International Software Systems - Weekly Report

Weekly Report
Aug 25, 2025 - Aug 31, 2025

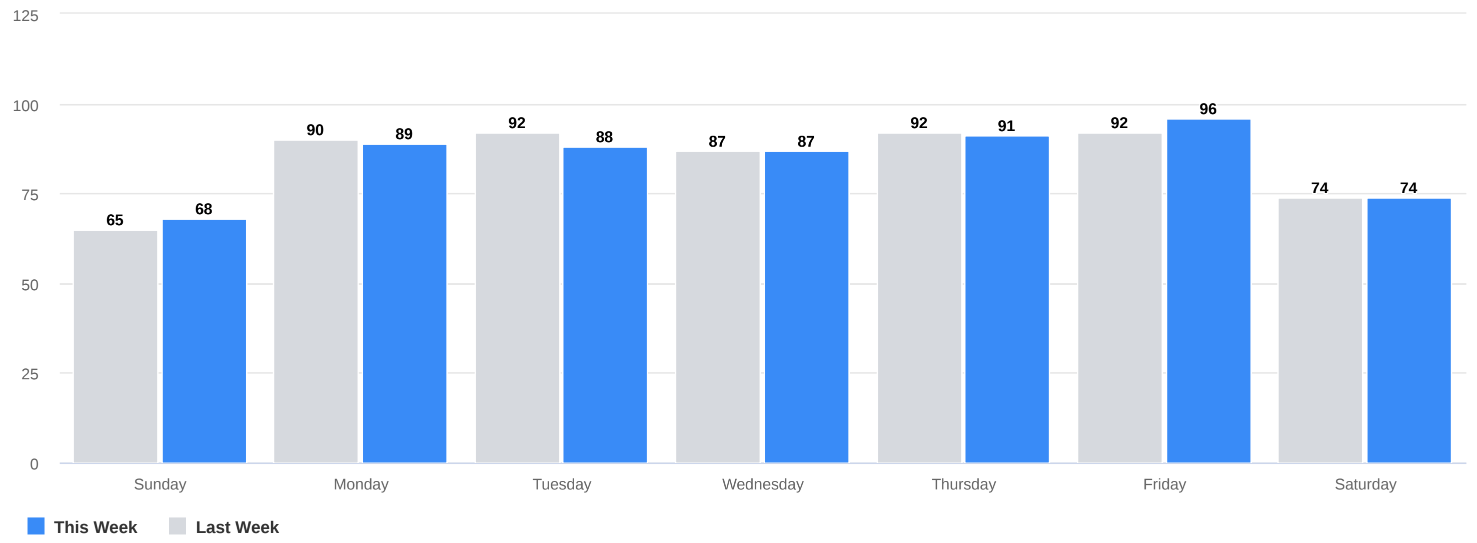
Account Settings
Update Account Information

Contacts
ahurd@issi-software.com
upokhrel@issi-software.com
bganti@issi-software.com

Response Mode
Authorize

Devices Sending Telemetry

View All



Sophos MDR Cases

Total Cases: 0 View All

Cases by Status

0 View
New

0 View
In Progress

0 View
Action Required

0 View
Resolved/Closed

Cases by Type

0 View
MDR Investigation

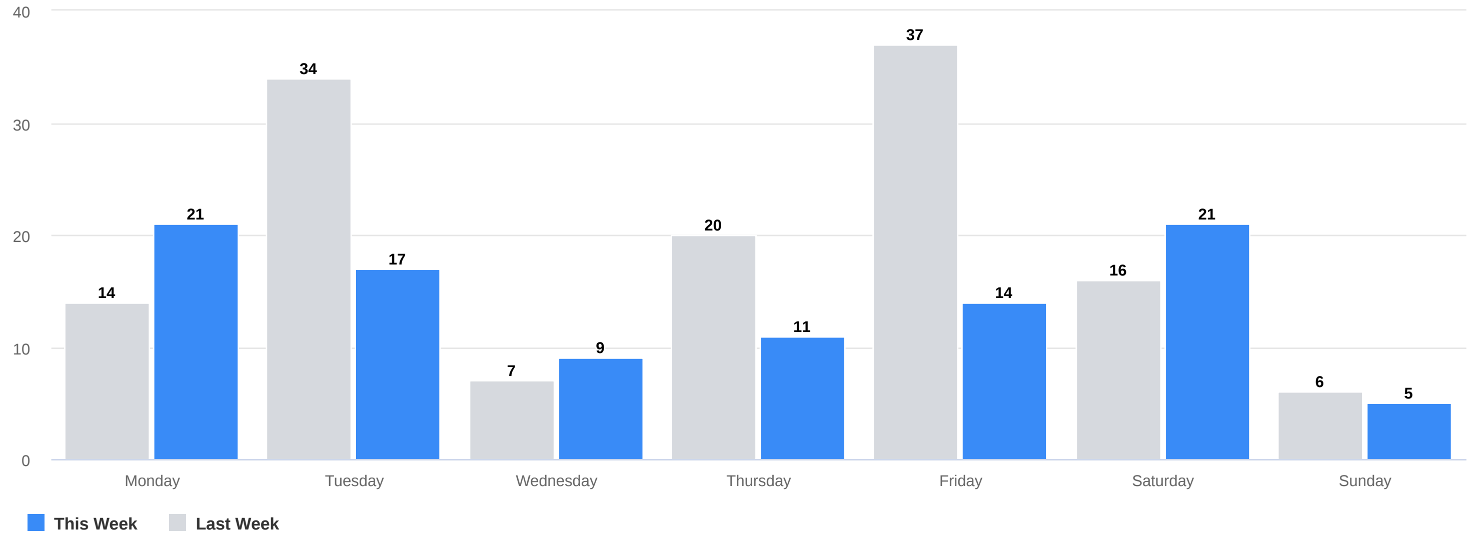
0 View
Health Check

0 View
Customer Requested Investigation

Sophos Detections

Detections This Week

View All



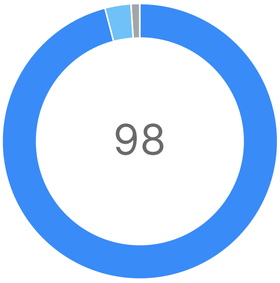
International Software Systems - Weekly Report

Weekly Report
Aug 25, 2025 - Aug 31, 2025

Account Settings	Contacts	Response Mode
Update Account Information	ahurd@issi-software.com upokhrel@issi-software.com bganti@issi-software.com	Authorize

Detection Classification Summary

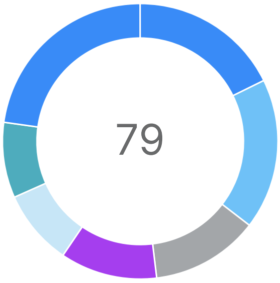
View More



●	Suspicious Activity	94
●	Defense Evasion	3
●	Credential Access	1

MITRE ATT&CK Framework

View More



●	Archive via Utility	14
●	PowerShell	14
●	Windows Command Shell	10
●	Code Signing Certificates	9
●	Ingress Tool Transfer	7
●	NTDS	7
	All Other Techniques	18

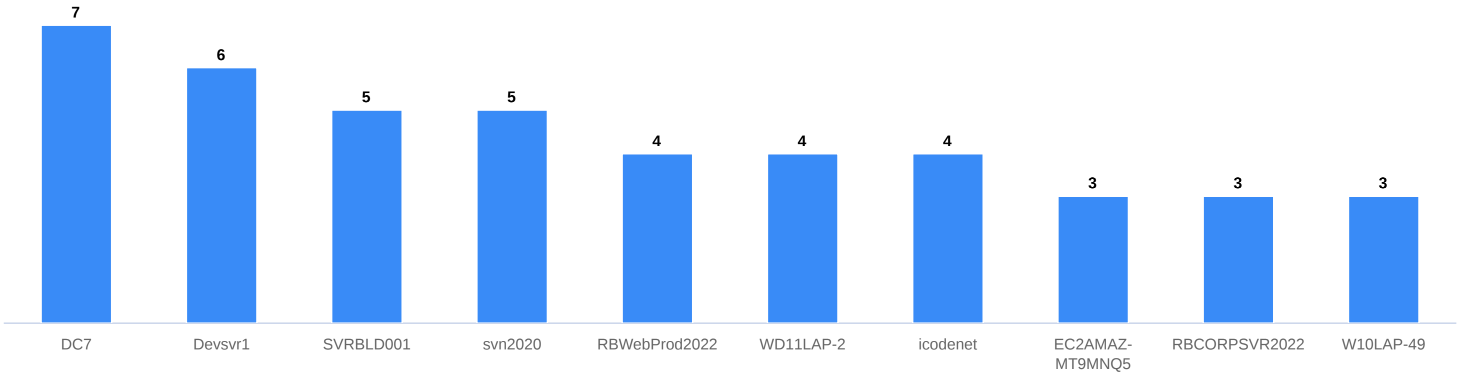
MDR Integrations with Detections

View More

MDR integrations with events that matched rules to generate detections for this week.

Endpoint Sophos Endpoint	58
Cloud Microsoft	39
Compound Sophos	1

Top 10 Devices with Most Detections



Top 10 Devices with Most Detections

Hostname	Top Detections	Count	Category
DC7	WIN-DET-CREDS-NTDS-DUMP-FILE-1	7	Suspicious Activity
Devsvr1	WIN-DET-COLLECT-ARCHIVE-FILE-WRITE-1	6	Suspicious Activity
SVRBLD001	WIN-DET-COLLECT-ARCHIVE-FILE-WRITE-1	5	Suspicious Activity
svn2020	WIN-DET-T1553.002 WIN-DET-T1587.002	3 2	Suspicious Activity Suspicious Activity
RBWebProd2022	WIN-CRD-DM-BRUTE-FORCE-1	4	Suspicious Activity
WD11LAP-2	WIN-DET-EVADE-SAFE-MODE-SERVICE-INSTALLED-1	4	Suspicious Activity
icodenet	WIN-DET-T1587.002	4	Suspicious Activity
EC2AMAZ-MT9MNQ5	WIN-CRD-DM-BRUTE-FORCE-1	3	Suspicious Activity
RBCORPSVR2022	WIN-DET-COLLECT-ARCHIVE-FILE-WRITE-1	3	Suspicious Activity
W10LAP-49	WIN-DET-PERSIST-SCHEDULED-TASK-2 WIN-DET-T1529	2 1	Suspicious Activity Suspicious Activity

Top 5 Detections

Detection Name	Count	Description	Category
MS-SEC-GRAPH-EMAIL-REPORTED-BY-USER-AS-JUNK	18	This alert is triggered when any email message is reported as junk by users -V1.0.0.0	Suspicious Activity
WIN-DET-COLLECT-ARCHIVE-FILE-WRITE-1	14	-	Suspicious Activity
MS-SEC-GRAPH-EMAIL-MESSAGES-CONTAINING-MALICIOUS-URL-REMOVED-AFTER-DELIVERYâ€‹	7	Emails with malicious URL that were delivered and later removed - V1.0.0.3	Suspicious Activity
WIN-CRD-DM-BRUTE-FORCE-1	7	Windows Event Brute Force Attempt Detected	Suspicious Activity
WIN-DET-CREDS-NTDS-DUMP-FILE-1	7	-	Suspicious Activity

Bottom 5 Detections

Detection Name	Count	Description	Category
MS-SEC-GRAPH-CREATION-OF-FORWARDING/REDIRECT-RULE	1	This alert is triggered when someone in your organization sets up auto-forwarding, email forwarding, redirect rule or a mail flow rule -...	Suspicious Activity
MS-SEC-GRAPH-EMAIL-REPORTED-BY-USER-AS-NOT-JUNK	1	This alert is triggered when any email message is reported as not junk by users -V1.0.0.0	Suspicious Activity
PD-WIN-CRD-BRUTE-FORCE-EXPOSED-DEVICE-1	1	Brute force targeting EC2AMAZ-MT9MNQ5 as been observed that has not previously been observed in the past 7 days. This indicates...	Credential Access
WIN-DET-EVADE-DLL-TRUSTED-EXE-SIDELOADING-1	1	-	Suspicious Activity
WIN-DET-T1053.005	1	-	Suspicious Activity

Additional Sophos MDR Efforts

Previous 7-days Response Actions

No active cases for this report

We didn't see active case data to generate a useful visual representation.

Previous 7-days Communications

No active cases for this report

We didn't see active case data to generate a useful visual representation.