

SECURITY OPERATIONS CENTER

Report SOC

January — September 2026

signum SOC

Period January — September 2026

Tenant signum SOC

Classification Confidential

Generated on September 30, 2026

Contents

1	Active SOC Services	2
2	Executive Summary	2
2.1	Historical Trend (last 6 months)	2
2.2	Monthly Trend for the Period	3
2.3	Mean Time to Acknowledge (MTTA)	3
2.4	Correlation Efficiency	3
2.5	Mean Time to Resolve (MTTR)	3
2.6	Alarm Distribution by Status	4
3	Security Incidents	4
3.1	Distribution by Severity	4
3.2	By Source Service	4
3.3	Root Cause Analysis	4
3.4	Incident List	4
4	Top 3 Incidents	5
5	Operational Detail	5
5.1	Top 10 Hosts by Alarm Volume	5
5.2	Top Detection Rules	5
5.3	Top Source IP	5
5.4	Top Destination IP	6
5.5	SOC Analyst Activity	6
5.6	Notable Alarm List	6

1 Active SOC Services

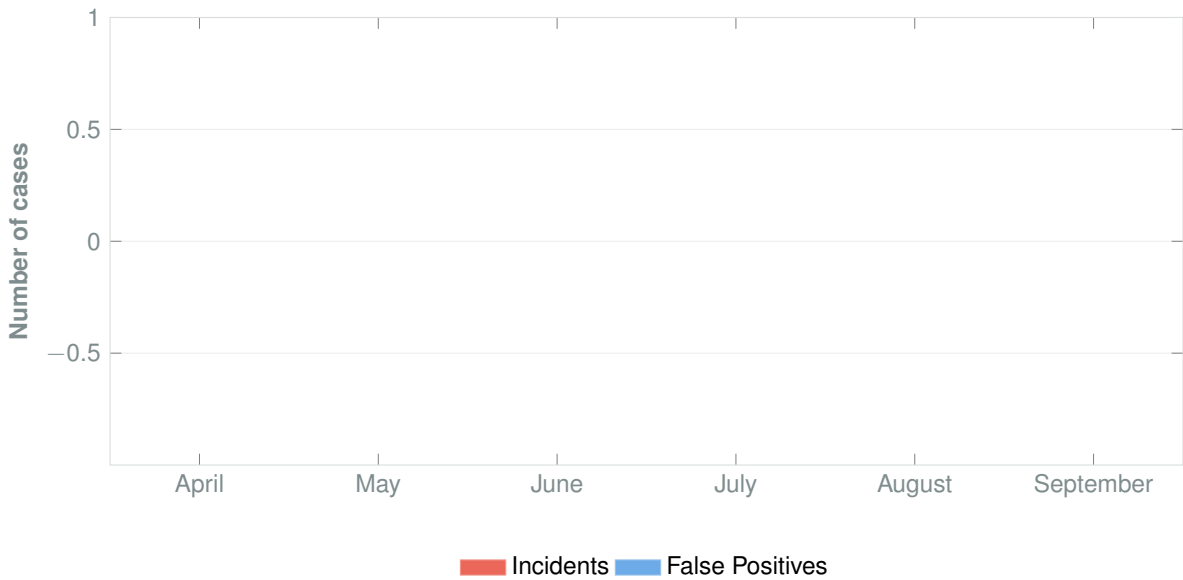
Services included in the security perimeter and under continuous monitoring.

Service	Status	Product
crowdstrike	active	crowdstrike
custom	active	custom
suricata	active	suricata
wazuh	active	wazuh
zabbix	active	zabbix

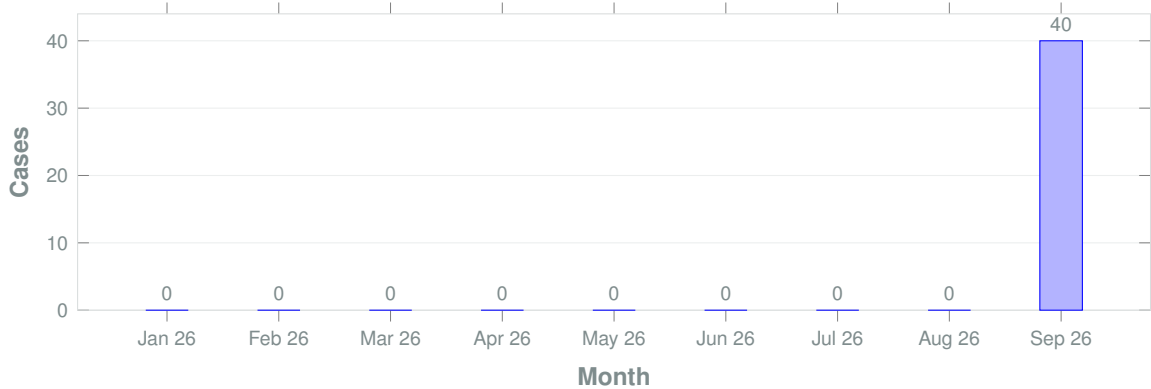
2 Executive Summary



2.1 Historical Trend (last 6 months)



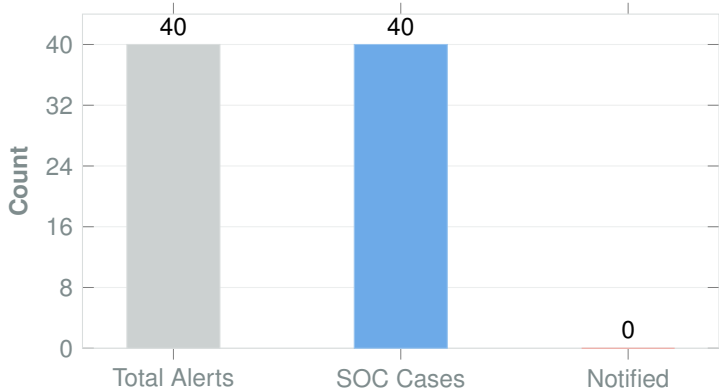
2.2 Monthly Trend for the Period



2.3 Mean Time to Acknowledge (MTTA)

Severity	Mean time (hours)
Critical	N/A
High	N/A
Medium	N/A
Low	N/A
Info	N/A

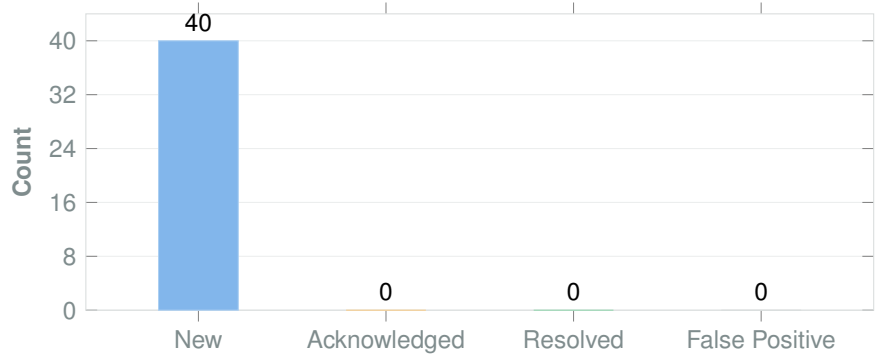
2.4 Correlation Efficiency



2.5 Mean Time to Resolve (MTTR)

Severity	Tempo medio (ore)
Critical	N/A
High	N/A
Medium	N/A
Low	N/A
Info	N/A

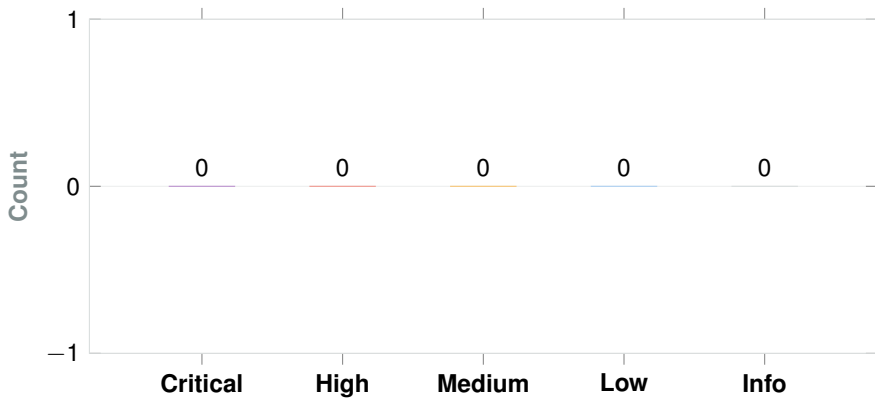
2.6 Alarm Distribution by Status



3 Security Incidents

During the period 0 incidents were handled, of which 0 were reported to the customer.

3.1 Distribution by Severity



3.2 By Source Service

Service	Cases
suricata	11
crowdstrike	9
custom	8
wazuh	8
zabbix	4

3.3 Root Cause Analysis

Root Cause	N.	Description
—	0	—

3.4 Incident List

Details of all incidents handled in the period, ordered by severity.

ID	Title	Severity	Status	Date
No incidents recorded in the period				

4 Top 3 Incidents

Most significant incidents in the reporting period.

No significant incidents reported in the period.

5 Operational Detail

5.1 Top 10 Hosts by Alarm Volume

Host	Alarms
SCADA-RTU-07	6
SW-CORE-01	6
PLC-OT-12	6
DC01	5
web-server-01	3
VPN-GW-01	3
FW-EDGE-01	3
MAIL-GW02	2
DB-PROD-04	2
SRV186	2

5.2 Top Detection Rules

Rule	Occurrences
Mass File Rename Detected Rule	4
Database Dump Detected Rule	3
Trojan Activity Detected Rule	2
Unauthorized Access to Restricted Resource Rule	2
Known CVE Exploitation Attempt Rule	2
DNS Tunneling Suspected Rule	2
Security Tool Disabled Rule	2
Ransomware Encryption Behavior Detected Rule	2
Unpatched Service Exposed Rule	1
Credential Dumping Detected (LSASS Access) Rule	1

5.3 Top Source IP

Source IP	Occurrences
10.35.63.235	2
38.137.54.130	1
144.39.48.76	1
97.73.53.111	1
52.168.121.243	1

5.4 Top Destination IP

Destination IP	Occurrences
10.7.116.35	2
10.8.238.90	1
10.3.148.189	1
10.37.155.168	1
10.10.67.136	1

5.5 SOC Analyst Activity

Analyst	Alarms handled
—	0

5.6 Notable Alarm List

Most significant alarms of the period (up to 40), ordered by severity and date.

Date	Severity	Source	Description	Status
2026-09-26	critical	wazuh	LSASS Memory Access - Credential Dumping Pattern	new
2026-09-16	critical	zabbix	DNS Tunneling Suspected Rule	new
2026-09-16	critical	suricata	Suspicious Executable Dropped Rule	new
2026-09-26	high	crowdstrike	Trojan Activity Detected Rule	new
2026-09-26	high	custom	Unauthorized Access to Restricted Resource Rule	new
2026-09-26	high	wazuh	Credential Dumping Detected (LSASS Access) Rule	new
2026-09-23	high	suricata	Sensitive File Access and Transfer Detected Rule	new
2026-09-19	high	custom	Security Tool Disabled Rule	new
2026-09-18	high	wazuh	Unauthorized Network Access Detected Rule	new
2026-09-16	high	custom	Mass File Rename Detected Rule	new
2026-09-27	medium	suricata	Unpatched Service Exposed Rule	new
2026-09-27	medium	crowdstrike	Mass File Rename Detected Rule	new
2026-09-25	medium	suricata	Mass File Rename Detected Rule	new
2026-09-24	medium	custom	USB Storage Device Policy Violation Rule	new
2026-09-24	medium	crowdstrike	Port Scan Detected Rule	new
2026-09-22	medium	wazuh	Log Clearing Detected Rule	new
2026-09-18	medium	zabbix	Security Tool Disabled Rule	new
2026-09-18	medium	crowdstrike	Database Dump Detected Rule	new
2026-09-17	medium	suricata	Database Dump Detected Rule	new
2026-09-17	medium	wazuh	New Privileged Account Created Rule	new

Date	Severity	Source	Description	Status
2026-09-16	medium	suricata	Unusual PLC Write Operation Detected Rule	new
2026-09-16	medium	custom	Database Dump Detected Rule	new
2026-09-15	medium	zabbix	Suspicious External Login Detected Rule	new
2026-09-15	medium	custom	Malicious Attachment Executed Rule	new
2026-09-24	low	crowdstrike	Known CVE Exploitation Attempt Rule	new
2026-09-24	low	custom	Network Enumeration Detected Rule	new
2026-09-24	low	wazuh	Privilege Misuse Detected Rule	new
2026-09-22	low	zabbix	Unauthorized Access to Restricted Resource Rule	new
2026-09-21	low	wazuh	Known CVE Exploitation Attempt Rule	new
2026-09-19	low	crowdstrike	DNS Tunneling Suspected Rule	new
2026-09-19	low	suricata	Ransomware Encryption Behavior Detected Rule	new
2026-09-19	low	suricata	Suspicious PowerShell Execution Rule	new
2026-09-15	low	suricata	Ransomware Encryption Behavior Detected Rule	new
2026-09-15	low	wazuh	Trojan Activity Detected Rule	new
2026-09-14	low	suricata	Intrusion Attempt Detected Rule	new
2026-09-14	low	crowdstrike	Pass-the-Hash Attempt Detected Rule	new
2026-09-24	info	custom	Credential Harvesting Attempt Detected Rule	new
2026-09-21	info	crowdstrike	Mass File Rename Detected Rule	new
2026-09-14	info	crowdstrike	Firewall Rule Violation Detected Rule	new
2026-09-14	info	suricata	Account Lockout Threshold Reached Rule	new

End of report — Confidential document

Security Operations Center — signum SOC