







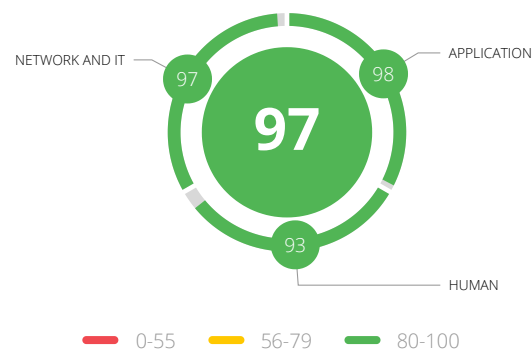
OVERVIEW

FOCI Fiber Optic Communications, Inc. is a leading company established in 1995 by a core team from the prestigious Industrial Technology Research Institute in Taiwan. FOCI specializes in fiber optic interconnect, FBT, and PLC technology development, of...

 Communications	 --
 --	 Privately Held
 --	 11-50 employees

Cyber Assessment

Cyber Posture Rating

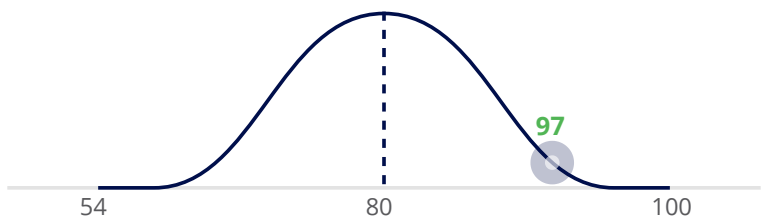


Posture By Categories

Application	98	Human	93	Network and IT	97
Application Security	100	Responsiveness	100	Asset Reputation	100
Domain Attacks	100	Employee Attack Surface	100	Cloud	--
Exposed Services	96	Security Team	--	DNS	94
Technologies	100	Social Posture	33	Endpoint	--
				Mail Server	100
				TLS	97
				Web Server	90

Industry Range

Communications



Assets

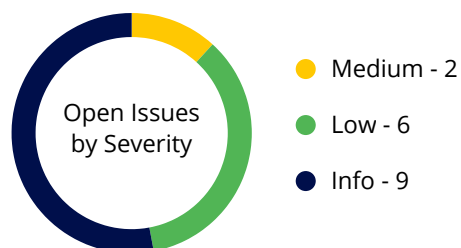
Geolocation



IPs Distribution



Network and IT



Issues By Sub-Category

Asset Reputation			100
<u>CRITICAL</u>		<u>LOW</u>	
No Critical severity tests in this section		Suspicious Communication Samples	No Findings
<u>HIGH</u>		Suspicious URLs	No Findings
Hosting Malicious Content	--	<u>INFO</u>	
Hosting Phishing Site	No Findings	No Info severity tests in this section	
<u>MEDIUM</u>			
Asset Flagged as Anonymizer	--		
Asset Flagged as Malicious	--		
Asset Flagged as Spammer	--		
Hosting Adult Content	No Findings		
Cloud			--
<u>CRITICAL</u>		<u>LOW</u>	
No Critical severity tests in this section		Cloud Single Region	--
<u>HIGH</u>		<u>INFO</u>	
Cloud Private Services Exposed	--	Cloud Bucket Hosting Website	--
<u>MEDIUM</u>			
Cloud Bucket Public Listing	--		
DNS			94
<u>CRITICAL</u>		<u>LOW</u>	
DNS Zone Transfer	No Findings	DNS Wildcard Record	No Findings
<u>HIGH</u>		DNSSEC Configuration	2 issues
Open DNS Resolver	--	<u>INFO</u>	
<u>MEDIUM</u>		Company is Missing DNS MX Record	No Findings
No Medium severity tests in this section		Company is Missing DNS NS Record	No Findings

Endpoint

--

CRITICAL

No Critical severity tests in this section

HIGH

No High severity tests in this section

MEDIUM

Browser Vulnerabilities Accessing Company Services --

End-of-Life Browsers Accessing Company Services --

Operating System Vulnerabilities Accessing Company Services --

Operating System is End-of-Life of Company Services --

LOW

No Low severity tests in this section

INFO

Endpoint Devices Detected of Company Services --

Mail Server

100

CRITICAL

No Critical severity tests in this section

HIGH

SPF Existence No Findings

MEDIUM

DKIM Existence No Findings

DMARC Existence No Findings

LOW

DKIM Configuration No Findings

DMARC Configuration No Findings

SPF Configuration No Findings

User Enumeration --

INFO

No Info severity tests in this section

TLS

97

CRITICAL

TLS Critical Vulnerabilities No Findings

HIGH

HTTPS Not Supported No Findings

TLS Certificate Untrusted No Findings

TLS Deprecated Protocols No Findings

TLS High Severity Cipher Suite Findings No Findings

TLS High Severity Vulnerabilities No Findings

MEDIUM

Missing HTTP to HTTPS Redirect 1 issues

TLS Certificate Validity Too Long No Findings

TLS Medium Severity Cipher Suite Findings No Findings

TLS Weak Certificate Keys No Findings

LOW

TLS Certificate Chain Installation 1 issues

TLS Configuration Bad Practices No Findings

TLS Low Severity Vulnerabilities 1 issues

TLS Renegotiation Findings 2 issues

TLS SCTs Extension Not Implemented No Findings

INFO

TLS Anonymous Authentication No Findings

TLS Certificate Extended Validation 6 issues

TLS Certificate Upcoming Expiration 3 issues

CRITICAL

No Critical severity tests in this section

HIGH

Content-Security-Policy High Severity Findings --

Missing Content-Security-Policy Header --

Missing WAF on Significant Asset --

MEDIUM

Versions Exposed in Web Server Headers 1 issues

LOW

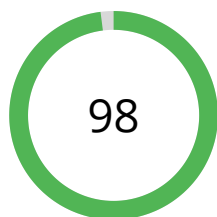
Content-Security-Policy Findings --

Set-Cookie Response Header No Findings

INFO

No Info severity tests in this section

Application



Issues By Sub-Category

Application Security		100
<u>CRITICAL</u> No Critical severity tests in this section		<u>LOW</u> Unrecommended SSH Algorithms --
<u>HIGH</u> Insecure SNMP Community String --		<u>INFO</u> No Info severity tests in this section
Open Sensitive NTP Commands --		
SSH Version 1 Protocol --		
Web App Disclosed Vulnerability	No Findings	
WordPress User Data Exposure	No Findings	
<u>MEDIUM</u> Unrestricted Access to WordPress Admin Page	No Findings	
Vulnerable SSH Algorithms --		
Web App Undisclosed Vulnerability	No Findings	
WordPress User Enumeration	No Findings	

Domain Attacks		100
<u>CRITICAL</u> No Critical severity tests in this section		<u>LOW</u> Domain Typosquatting No Findings
<u>HIGH</u> Domain Hijacking No Findings		<u>INFO</u> Domain Upcoming Expiration No Findings
<u>MEDIUM</u> No Medium severity tests in this section		Newly Registered Domains No Findings

Exposed Services

96

CRITICAL

Exposed Database Services

No Findings

Exposed Services Used in Ransomware Campaigns

No Findings

HIGH

Exposed Cleartext Management Services

No Findings

MEDIUM

Exposed Console Services

No Findings

Exposed OT Devices

No Findings

LOW

Exposed Bad Practice Administration Services

1 issues

Exposed Common Gaming Services

No Findings

Exposed Common Trojan Services

No Findings

INFO

No Info severity tests in this section

Technologies

100

CRITICAL

Technologies with Known Exploited Vulnerabilities

No Findings

HIGH

Technologies with High Severity Vulnerabilities

No Findings

MEDIUM

Technologies with Medium Severity Vulnerabilities

No Findings

LOW

Technologies with Low Severity Vulnerabilities

No Findings

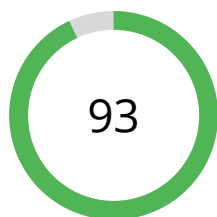
Technologies with Outdated Version

No Findings

INFO

No Info severity tests in this section

Human



Issues By Sub-Category

Responsiveness			100
<u>CRITICAL</u> No Critical severity tests in this section		<u>LOW</u> Asset Reputation Resolution	No Findings
<u>HIGH</u> No High severity tests in this section		<u>INFO</u> No Info severity tests in this section	
<u>MEDIUM</u> Critical Findings Resolution	No Findings		
Technologies Patching	--		
Employee Attack Surface			100
<u>CRITICAL</u> Compromised Credentials of Company Employees	No Findings	<u>LOW</u> Employee High Attack Likelihood (Top 10)	No Findings
		Employee Public Digital Footprint	No Findings
<u>HIGH</u> No High severity tests in this section		Employees in Breached Account Dumps	No Findings
<u>MEDIUM</u> Employee High Attack Likelihood	No Findings	<u>INFO</u> Compromised Credentials of Company Services	No Findings
Security Team			--
<u>CRITICAL</u> No Critical severity tests in this section		<u>LOW</u> Bug Bounty Program	--
<u>HIGH</u> No High severity tests in this section		Size of Information Security Team	--
<u>MEDIUM</u> Presence of CISO	--	<u>INFO</u> No Info severity tests in this section	
Presence of Dedicated Information Security Team	--		

CRITICAL

No Critical severity tests in this section

HIGH

No High severity tests in this section

MEDIUM

No Medium severity tests in this section

LOW

Facebook Company Profile

1 issues

LinkedIn Company Profile

No Findings

X Company Profile

1 issues

INFO

No Info severity tests in this section