxxxxxx xxxxxxxxxx	No OOBM	RA	Security Control	CASA-ND-000270	The Cisco ASA mı	0	0	July 5, 2023	Pending Renewal	March 31, 2023	David Childe	

cisco

ARISTA

JUNIPER NETWORKS

aruba a Hewlett Packard Enterprise company

SDN/Cloud

DEFENSE INFORMATION SYSTEMS AGENCY

SQUIRREL COMPLIANCY SOLUTIONS

Defender License Model

Device License

Product Subscription	Priced
Defender License	Per Device

Subscription Based

Annual / Multi-Year Options

License required for each device managed by Defender

* License required only for management IP of stacked switches

** License required only for Wireless LAN Controllers (WLC). Wireless Access Points (APs) do not require Defender License [subject to change in 2025])

Support License

Support Subscription
Platinum
Gold
Silver

Support License required for each Defender Device License (1:1)

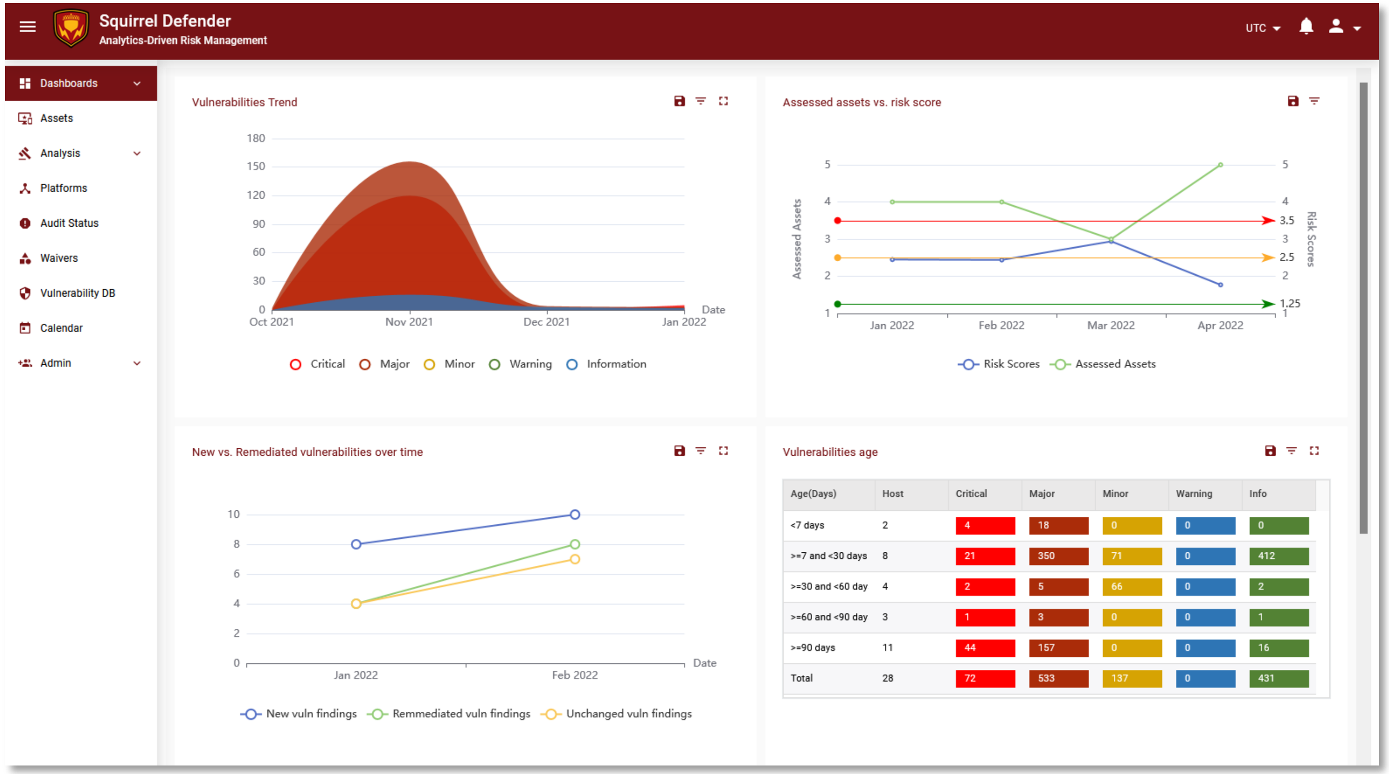
Services

Product Services
Installation Services
Remote Credits
Professional Services

DEFENDER

Demonstration

1. Dashboard Summaries & Trends
2. Layer 2 & 3 Network Asset Inventory
3. Analysis Rules, Policies, & Audit
4. Audit Execution & State
5. Remediation Execution
6. Post Remediation Audit
7. Embedded Rule Logic GUI
8. Waiver Management System



Vulnerabilities age

Age(Days)	Host	Critical	Major	Minor	Warning	Info
<7 days	2	4	18	0	0	0
>=7 and <30 days	8	21	350	71	0	412
>=30 and <60 day	4	2	5	66	0	2
>=60 and <90 day	3	1	3	0	0	1
>=90 days	11	44	157	0	0	16
Total	28	72	533	137	0	431

SQUIRREL
COMPLIANCY SOLUTIONS

DEFENDER

Contacts

James Cobb
Federal Account Executive
Email: jcobb@squirrelcs.com
Mobile: 614-361-4335

Dave Lundgren
Business Development Manager
Email: dlundgren@squirrelcs.com
Mobile: 703-755-5262

https://www.squirrelcs.com
1-833-4SQUIRREL (1-833-477-8477)
info@squirrelcs.com

SQUIRREL COMPLIANCY SOLUTIONS