SANGFOR TIARA & MDR

Threat Identification, Analysis and Risk Assessment & Managed Detection and Response Services

SANGFOR

What are TIARA & MDR?

Cyber Command

Security Consultants

- CREST Registered Tester (CRT)
- Offensive Security Certified Professional (OSCP)
- CompTIA Pentest+ (Pentest+)
- Certified Ethical Hacker (CEH)
- Certified Information System Security Professional (CISSP)
- ISO27001 Auditors

TIARA

Threat Identification,
Analysis and Risk Assessment

MDR

Managed Detection and Response

1 SANGFOR TIARA

TIARA is a turnkey service, including Sangfor HW, SW and Services, that helps customers quickly understand it current threat posture in just four weeks.

- **Assessment:** TIARA is a preliminary lightweight security posture assessment service which helps customers to determine the current threat posture of their complete network in a short period of time.
- **Recommendation:** TIARA also provides recommendations, improvement plans and remediation assistance to take overall security posture to the next level.

2 SANGFOR MDR

MDR is an ongoing service to help customers conduct comprehensive threat analysis, asset identification, effectiveness and efficiency as well as improving daily security operations and security controls. These functions combined improve the overall security posture and increase the maturity level of organization security operations.

- **Root-cause analysis:** Sangfor security experts conduct root cause analysis and provide long-term improvement, while most of other security operations simply focus on event-by-event remediation methods.
- **Recommendation:** Sangfor security experts have years of experience in different industries or scenarios, handling similar issues within other similar organizations.

What's Keeping CISO's Up?

Unnoticed Attack Surfaces & Hidden Threats

- Difficulty in uncovering internal insecure practices and abnormal traffic that could expose or create unnoticed attack surfaces.
- Hidden threats in the system that are not visible to the IT administrators.

Overall Security Maturity Level & Threat Posture

- Lack of visibility into overall security posture, making it difficult for management to provide the right investments in the right countermeasures.

Return on Investment

- Some customers have invested a lot of money and human resources budget on SIEM or SOC, but the progress is slow and leads to ineffective and inefficient daily operation.
- Unnecessary extra work means resources are wasted.

Out of Control Breaches

- Multiple systems down due to hidden malware & ransomware spread.
- External threats change too quickly, not allowing organizations to effectively respond with their existing security capabilities.

Lack of Comprehensive Security Protection Means Breaches Occur

- Insufficient and iless than comprehensive security protection leasd to bypassed attack traffic.
- Despite investment in existing security control measures, breaches still occur.
- Overly dependent on products' capability and overlook the importance of operation.

Legal and Compliance Risks

- Involved in legal issues due to regulatory compliance violations, data breaches or sensitive data leakage.
- External regulatory requirements are becoming stricter and organizations cannot comply with the requirements.

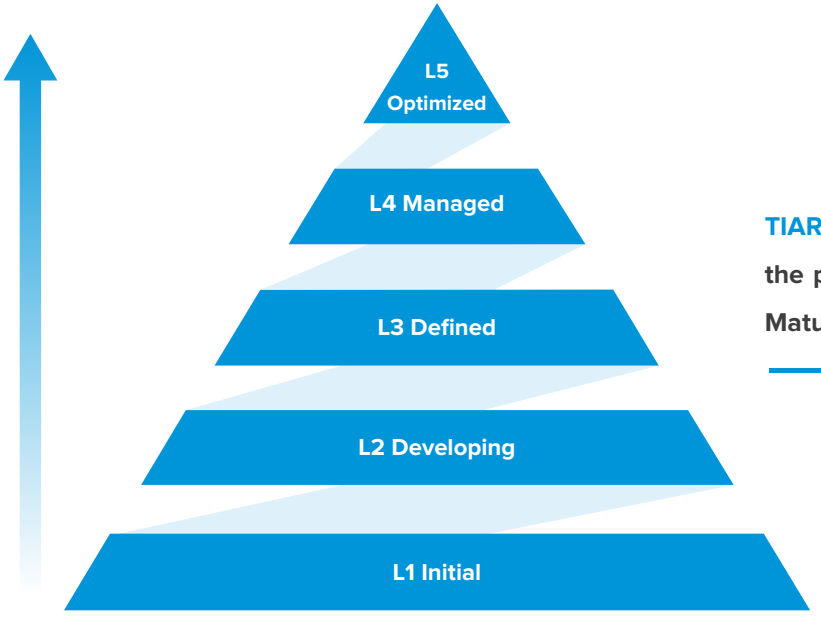
TIARA and MDR Help CISO's...

- Help customers who lack on-site security experts to identify root causes of attacks and provide a long-term improvement plan, instead of focusing on individual remediation methods.
- Provide Business Impact Analysis (BIA) to help management understand the importance of asset prioritization and the business impacts, should assets be compromised.
- Provide lightweight network risk assessment and a suggested course of action to achieve risk acceptance, avoidance, mitigation and transference.
- Correlate security events and identify potential threats before they morph into security incidents.
- Deliver a rich security protection experience for any industry or enterprise dealing with the potential of devastating security breaches.
- Evaluate the efficiency and effectiveness of existing security practices and provide suggestions on how to improve them.

Value to CISOs

1. Credible assessment of your current security posture delivered by independent and certified consultants with unbiased opinion
2. Significantly improve your current security posture by addressing misconfiguration and or by deploying additional security controls
3. Improve business continuity and achieve compliance while minimizing legal issues
4. Improve security benchmark among peers
5. Significantly improve the productivity of security operations with minimum investment

Going Above and Beyond



TIARA & MDR help organizations accelerate the process of advancing into next Capability Maturity Model level.

TIARA Works Quickly

Unlike cumbersome and complicated consultation services, TIARA provides organizations a method of identifying hidden threats and determining their overall security posture in just a few weeks, helping to identify any insufficient security controls within the environment.

Week	Activity	Content	Resources	
As Arranged	Kick Off Meeting	• Define service scope, service content and delivery plan • Gather user requirements • Gather user information	Field Engineer, Security Consultant	IT Manager, IT Team
1	Service Components Mounting	• Mount service components • Configure the settings of components ensure connectivity in order • Verify licenses, serial number, policies and rule base are in order • Fine tuning service to ensure no false positives	Field Engineer	IT Team
2	Threat Monitoring and Analysis Service	• Network threat monitoring and analysis • Onsite deep threat analysis • Onsite security event diagnosis • Technical discussion	Security Consultant	IT Team
3	Executives Presentation	• Report preparation • Business Impact Analysis (BIA) • Gap analysis • Long term improvement plan recommendation • Executives presentation slides preparation	Sales, Field Engineer, Security Consultant	Executives, IT Manager, IT Team
4	Project Closure	• Service components unmounting • Project Closure	Sales, Field Engineer	IT Manager, IT Team

How Do TIARA & MDR Differ from Traditional

✗ Extra ordinary Vulnerability Assessment and Penetration Testing (VAPT)	✓ Focus on overall security posture assessment of organization's environment
✗ Not limited to System Vulnerabilities	✓ Focus on asset management + system vulnerabilities + network threats + insecure practices + abnormal behaviors
✗ Expensive third party & time-consuming consultation	✓ Inexpensive & less time required
✗ Event-based remediation methods	✓ Focus on Root Cause Analysis and provide long term improvement plan

TIARA Case Study

Customer Background

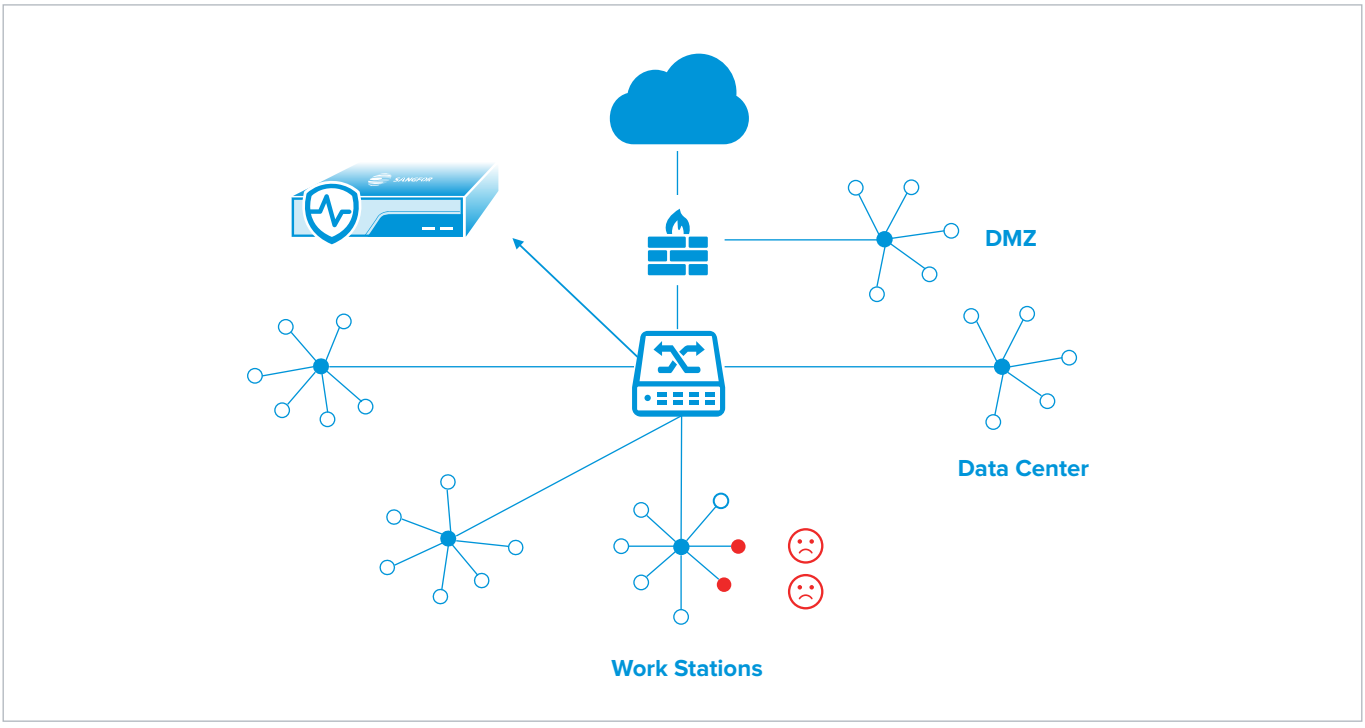
In 2018 a mid-sized financial services company, serving the investment needs of large enterprises, SOEs, banks and insurance companies, discovered that two of its virtual servers were infected with 2 different types of ransomware. Sangfor deployed their Endpoint Secure and Cyber Command solutions.

Existing Security Protection

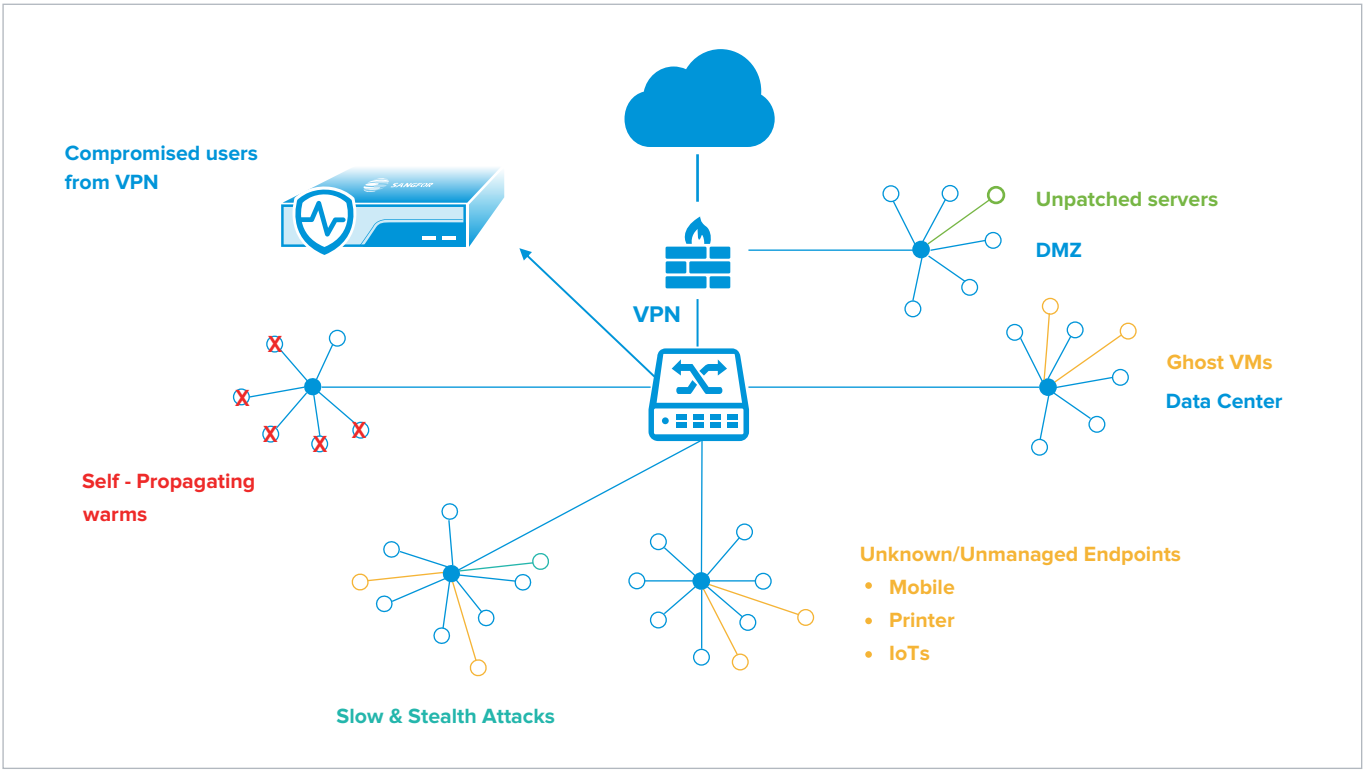
- Perimeter gateways
- Endpoint protection

Pitfalls of the Traditional Approach

- **Limited Detection:** Traditional FW and AV are limited to known attacks
- **Narrow Scope:** FW blind to internal activities & AV limited to managed endpoints
- **Lack of Security Operations:** Protection available without response capabilities
- **Wide Open:** FW is designed to open doors to apps & partners



Customer IT was reported two incidents of ransomware, unsure if they had more, IT called in TIARA.



A week after Cyber Command was deployed, TIARA uncovered hundreds of servers infiltrated with mining malware, among several other security issues.

Sangfor Helps Customers Improve Security Control

Instead of providing event-based remediation methods, **Sangfor's security consultants** perform analysis on all security events discovered. After event correlation and diagnosis, the root causes are identified. Threat Analysis Report (TAR) details the business impact, performs security gap analysis, a detailed description of issues and potential impacts and professional long-term remediation recommendations.

The customer gladly implemented Sangfor's recommendations and remediated the threats and risks identified, hence **improving the overall security posture**, enabling the customer to **meet regulatory compliance standards** and **raising the overall security capability maturity ranking.**

SANGFOR TIARA & MDR

SANGFOR INTERNATIONAL OFFICES

SANGFOR SINGAPORE
8 Burn Road # 04-09, Trivex,
Singapore (369977)
Tel: (+65) 6276 9133

SANGFOR HONG KONG (CHINA)
Unit 04, 6/F, Greenfield Tower, Concordia Plaza, No.1 Science Museum Road, Tsim Sha Tsui East, Kowloon, Hong Kong
Tel: (+852) 3427 9160

SANGFOR INDONESIA
MD Place 3rd Floor, Jl Setiabudi No.7, Jakarta Selatan 12910, Indonesia
Tel: (+62) 21 2966 9283

SANGFOR MALAYSIA
No. 47-10 The Boulevard Offices, Mid Valley City, Lingkaran Syed Putra, 59200 Kuala Lumpur, Malaysia
Tel: (+60) 3 2201 0192

SANGFOR THAILAND
6th Floor, 518/5 Maneeya Center Building, Ploenchit Road, Lumpini, Patumwan, Bangkok, 10330 Thailand
Tel: (+66) 22517700

SANGFOR PHILIPPINES
7A, OPL Building, 100 Don Carlos Palanca, Legazpi, Makati, 122 Metro, Manila, Philippines.
Tel: +63(0) 9175081244 / +63(0) 9171179346

SANGFOR VIETNAM
OTX2-0327 Sunrise City, 27 Nguyen Huu Tho, Tan Hung Ward, Dist. 7, HCMC, Vietnam.
Tel: (+84) 28 62700133

SANGFOR SOUTH KOREA
Floor 17, Room 1703, Yuwon bldg. 116, Seosomun-ro, Jung-gu, Seoul, Republic of Korea
Tel: (+82) 2 6261 0999

SANGFOR EMEA
C-80 (C-Wing), Dubai Silicon Oasis HQ Building, Dubai, UAE
Tel: +971-52-9606471

SANGFOR PAKISTAN
D203, Navy Housing Scheme, ZamZamma, Karachi, Pakistan
Tel: +92 3142288929

SANGFOR ITALY
Sede Legale ed Operativa via E. Berlinguer, 9 20834 Nova Milanese MB Italia
Tel: +393400616767

SANGFOR USA
46721 Fremont Blvd, Fremont, CA 94538, USA
Tel: +1 (510) 573-0715

AVAILABLE SOLUTIONS

IAM	Simplify User & Network Management
NGAF	Smarter Security Powered By AI
Endpoint Secure	The Future of Endpoint Security
Cyber Command	Intelligent Threat and Detection Platform
SD-WAN	Boost Your Branch Business With Sangfor
WANO	Enjoy a LAN Speed on your WAN
HCI	Driving Hyperconvergence to Fully Converged
aCLOUD	Enterprise Cloud Built on HCI
VDI	Ultimate User Experience that Beats PC
aBOS	The World First NFV Converged Gateway
CM	Centralized Management Platform

SANGFOR

www.sangfor.com

Sales : sales@sangfor.com
Marketing : marketing@sangfor.com
Global Service Center : +60 12711 7129 (or 7511)

Our Social Networks :

https://twitter.com/SANGFOR
https://www.linkedin.com/company/sangfor-technologies
https://www.facebook.com/Sangfor
https://plus.google.com/+SangforTechnologies
http://www.youtube.com/user/SangforTechnologies

Sangfor_BR_P_TIARA & MDR Brochure_20200327