TLP:AMBER

CYBERSECURITY DASHBOARD REPORT

GLESEC

September 04, 2026

TLP AMBER
CYBERSECURITY DASHBOARD REPORT

About this report

This is a SKYWATCH report that presents the most up-to-date information for the Cybersecurity Dashboard.

Cybersecurity Overview

Global Cybersecurity Condition

n/a

Threat Level

n/a

Active Critical/High GNEs

n/a

Exposure Pressure

n/a

Protection Effectiveness

n/a

Cybersecurity Workflow Health

n/a

LATAM HQ
+507 836-5355

US HQ
+1 (321) 430-0500

Risk & Intelligence

Active Risk Drivers

Rank	Score	Condition	Risk Driver	GNE	Case	State	Priority	Age (d)	SLA	Owner
1	56	Elevated	Internal user deleted or moved a SoftwareMine	-	47,507	Answered	P2	64.20	OVERDUE	Alejandro Vargas
2	56	Elevated	High Persistency Detection	15	49,189	Answered	P2	55.50	OVERDUE	Deyka Atencio
3	56	Elevated	High Persistency Detection	15	50,829	Answered	P2	45.00	OVERDUE	Deyka Atencio
4	56	Elevated	High Persistency Detection	15	52,972	Answered	P2	35.80	OVERDUE	Deyka Atencio
5	56	Elevated	Change in Systems Availability	13	53,233	Answered	P2	35.10	OVERDUE	-
6	56	Elevated	High Persistency Detection	15	54,607	Answered	P2	31.20	OVERDUE	Genesis Rodr&#xfffd;guez
7	53	Elevated	ClickLock Stealer Targets macOS Users Via ClickFix Social Engineering	-	55,088	Answered	P2	27.60	OVERDUE	Jorge Carracedo
8	53	Elevated	Shai-Hulud-Style npm Worm Hits	-	55,539	Answered	P2	23.70	OVERDUE	Nadji Salazar
9	53	Elevated	High Persistency Detection	15	55,619	Answered	P2	22.50	OVERDUE	Jan De Gracia
10	53	Elevated	Operation Dream Job Exploits Zero-Day In Targeted Attack	-	55,935	Answered	P2	18.20	OVERDUE	Nadji Salazar

LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

TLP:AMBER

CYBERSECURITY DASHBOARD REPORT

GLESEC 09/04/2026

Threat & Validation Intelligence

Threat	Category	RS/TRS	Target Sector	Validation	Relevance
CobaltStrike	Malware Family	74/69	—	—	58
ClearFake	Malware Family	74/69	—	—	56
Mozi	Malware Family	74/69	—	—	54
Mirai	Malware Family	74/69	—	—	48
ClickFix	Malware Family	74/69	—	—	42
Cobalt Strike	Malware Family	74/69	—	—	38
Vidar	Malware Family	74/69	—	—	34
ACRStealer	Malware Family	74/69	—	—	32
asyncrat	Malware Family	74/69	—	—	24
gafgyt	Malware Family	74/69	—	—	23

Protection Effectiveness Control Matrix

Control	Status	Blocked 30d	BAS risk	GapScore	Condition
DLP	Validated (BAS)	—	68	68	High
Web App Firewall (WAF)	Validated + Deployed	—	51	51	Elevated
Email Gateway	Deployed / silent	—	—	50	Elevated
EDR	Validated + Deployed	—	45	45	Elevated
IPS / Firewall (UTM/DDoS)	Validated + Deployed	15,357	34	34	Guarded
Web Gateway	Validated (BAS)	—	23	23	Guarded
AntiVirus	Validated + Deployed	—	19	19	Stable

LATAM HQ
+507 836-5355

US HQ
+1 (321) 430-0500

TLP:AMBER

CYBERSECURITY DASHBOARD REPORT

GLESEC 09/04/2026

Exposure Intelligence

Rank	Exposure Class	Asset/Domain	Critical	High	Total C/H	Business Impact	Score	Condition	Last Seen
-	MATRIX	Ext C:0 H:2 | Int C:149 H:226 | IoT:3 | URLs:38	149	228	377	-	0	-	-
1	Internal	netbox.in.glesec.com	8	41	49	High	83	Critical	2026-08-29
2	Internal	192.168.52.28	5	6	11	High	83	Critical	2026-08-29
3	IoT	5 IoT/OT devices (max risk 10.00)	3	0	3	IoT/OT	83	Critical	2026-09-03
4	Domain	5 apex / 15 subdomains / 38 exposed URLs	0	38	38	External Surface	80	High	2026-09-03
5	Internal	bancodelta-itsmine-connector.in.glesec.com	45	20	65	Medium	76	High	2026-08-29
6	Internal	192.168.100.190	11	39	50	Medium	76	High	2026-08-29
7	Internal	GLESEC-AWS-CYMULATE.GLESEC.com	10	23	33	Medium	76	High	2026-08-29
8	Internal	192.168.100.73	9	26	35	Medium	76	High	2026-08-29
9	Internal	dc-02.in.glesec.com	8	12	20	Medium	76	High	2026-08-29
10	Internal	dc-01.in.glesec.com	8	11	19	Medium	76	High	2026-08-29

Operations

Operational Bottlenecks

Where	Type	Cases	Worst Age (d)	Backlog 7d	Condition
ALL SERVICES	Stalled	3,292	2,612	+2.4%	Degraded
(none)	Stalled	3,147	2,612	+2.0%	Degraded
MSS-SIEM	Stalled	30	384	+0.0%	Degraded
MSS-VM	Stalled	19	2,102	+0.0%	Degraded
MSS-EASM	Stalled	18	436	-10.00%	Degraded
MSS-INT	Stalled	16	238	+0.0%	Degraded
MSS-DDOS	Stalled	9	56	+125.0%	Guarded
MSS-INT-V	Stalled	8	186	+83.3%	Degraded
MSS-BAS-WEB	Stalled	8	182	+0.0%	Guarded
MSS-WAF-CLOUD	Stalled	8	252	+233.3%	Guarded
MSS-CSM	Stalled	7	1,346	-12.50%	Degraded
MSS-EDR	Stalled	3	211	+0.0%	Degraded

LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

TLP:AMBER

CYBERSECURITY DASHBOARD REPORT

GLESEC 09/04/2026

Persistent Threat Pressure

Rank	Source (Threat Entity)	Target Asset	Blocked 30d	% of Total	Trend	Business Impact	Score	Condition
1	172.110.223.179	intranet-dev.in.glesec.com (10.4.0.60)	210	7.43	new	High	66	High
2	100.64.0.198	PRTG.in.glesec.com (192.168.100.173)	400	14.16	new	Medium	61	High
3	172.110.223.179	Unknown (10.4.0.200)	210	7.43	new	Medium	61	High
4	172.28.1.77	100.64.0.227	306	10.83	new	Unknown	54	Elevated
5	172.110.223.127	gmp.glesec.com (10.4.0.51)	6	0.21	new	Critical	44	Elevated
6	66.132.172.251	gmp.glesec.com (10.4.0.51)	3	0.11	new	Critical	44	Elevated
7	172.110.223.154	gmp.glesec.com (10.4.0.51)	3	0.11	new	Critical	44	Elevated
8	18.116.101.220	gmp.glesec.com (10.4.0.51)	3	0.11	new	Critical	44	Elevated
9	18.218.118.203	gmp.glesec.com (10.4.0.51)	3	0.11	new	Critical	44	Elevated
10	66.132.172.252	gmp.glesec.com (10.4.0.51)	3	0.11	new	Critical	44	Elevated

Identity & Access Intelligence

Indicator	Value	Signal
Identity Risk Score	54	Elevated
Auth Failures (7d)	76	Attention
Denied Rate	16.30%	Elevated
Account Lockouts	0	Clear
Fraud Flags	0	Clear
At-Risk Users	7	7 users

LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

IoT/OT Exposure

Device	Type	Managed?	Risk (0-10)	Business Impact	Condition	Exposure
- FLEET IoT/OT EXPOSURE -	8 devices	3 unmanaged-crit	7.10	1 unknown	Score 71/100	
Admin USA Phone	SIP-T23G	Unmanaged	10.00	(not in CAD)	Critical	UNMANAGED CRITICAL
GOC USA Phone	SIP-T23G	Unmanaged	10.00	(not in CAD)	Critical	UNMANAGED CRITICAL
GOC USA S&E Phone	SIP-T23G	Unmanaged	9.90	(not in CAD)	Critical	UNMANAGED CRITICAL
GLESEC-AWS-UTM-1A	PA-VM	Managed	10.00	(not in CAD)	Critical	Critical risk
GLESEC-AWS-UTM-1B	PA-VM	Managed	10.00	(not in CAD)	Critical	Critical risk
MSS-UTM-PaloAlto-Panorama	Panorama	Managed	0.00	(not in CAD)	Stable	UNKNOWN - no risk data
GOC USA Router	SG-3100	Unmanaged	0.00	(not in CAD)	Stable	OK
HP OfficeJet Pro 6,968 All-in-One	HP OfficeJet Pro 6,968 All-in-One	Unmanaged	0.00	(not in CAD)	Stable	OK

TLP:AMBER = Limited disclosure, restricted to participants' organizations. Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved. Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. **Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.**

LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

TLP:AMBER

CYBERSECURITY DASHBOARD REPORT

HOW CAN WE HELP?

Contact us today for more information on
our services and security solutions.

LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500