

SECURITY OPERATIONS CENTER

Report SOC

Gennaio — Dicembre 2026

signum SOC

Periodo Gennaio — Dicembre 2026

Tenant signum SOC

Classificazione **Confidenziale**

Generato il 30 settembre 2026

Indice

1	Servizi SOC Attivi	2
2	Executive Summary	2
2.1	Andamento Storico (ultimi 6 mesi)	2
2.2	Andamento Mensile del Periodo	3
2.3	Tempo Medio di Presa in Carico (MTTA)	3
2.4	Efficienza di Correlazione	3
2.5	Tempo Medio di Risoluzione (MTTR)	3
2.6	Distribuzione Allarmi per Status	4
3	Incidenti di Sicurezza	4
3.1	Distribuzione per Severity	4
3.2	Per Servizio Sorgente	4
3.3	Root Cause Analysis	4
3.4	Elenco Incidenti	4
4	Top 3 Incidenti	5
5	Dettaglio Operativo	5
5.1	Top 10 Host per Volume Allarmi	5
5.2	Top Detection Rules	5
5.3	Top Source IP	5
5.4	Top Destination IP	6
5.5	Attività Analisti SOC	6
5.6	Elenco Allarmi Rilevanti	6

1 Servizi SOC Attivi

Servizi inclusi nel perimetro di sicurezza e oggetto di monitoraggio continuativo.

Servizio	Stato	Prodotto
crowdstrike	active	crowdstrike
custom	active	custom
suricata	active	suricata
wazuh	active	wazuh
zabbix	active	zabbix

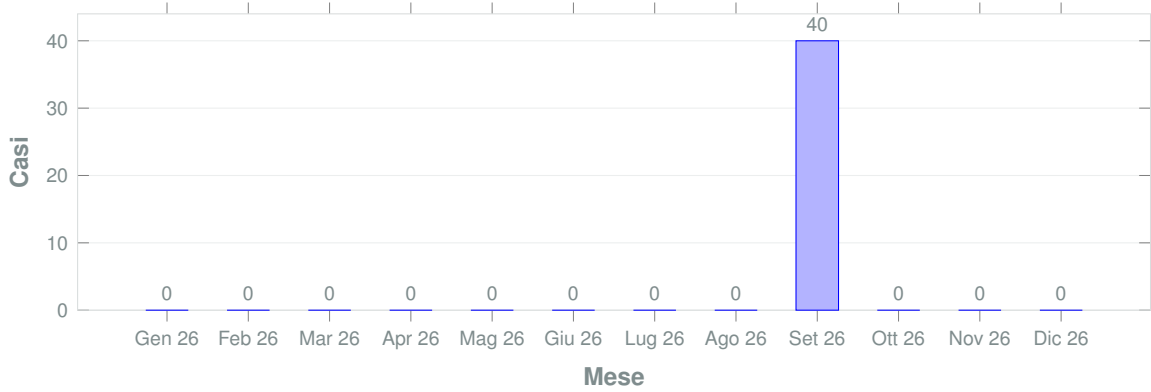
2 Executive Summary



2.1 Andamento Storico (ultimi 6 mesi)



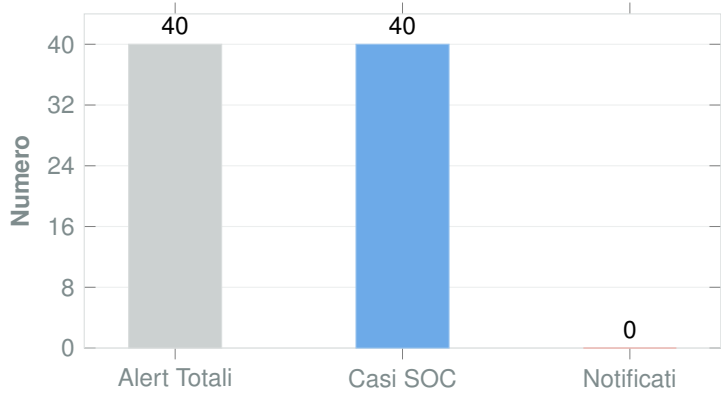
2.2 Andamento Mensile del Periodo



2.3 Tempo Medio di Presa in Carico (MTTA)

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

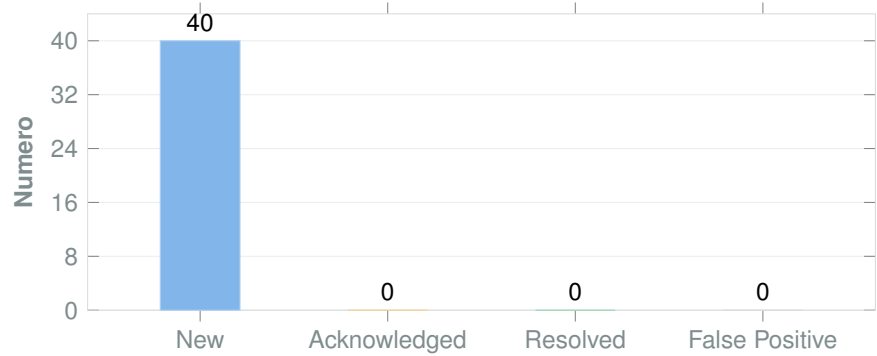
2.4 Efficienza di Correlazione



2.5 Tempo Medio di Risoluzione (MTTR)

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

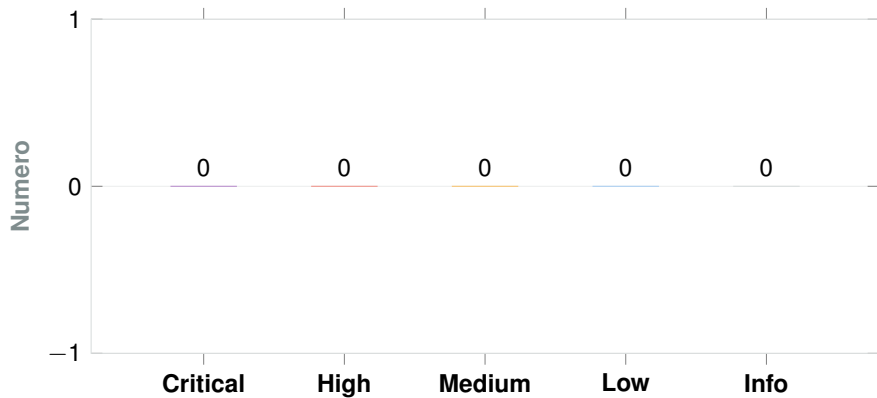
2.6 Distribuzione Allarmi per Status



3 Incidenti di Sicurezza

Nel periodo sono stati gestiti 0 incidenti, di cui 0 segnalati al cliente.

3.1 Distribuzione per Severity



3.2 Per Servizio Sorgente

Servizio	Casi
suricata	11
crowdstrike	9
custom	8
wazuh	8
zabbix	4

3.3 Root Cause Analysis

Root Cause	N.	Descrizione
—	0	—

3.4 Elenco Incidenti

Dettaglio di tutti gli incidenti gestiti nel periodo, ordinati per severity.

ID	Titolo	Severity	Status	Data
Nessun incidente registrato nel periodo				

4 Top 3 Incidenti

Incidenti di maggiore rilevanza nel periodo di riferimento.

Nessun incidente rilevante segnalato nel periodo.

5 Dettaglio Operativo

5.1 Top 10 Host per Volume Allarmi

Host	Allarmi
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	Occorrenze
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	Occorrenze
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	Occorrenze
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 Attività Analisti SOC

Analista	Allarmi gestiti
—	0

5.6 Elenco Allarmi Rilevanti

Allarmi più significativi del periodo (fino a 40), ordinati per severity e data.

Data	Severity	Sorgente	Descrizione	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

Data	Severity	Sorgente	Descrizione	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

Fine del report — Documento confidenziale

Security Operations Center — signum SOC