Cyber Command Datasheet

Intelligent Threat Detection and Response Platform

Cyber Command_DS_P_Cyber-Command-Datasheet_20240422

Stay Ahead Of Emerging Threats With Sangfor Cyber Command

Sangfor Cyber Command is a best-in-class Network Detection and Response (NDR) solution that is designed to help organizations detect and respond to advanced and unknown security threats residing in their network.

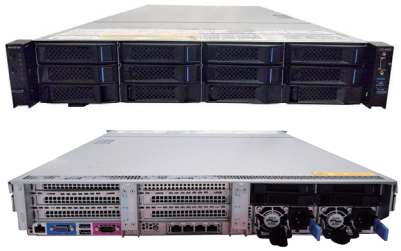
Cyber Command harnesses the power of advanced artificial intelligence (AI) and machine learning (ML) technologies to monitor and analyze network-wide traffic in real-time, identifying and alerting security teams to any anomalies in network activity. These anomalies can otherwise appear as benign network traffic that has been manipulated or disguised by intelligent malware or sophisticated adversary techniques.

By providing unprecedented visibility of their network environment, Cyber Command empowers security teams to take rapid action to remediate hidden threats, attacks in progress, as well as risks and vulnerabilities. Cyber Command's built-in SOAR module further enables security teams to automate response actions to detected threats, significantly minimizing the impact caused by security incidents.

With Sangfor Cyber Command, organizations can transform from passive bystanders to active participants in the battle against cyber threats. Equipped with this advanced security solution, they can effectively stay ahead of increasingly sophisticated cyber threats of both today and tomorrow.

Sangfor Stealth Threat Analysis (STA) is the sensor used in the Cyber Command solution. It is a hardware device that collects raw network traffic mirrored from switches and extracts traffic metadata, such as the source and destination IP addresses, protocol, port, packet size, timestamp, and other network-level data. It correlates the data into contextualized event logs and then forwards them to Cyber Command for more in-depth analysis.

Stealth Threat Analysis (STA) Front & Rear view



Cyber Command Front & Rear view

Cyber Command collects data from the STA sensor and applies AI and machine learning techniques to correlate and analyze the data. It then compares the real-time analysis results with established baselines of normal network behaviors to detect anomalies concealing malicious activities, such as stealthy command and control (C2) communication, lateral movement disguised as business traffic and irregular user behavior indicating insider threats.

Sangfor Cyber Command – Physical Appliance

Model		CC-1000	CC-2000	CC-3000
Performance				
Based on STA	STA	5STA-100	8STA-100	12STA-100
	Throughput (Gbps)	5	8	12
Based on Logs	Daily access log number (Million/Day)	200	250	350
	Average EPS (Per log/Sec)	3,130	4,380	6,255
	Peak EPS (Per log/Sec)	12,000	15,000	18,000
	Disk consumption (GB/Day)	112	140	196
	Estimated storage days/1Gbps (Assumed throughput)	1,200	1,500	1,800
Technical Specifications				
Memory (GB)		128	128	256
CPU (Cores)		12	16	48
System Disk		240GB SSD	240GB SSD	240GB SSD
Data Hard Drive Capacity		SATA 4TB*8 (Total: SATA 32TB)	SATA 4TB*10 (Total: SATA 40TB)	SATA 4TB*12 (Total: SATA 48TB)
LSI Raid		9460-8i	9460-8i	9361-8i or 9460-8i
Hardware Specifications				
Dimension (L x W X H) (mm)		790*447*86.1	790*447*86.1	790*447*86.1
Rack Height		2U	2U	2U
Gross Weight (kg)		28	28	37.5
Power Supply		Redundant	Redundant	Redundant
Rated Power (W)		345	380	900/948 [200-240VAC]
Maximum Power (W)		900	900	1300/900 [200-240VAC]
Bypass		N/A	N/A	N/A
Copper Ports		10/100 /1000BASE-T*4	10/100 /1000BASE-T*4	10/100 /1000BASE-T*4
SFP/SFP + Ports		N/A	10GbE SFP+*2	10GbE SFP+*2
USB		4**USB2.0 or above	4**USB2.0 or above	4**USB2.0 or above
Conversion Relation For STA		STA-300 = STA-100*3 , STA-500 = STA-100*10		

Stealth Threat Analysis (STA) – Physical Appliance

Model	STA-50	STA-100	STA-300	STA-500
Performance				
Peak Sustained Throughput	Up to 500Mb	Up to 1Gb	Up to 3Gb	Up to 10Gb
Maximum Unique Internal Devices Analyzed	1,000	3,000	10,000	35,000
Technical Specifications				
Memory (GB)	4	8	8	48
Hard Drive	128GB SSD	128GB SSD	480GB SSD (2TB SATA HDD - Optional)	960GB SSD
Hardware Specifications				
Dimension (L x W X H) (mm)	175 x 275 x45	400 x 430 x 44.5	600 x 440 x 89	600 x 440 x 89
Rack Height	1U	1U	2U	2U
Gross Weight (kg)	2.3	7.5	18.65	21
Power Supply	Single	Single	Dual	Dual
Rated Power (W)	22	30	55	250
Maximum Power (W)	24	60	150	300
Bypass	N/A	N/A	N/A	N/A
Copper Ports	10/100/1000 Base-T*4	10/100/1000BASE-T*6	10/100/1000BASE-T*6	10/100/1000BASE-T*4
SFP/SFP + Ports	N/A	1GbE SFP*2	10GbE SFP+*2	1GbE SFP*4 10GbE SFP+*8
Serial Ports	RJ45*1	RJ45*1	RJ45*1	RJ45*1
USB	USB2.0*2	USB2.0*2	USB2.0*2	USB2.0*2

Sangfor Cyber Command - Virtual

Model	vCC-10	vCC-50	vCC-100	vCC-500	vCC-1000	vCC-2000	vCC-3000
Performance							
Traffic Handling Capacity (Gbps)	0.5	1	2	3	5	8	12
Blog Handing Capacity (EPS/s, Peak)	5,000	5,000	5,000	5,000	10,000	12,000	15,000
Technical Specifications							
CPU (Main Frequency, Number of Cores)	2.10Hz*8	2.10Hz*8	3.60GHz*8	3.60GHz*8	2.10GHz*16	2.10GHz*32	2.60GHz*40
Memory (GB)	32	32	64	64	128	128	256
System Disk	128GB SSD	128GB SSD	128GB SSD	128GB SSD	128GB SSD	128GB SSD	128GB SSD
Minimum Hard Disk Requirement	1TB	1TB	2TB	2TB	4TB	8TB	8TB
Recommended Hard Disk Requirement	6TB	6TB	12TB	12TB	24TB	48TB	48TB

Notes: With larger hard disk capacities, the duration for retaining data is extended, enabling more prolonged storage

Stealth Threat Analysis (STA) Sensor - Virtual

Model	vSTA-10	vSTA-30	vSTA-50	vSTA-100	vSTA-200	vSTA-500	vSTA-1000
Performance							
Traffic Handling Capacity	100Mb	300Mb	500Mb	1Gb	2Gb	5Gb	10Gb
Technical Specifications							
CPU (Main Frequency, Number of Cores)	2.4GHz*4	2.4GHz*4	2.4GHz*4	2.4GHz*4	2.4GHz*8	2.4GHz*16	2.4GHz*28
Memory (GB)	4	4	4	8	16	32	48
System Disk	> 64GB	> 64GB	> 64GB	> 64GB	> 64GB	> 64GB	> 64GB
Recommended Minimum Data Disk	> 128GB	> 128GB	> 128GB	> 128GB	> 480GB	> 480GB	> 480GB