сомодо

SOC as a platform (SOCaaP), a next-gen SOC-as-a-Platform offering, which includes people, process and technology. SOCaaP offers full white-label capability that makes it easy to add managed security services to a portfolio.

White Label our SOC Platform with Your Brand

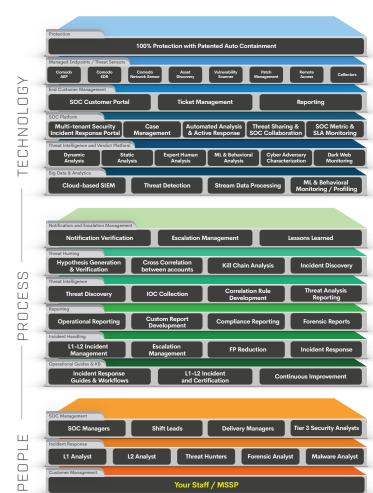
Comodo's complete SOC platform offers full white label capability for any MSP, MSSP or enterprise. SOCaaP is ready-made to provide access to your own SOC in under 24 hours, with zero capital outlay. It provides full-stack autonomous security that eliminates false positives and reduces attacker dwell time to seconds. It also includes the following:

Protection with Auto Containment

The patent-pending auto containment technology is the world's only active breach protection that stops ransomware, malware, or cyber-attacks from causing damage. This allows protection of the systems without having to rely on detection of any sort.

SOC Management Platform

A cloud native platform covering SIEM, analytics, case management and threat sharing, with artificial intelligence capabilities and a semi-supervised artificial intelligence engine that learns from the activities, events and operations.



Cloud-Native Network Detection and Response

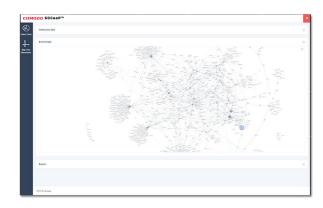
Enterprise-class network traffic analysis that detects suspicious behaviors, prioritizes investigations for the highest risk threats, and automates responses. It captures network traffic, generates extensive metadata for important network protocols, and sends this data to the cloud to correlate with endpoint sensor data.

SOC-as-a-Service

Full blown SOC services with threat hunting teams combined with system-generated alerts to detect malicious activity and provide incident response. It incorporates artificial intelligence capabilities with a semi-supervised artificial intelligence engine that learns from activities and operations of Comodo's cybersecurity experts, accelerating the detection and response to new threats.

Visual Analytics

Co-managed SIEM and visual analytics platform accessible by you and customers. It enables highlighting hidden threats and helps with understanding the main causes of any incidents so it can be described to customers.



DMODO SOCaaP™	as room						Baker Engliss	· : •
ferrore Summery	AD Business Solutions		Ap Denetics		AIC Insurance		AJ Pallets	
Incidents Overview V Log Collection Summary	Unveid Reports :	•	Crewed Reports :	۰	Chread Reports :	0	Chread Reports :	
Threat Communication Graph	Escalated Tickets :		Escalated Tockets :	٥	Exceleted Totets :	0	Escalated Tokets :	
Toluts	🛕 Open Tickets :	۰	🛕 Open Tickets :	۰	🛕 Open Tickets :	۰	🛕 Open Tickets :	0
	🕥 incidents :	۰	🕐 Incidenta :	۰	🚫 incidents :	۰	🕜 incidenta :	0
	Tickets Notified :	•	Tickets Notified :	٥	Tickets Notified :	0	Tickets Notified :	
	Baker Eng Inc.		Box Dairy		Bridgewater Dairy DH		Bridgewater Farming	
	Unved Reports :	224	Unwad Reports :	٠	Unwed Reports :		Ctread Reports :	
	Escalated Tickets :		Escalated Tokuts :	۰	Escelated Totats :	0	Escalated Tickets :	
	🛕 Open Tickets :		🛕 Open Tickets :	۰	🛕 Open Tickets :	0	A Open Tickets :	
	🕜 incidents :		📀 Incidents :	۰	🚫 incidents :	0	🕜 incidents :	0
	A Tickets Notified :		Tickets Notified :	٥	A Tickets Notified :	0	Tickets Notified :	
	Buffalo Christian		Call Land		CatchMark Technologies		Central Bands Dairy	
	Unved Reports :		Unwad Reports :	٠	Unwad Reports :	4	Utreed Reports :	
	Escelated Tickets :		Exceluted Talants :	0	Exceleted Tickets :	0	Escalated Tickets :	0

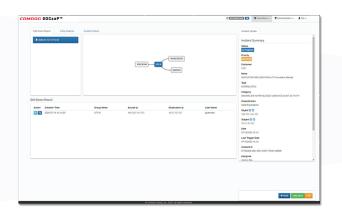
Multi-Tenant Security Incident Response Portal

Gives a snapshot of customer's security statuses, incident escalations and reporting needs. It is also a central portal where all customer interactions can be managed.

SOC Customer Portal

Co-managed SIEM and visual analytics platform accessible by you and customers. It enables highlighting hidden threats, helps you understand the main causes of any incidents and describe it to your customers.





Snapshot Reporting

Gives a snapshot of your customer's security statuses, incident escalations, reporting needs. It is also a central portal where all customer interactions can be managed.

сомојо

Solution Brief | SOC-as-a-Platform (SOCaaP™)

Analyzes and Automates

Automates all necessary early analysis, the system will analyze all observables that's been collected and prepares a consolidated result that can be used in the investigation and incident reporting. It combines various analysis tools into one unique service.

Diff Down Report Early Analysis Incident Hallony	magent Details
Carolan abor Carl Males accession	
	8 See Ad O Developed Al Incident Summary
 Apps and Services 	Status
	in Program
Network services seen on the foot Lat of user agents seen within HTTP for current host within test day	Priority
Apps detucted on host	
O Alla Meridiana	Customer
	Kana
Certificate Details	INDICATOR ODFUSICATION UTF-8 evasion attempt
SSL certificate domain	7/2+
SSL certificate bouwr	CONNELATED
SSL certificate class status In ok + reason	Category
	ANOMALIES IN PRIVLEGED USER ACCOUNT ACTIVITY
O DNS Activities	Classification
C UNS ALLWIDES	COLUMN (2) (2)
Child turnels seen within observable period	143.000 100
O Which IP's has been resolved	Systemet C C
 Comains has been resolved 	50.211 III 110
	Cote
C Endpoint Security Details	071520201212
	Last Trigger Date of 15 2020 12 12
 Were the indicators detected by endpoint solution (the Nash) 	Incident id
	87785426-85c-4021-8087-755411#96/b
O File Details	Assgree
	_ Attach Ba
Recert fie hashes	
C Data anount received per files Recent files downloaded	
Number of times same file, name seen within customer network.	
C outs anount sent per ties	
Non Oury	
	+ Tax Technol

1037			60		52 13		15			897	
	A2	Ope	Assigned	Covel		Re-Operad		is Progress		Exceleted	
essp	Customer	Security	Tubel D	Incident ID	Subject	Ward Date		End Date			
м	¥ A	- N	Town	Income la	B future					Sector Meansh	
Sec.	anigned to the										
	_										
· Center										Perhapit 10 v	
Total M	W55P Name	Current Name	Severity 17			Assgree	Reported By 27	Reported at 17	Lest Update 17	Status II	
1048	Catching provides	Rame Drig Inc.	Webut	(Fate Postve) Backboy Win32 PoChert Cric Out	BOUND	Ununiqued	Customer	13/07/2124-00 55	134572429 34 96	Capen L	
1047	Catching Technologies	Barar Digits	High	Monord and turner exploit	Anders, Bigs	900	05/07/21/20 17:25	104701093926	Cunnel		
1045	sedanedena	SelfCultoner1	- High	Endport compliance	Unaccigned	Cuclianer	23/06/21/20 07:40	224942929 87.40	Cyan I		
1045	1921	19215	19ph	Polantially Crivarian Application has been detached	Hautura Trivala	900	23/06/21/20 00 34	23/06/2120 13:34	Excellent		
1044	sedanedeno	SetOutprier1	- High	Englistimations	the lines	Cuthener	23/06/28/29 40:10	2349625293831	in Program 1		
1040	sedanedeno	SelfCutterier1	ings.	Photog Detector - Downland EVE or Scripts	the lines	500	2106202610647	210625293847	Excellent 1		
1042	sedanedena	TestCurterher1	High	Para Ada - Generic HTTP Grass Site Scratting Adven	010-010ar	900	21052120-00-44	210925293844	Excelored		
1041	sedanedeno	fectCurtaner1	The P	Enguet - Malvare Detected	Dis Diske	500	21092520-0938	234962529 13 22	Current		
1040	anotorias	500UA	Lew	Los level Break	Unasigned	Curitorian	190921210511	100621293501	Caper 1		
1009	and the first of the second	and all second and all second	Weben	AD User Enumeration		Red Torns	500	160621261717	100621291717	Excellent 1	
					Table 1007 dwine						
				-		9 10 - 1 1					

Collaborative SOC Platform

Provides central management of all incidents and responses. With our shared responsibility model, Comodo SOC will also collaborate with you to give the best security service for your customers. We can analyze, escalate, hunt and report together.

Ticket and Case Management

Provides security related ticket and case management. All security incidents can be escalated and reporting to your customers is in one place; all relevant evidences are automatically attached and sent to the customer.

Ticket Management 0	Detail			+ 0+A	Totel Halory Atachinetta		
MSSP Name:	Catchingto Technologies	Customer Name:	Rater Dig Inc.		Totel status changed to Closed by byperkmang		
Subject	Microsoft and barrier exploit	Reported at	07/05/2020 17/25				
Assignee:	Antony Tipe	Cast Update:	07/13/2020 09/26	Total has been moted with it \$19 by			
Severity:	rage	Toket Status:	Citraed	Bygramang:			
Ticket Id:	1047	Incident id:	70521011-0360-828-9580-896/57c	3675 😋			
Reported By:	500			Ticket has been repled with it \$18 by preyergy 09.55			
Description:	Nescripton:						
Monosoft and exe banker visity. Symptoms do not g Resolution:	activity detected from internal asset 112, 168 20 28 to e ularantee an infection.	demai 19 50 201 250 182 via port 8201. Th	e symptoms could be a wide range of behaviors	. Yon a surpcious file name to an unusual use of a	Ticket has been repled with id. \$17 by murail knohaginunt com at 2000-01-06 08:27		
Reset the password for the keep up to date with land p Kindly check the assets fo Block unwarted traffic in t	Toket has been repled with id, 814 by antonybou jesuantony grund core at 2020-07-05 17:32						
byorkman@calling	Trout status changed to Escalated by antonybigu assumptory grund core at 2000-0145 17 25						
Communication between	a local and offsite NAS device. Not a threat. Thanks				Ticket has been created by		
meyer@calchearthing	Reals to the Logic Christophie St						
	In computation is expected to the external publicities						
mural krahna@nurd.co							
Reset the password for the affic in the free allweb-fit	e host. Kindy let us to know that this activity is legisman or if possible	tor you, keep up to date with last patches	your internal asset. Kindly check the assets for a	my maturate activity and temove it. Block unwanted tr			
antonybęu jesuantonyd	Reply MI: 016 Date: 07/05/2020 17:32						
Raviog has been attache							
Attachments: Rawlog co	e (45.15 KB)						
1 1 1 1 1							



SOC METRIC & SLA MONITORING

Extract all SOC related operational metrics and monitor SLAs to your customers. Improving the efficiency is always highest priority where it starts with visibility over all SOC operations and metrics.