TLP:AMBER

MSS-EDR REPORT

ACME FINANCIAL SERVICES

September 02, 2026

TLP AMBER
MSS-EDR REPORT

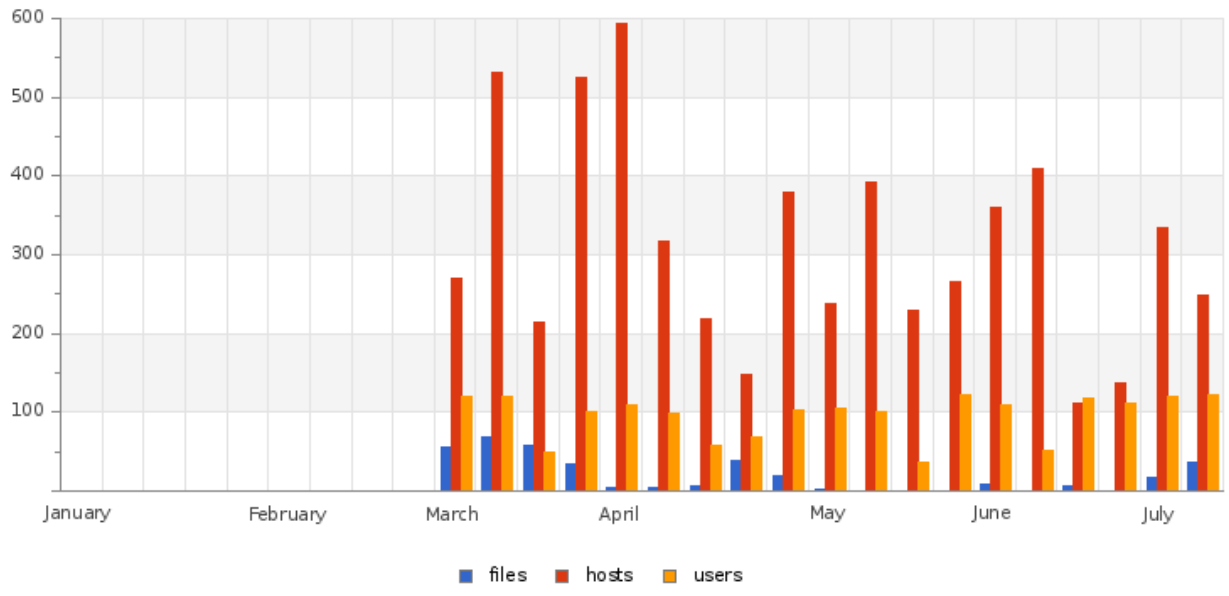
About this report

This is a SKYWATCH report that presents the most up-to-date information for the MSS-EDR as displayed in the service dashboard.

Average Threat - User Defined

98

Threat Score



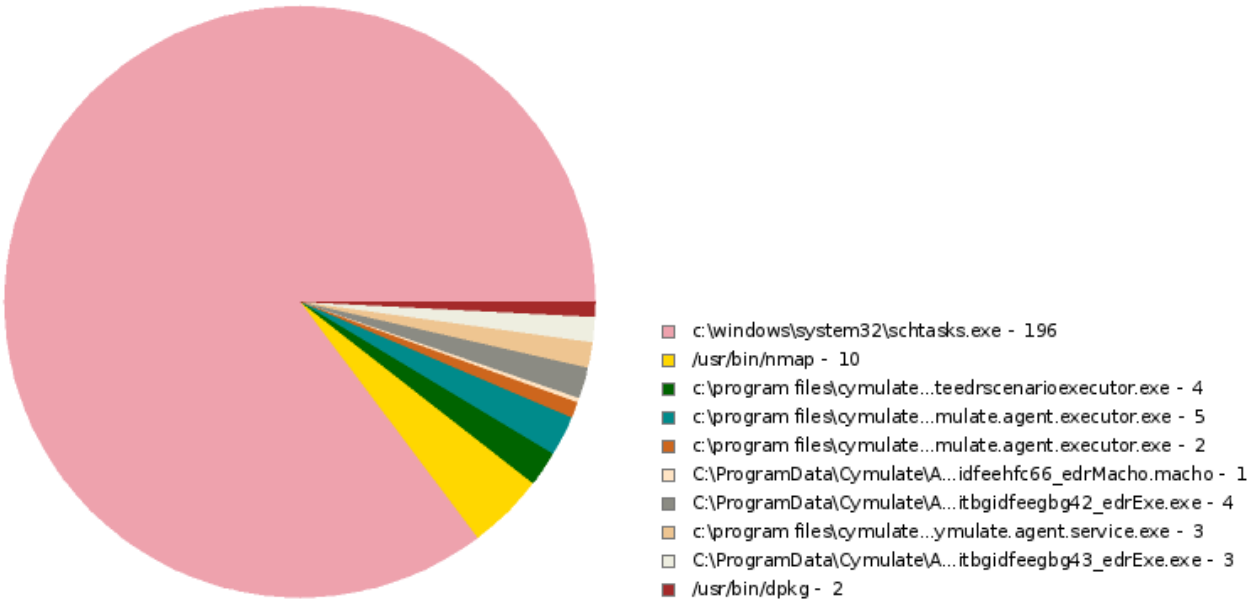
LATAM HQ
+507 836-5355

US HQ
+1 (321) 430-0500

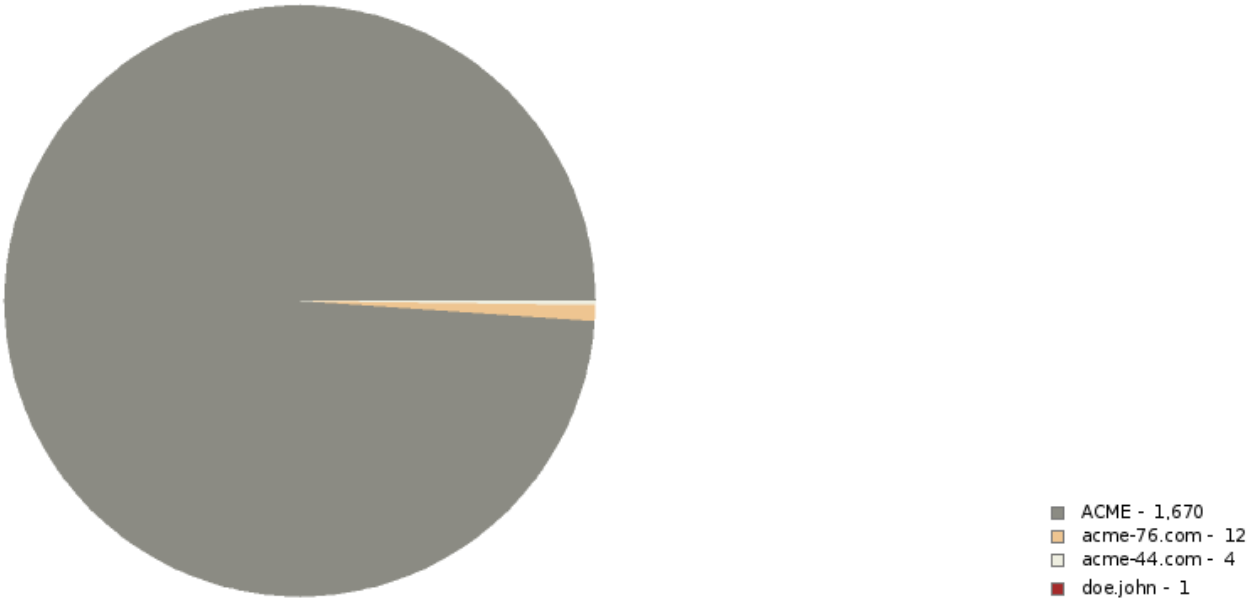
MSS-EDR REPORT

ACME FINANCIAL SERVICES 09/02/2026

Events by File Path - User Defined

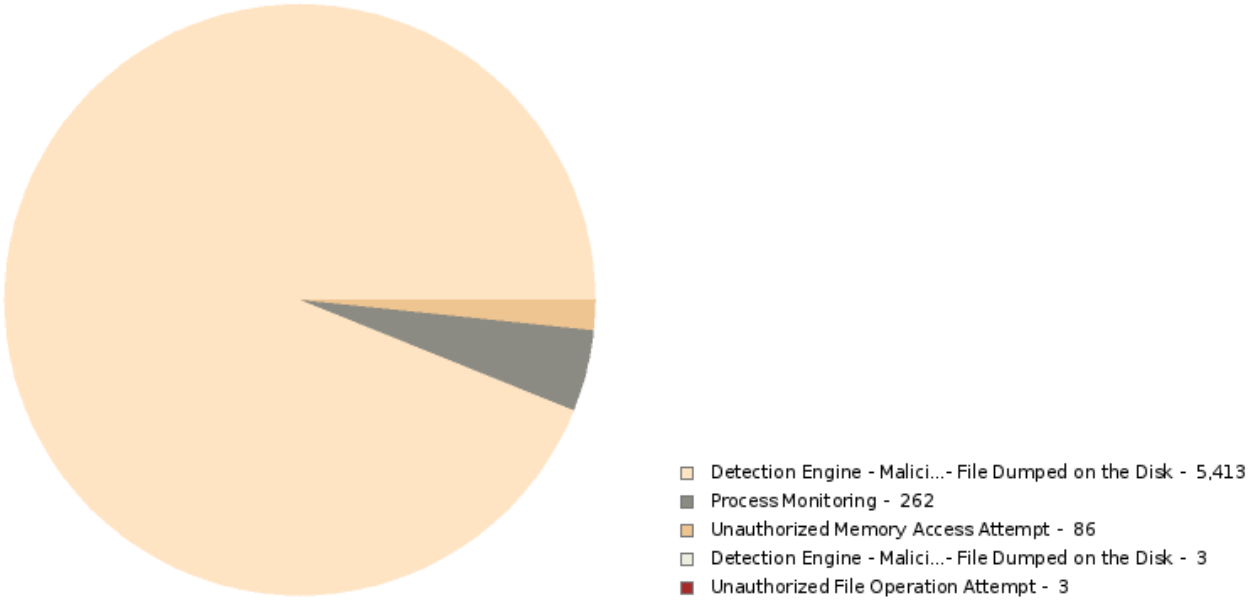


Events by Host Name - User Defined

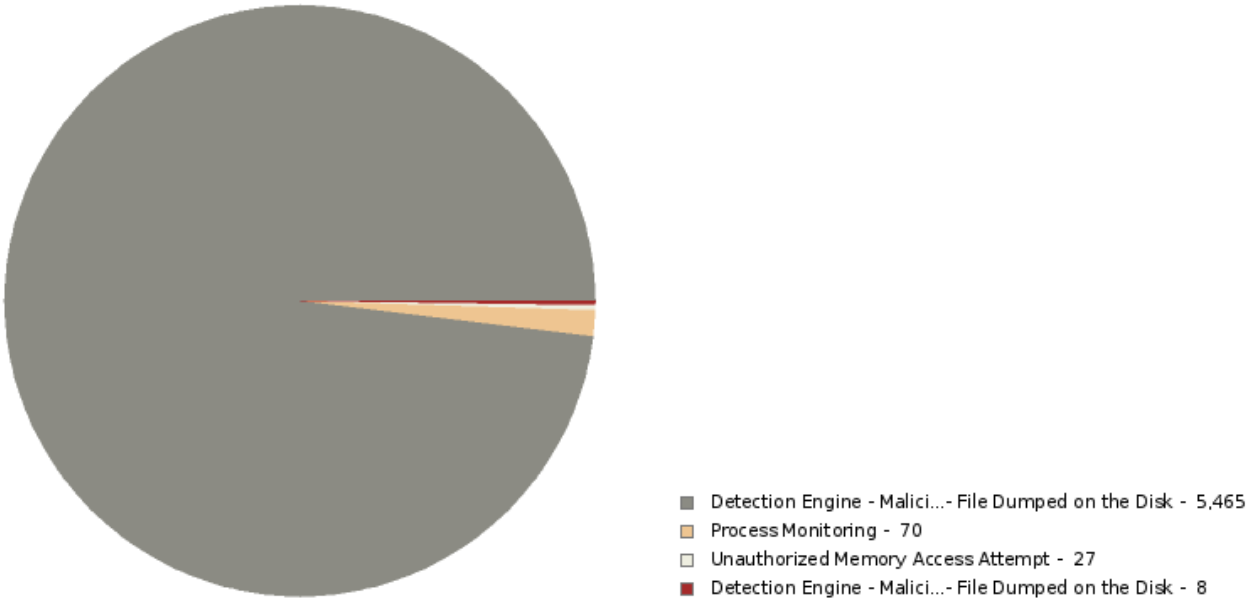


LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

Events by Event Name - User Defined



High Severity Events by Event Name - User Defined



LATAM HQ
+507 836-5355

US HQ
+1 (321) 430-0500

TLP:AMBER

MSS-EDR REPORT

ACME FINANCIAL SERVICES 09/02/2026

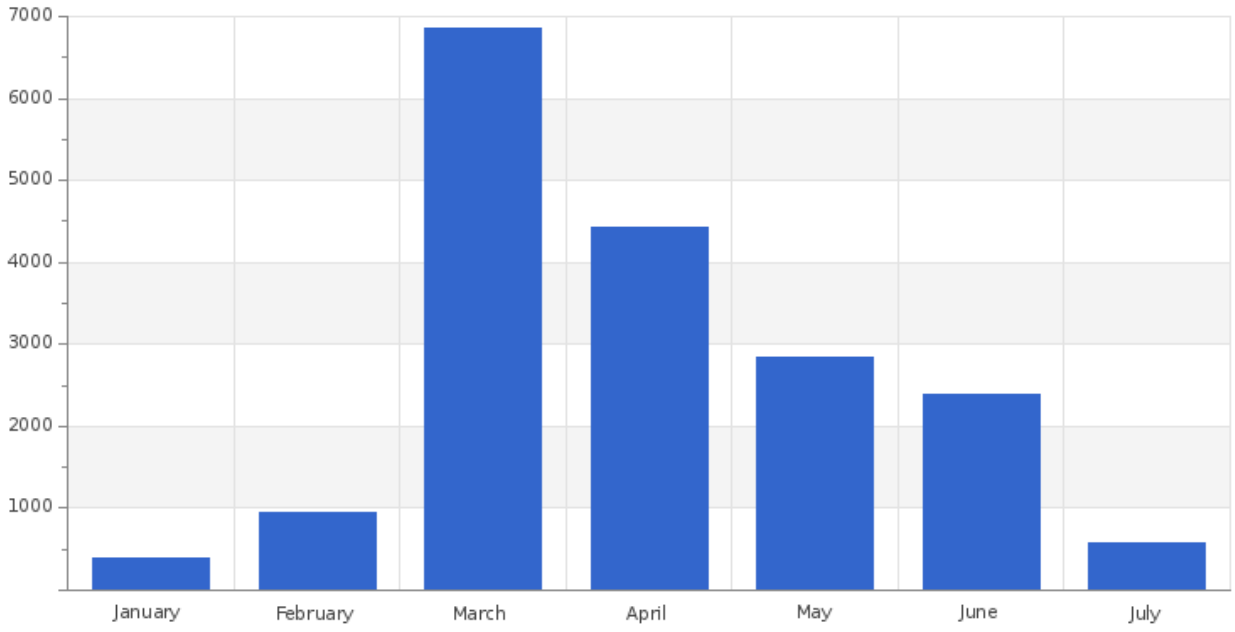
Brute Force Detection by Ratio - User Defined

Host \ User Name	Ratio (Bad : Good)	Probability
jane.doe	153 : 97	1.74

High Severity Events

Host	File Path	Severity	count
ACME	c:\windows\system32\control.exe	7	1
ACME	c:\windows\system32\mshta.exe	7	1
ACME	c:\windows\system32\regsvr32.exe	6	1
ACME	c:\windows\system32\schtasks.exe	7	61
ACME	c:\windows\system32\windowspowershell\v1.0\powershell.exe	2	2
doe.john	pdoe	2	2
jane36	udoe	5	2
acme-44.com	/bin/cat	6	2
acme-44.com	/bin/systemctl	2	2

Events

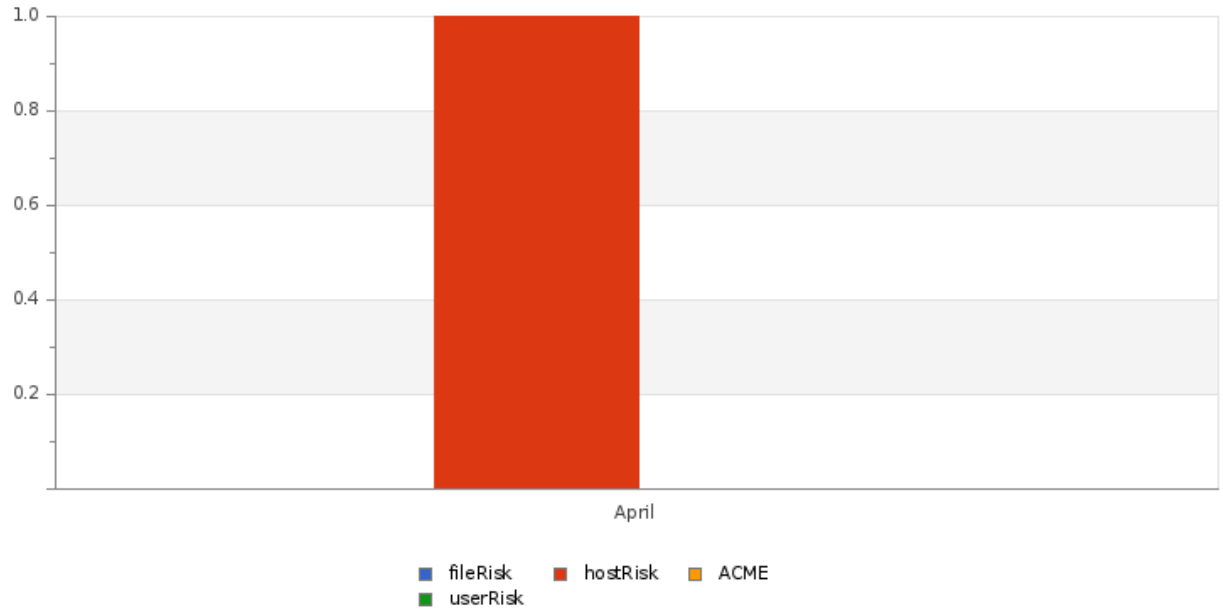


LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

MSS-EDR REPORT

ACME FINANCIAL SERVICES 09/02/2026

Close Alerts *



Total Hosts - User Defined

30

High Severity Events by File Path - User Defined

File Path	Severity	Event Count
C:\ProgramData\Cymulate\AV\64889a45063343e6a9618093\acme-106.com	7	2
C:\ProgramData\Cymulate\AV\64889a45063343e6a9618093\acme-106.com	5	2
C:\ProgramData\Cymulate\AV\64889a45063343e6a9618093\Sample11Xlsx.xlsx	3	2
C:\ProgramData\Cymulate\AV\64889a45063343e6a9618093\acme-106.com	9	1
C:\ProgramData\Cymulate\AV\64889a45063343e6a9618093\Sample13Exe_upx.exe_upx	7	1
C:\ProgramData\Cymulate\AV\64889a45063343e6a9618093\acme-106.com	5	2
C:\ProgramData\Cymulate\AV\64889a45063343e6a9618093\acme-106.com	10	2
C:\ProgramData\Cymulate\AV\64889a45063343e6a9618093\Sample13Xlsx.xlsx	5	2
C:\ProgramData\Cymulate\AV\64889a45063343e6a9618093\acme-106.com	6	1
C:\ProgramData\Cymulate\AV\64889a45063343e6a9618093\acme-106.com	3	1

LATAM HQ
+507 836-5355

US HQ
+1 (321) 430-0500

MSS-EDR REPORT

ACME FINANCIAL SERVICES 09/02/2026

High Severity Events by Host Name - User Defined

Host	Severity	Event Count
ACME	8	1,496
ACME	7	3,812
acme-44.com	6	11
doe.john	3	3

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.**

TLP:AMBER

MSS-EDR 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