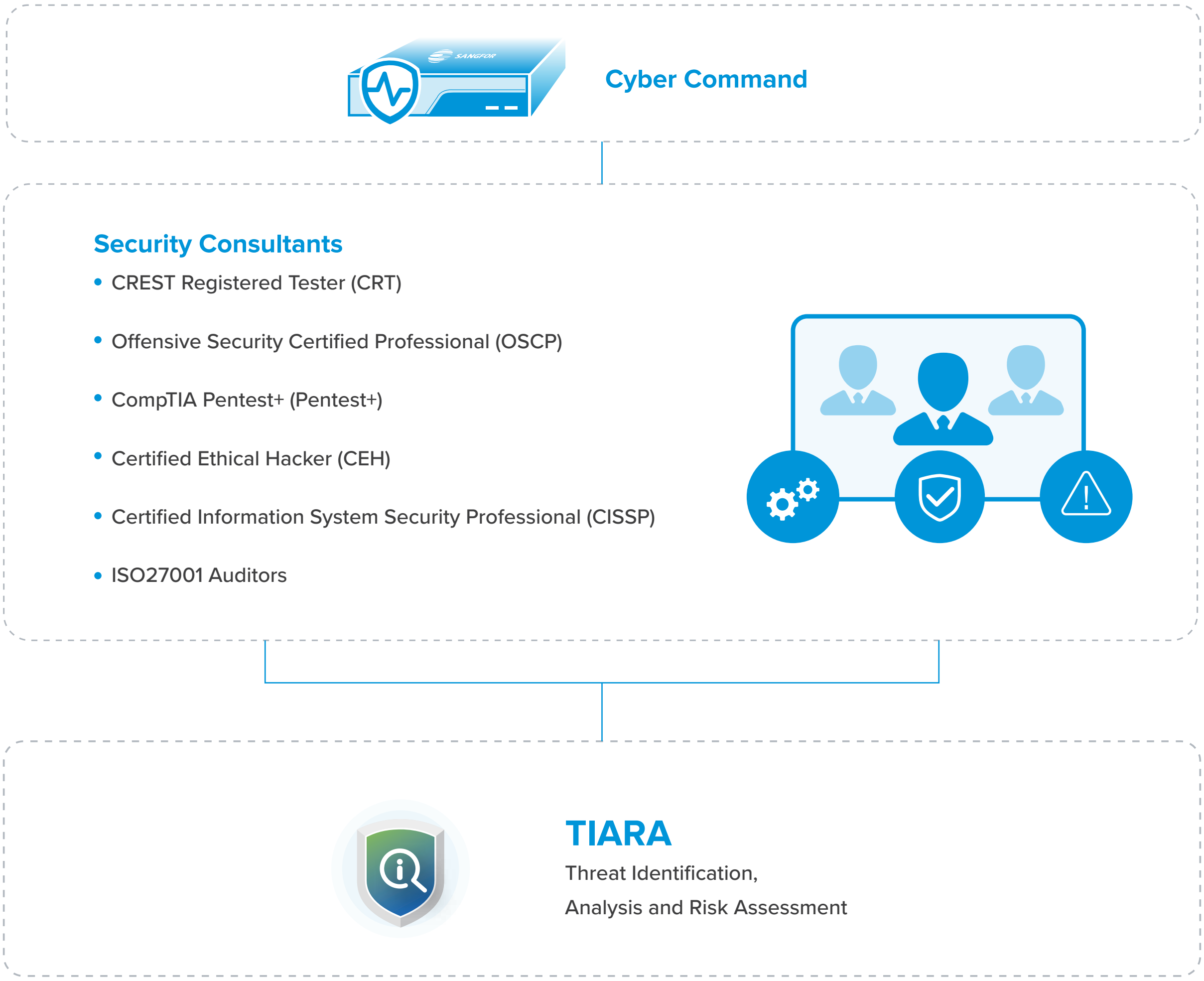
SANGFOR

SANGFOR TIARA

Threat Identification, Analysis and Risk Assessment

What is TIARA



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

1 SANGFOR TIARA

TIARA is a turnkey service that helps customers understand their current threat posture within 2-4 weeks duration, leveragin Sangfor's very own technology and hardware.

- **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.

What’s Keeping CISO’s Up?

Fear & Concerns

Out of control breaches due to hidden malware & ransomware

Lack of comprehensive security protection leads to bypassed attack traffic & breaches occuring

Legal or compliance risk issues due to regulatory compliance violation, data breaches or sensitive data leakage occur

Unnoticed attack surfaces & hidden threats due to insecure practices and abnormal traffic

Overall security maturity level & threat posture

Return on investment with products and human resources

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

- Invested technologies such as SIEM or SoC lack of more useful information on threat detection which leads to time-consuming operations through manual correlation of security events.
- Unnecessary extra work means resources are wasted.

Out-of-Control Breaches

- Unknown threats already within the network may cause more damage if not monitored and detected in a timely manner.
- External threats change too quickly, not allowing organizations to effectively respond with their existing security capabilities.

Lack of Comprehensive Security Protection Increases Risk on Cyber Breaches

- Traditional security technologies lack advanced and sophisticated detection capabilities required to detect more advanced attacks and malicious activities in the network.
- 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.

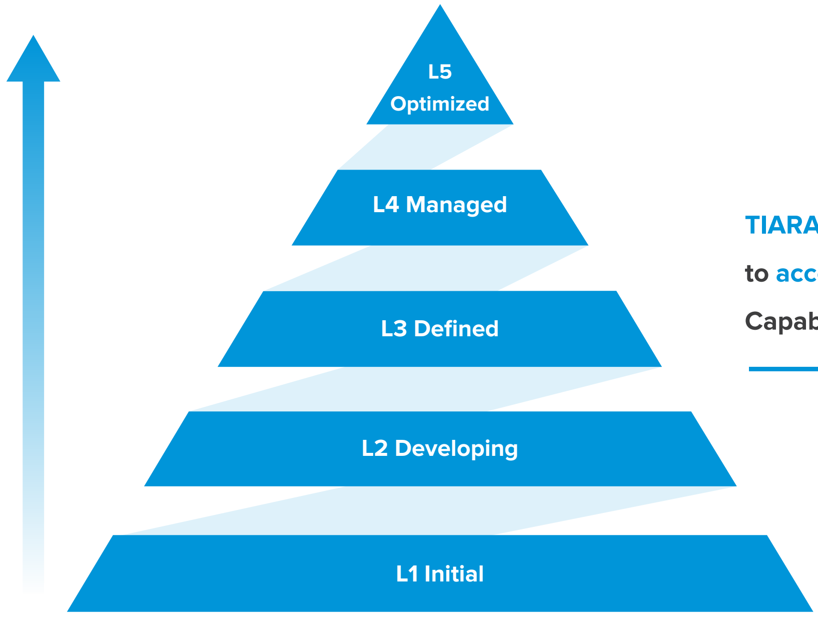
TIARA Helps CISO’s...

- 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 impact in the event of asset compromise.
- Provide lightweight network risk assessment and suggested course of action to achieve risk acceptance, avoidance, mitigation and transference.
- Correlate security events and identify potential threats before they become a security incident.
- Deliver a consistent threat identification service for all types of industries and enterprises that are prone to security breaches.
- Evaluate the efficiency and effectiveness of existing security practices and provide suggestions to enhance existing security controls and practices.

Value to CISOs

1. Credible and unbiased assessment of your current security posture delivered by certified and experienced consultants
2. Addressing misconfigurations and providing recommendations to significantly improve your current security posture
3. Improve business continuity and achieve compliance to minimize legal issues
4. Improve security benchmark among peers
5. Significantly improve the productivity of security operations with minimum investment

Going Above and Beyond



TIARA also helps organizations and enterprises to accelerate the process of advancing into next Capability Maturity Model level.

TIARA Works Quickly

Unlike cumbersome and complicated consultation services, TIARA provides organizations with a centralized platform to identify hidden threats, understand the overall network security posture, and identify other security control gaps in the environment, all delivered within 2 - 4 weeks.

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 Deployment	• 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	• Network threat monitoring and analysis • Onsite deep threat analysis • Onsite security event diagnosis • Technical discussion	Security Consultant	IT Team
3	Executives Presentation	• Business Impact Analysis (BIA) • Gap analysis • Long term improvement plan recommendation	Sales, Field Engineer, Security Consultant	Executives, IT Manager, IT Team
4	Project Closure	• Acceptance sign-off • Project Closure	Sales, Field Engineer	IT Manager, IT Team

How Do TIARA Differ from Traditional Security Services?

Conventional Security Services

- ✗ Unable to perform advance threat detection without going through a full vulnerability assessment and penetration testing (VAPT) which uncovers threats at the assessment point-of-time
- ✗ Identify security gaps through system vulnerabilities instead of proactive network threats monitoring
- ✗ Expensive third party & time-consuming consultation
- ✗ Event-based remediation methods

TIARA Services

- ✓ Focus on overall security posture assessment of organization’s environment
- ✓ Focus on asset management + system vulnerabilities + network threats + insecure practices + abnormal behaviors
- ✓ Inexpensive & less time-consuming
- ✓ Focus on Root Cause Analysis and provide long term improvement plans and recommendations
- ✓ Focus on identifying the source or root cause of the problem and provide long term improvement plans

TIARA Case Study

Customer Background

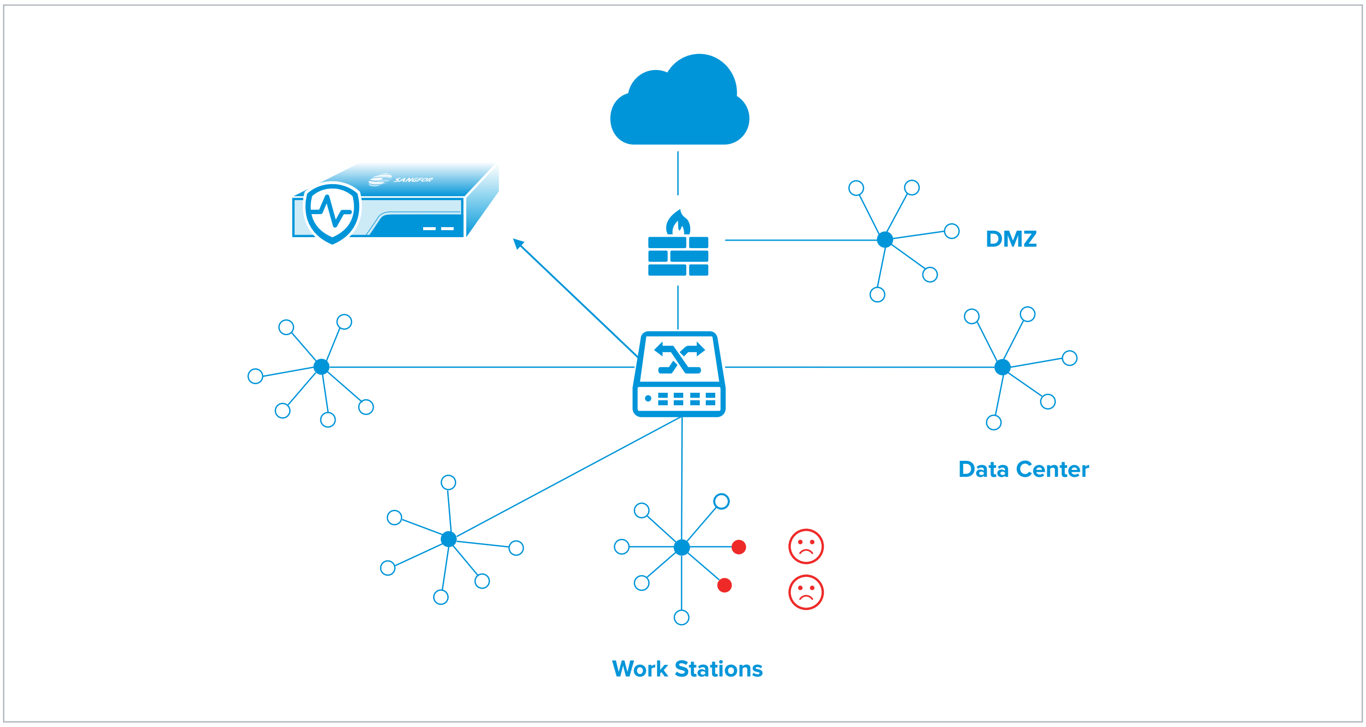
In 2018 a mid-sized financial services company, serving the investment needs of large enterprises, SOEs, banks and insurance companies, discovered that two of its virtual servers were infected with 2 different types of ransomware. Sangfor deployed their Endpoint Secure and Cyber Command solutions.

Existing Security Protection

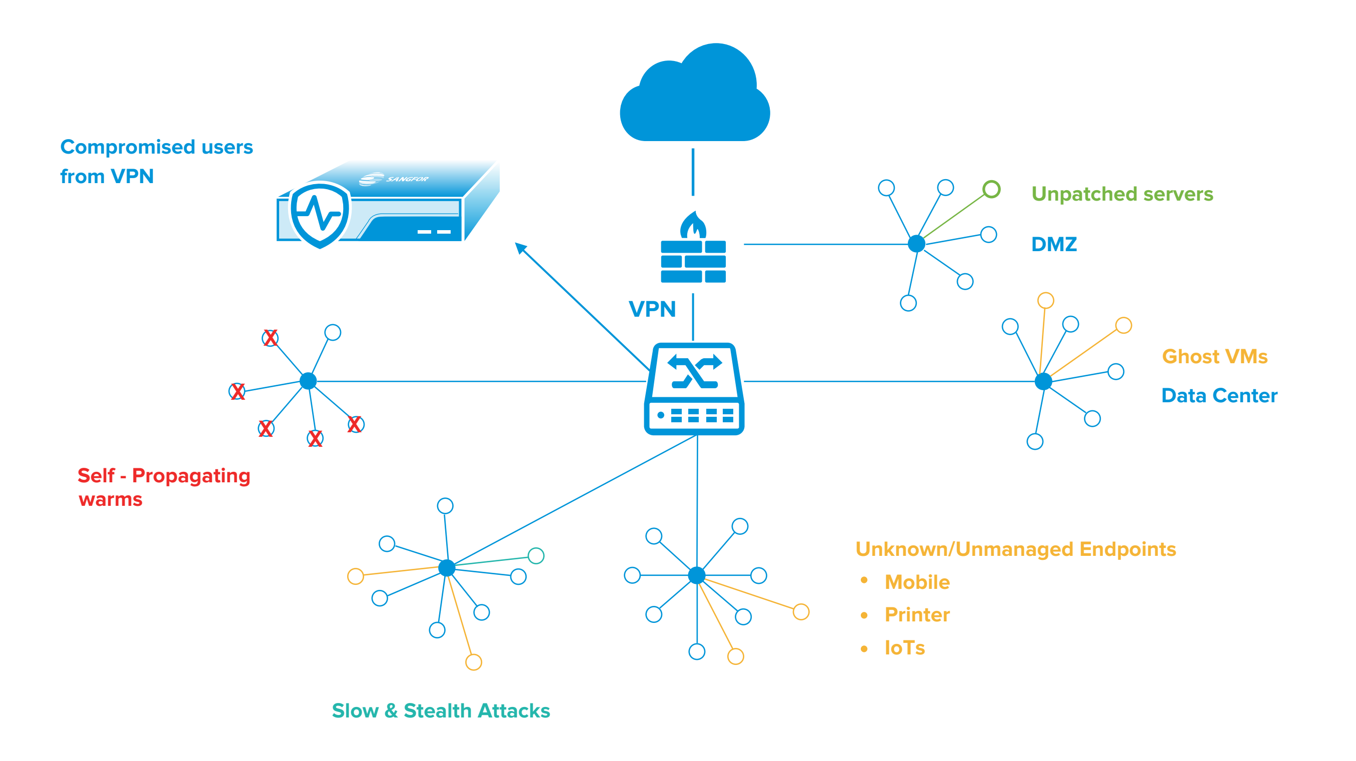
- Perimeter gateways
- Endpoint protection

Pitfalls of the Traditional Approach

- **Limited Detection:** Traditional FW and AV are limited to known attacks
- **Narrow Scope:** Lack of multiple firewall to monitor internal network or east-west traffic while AV was limited to endpoints monitoring
- **Lack of Security Operations:** Protection available without response capabilities
- **Wide Open:** FW is designed to open doors to apps & partners



The IT customer had recently faced by two (2) ransomware attack incident and was worried if there are anymore residual malwares or attacks within the network, which is where they had requested for 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** performed analysis on all security events discovered. Root cause were identified and presented after performing deep analysis through event correlation and diagnosis. Threat Analysis Report (TAR) detailed the business impact, identified security gap analysis, issues description and risk, and professional long-term remediation recommendations.

The customer express their gratitude on the values from implementing Sangfor's recommendations and remediated the threats and risks identified, hence improving overall security posture, enabling the customer to **meet regulatory compliance standards** and **raising the overall security capability maturity ranking.**

SANGFOR TIARA

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) 3-2702-3644

SANGFOR THAILAND
6th Floor, 518/5 Maneeya Center Building, Ploenchit Road,
Lumpini, Patumwan, Bangkok, 10330 Thailand
Tel: (+66) 22-517700

SANGFOR PHILIPPINES
7A, OPL Building, 100 Don Carlos Palanca, Legazpi, Makati,
122 Metro, Manila, Philippines.
Tel: (+63) 917-117-9346

SANGFOR VIETNAM
4th Floor, M Building, Street C, Phu My Hung,
Tan Phu Ward, District 7, HCMC, Vietnam
Tel: (+84) 287-1005018

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
D-81 (C-Wing), Dubai Silicon Oasis HQ Building 341041 Dubai,
United Arab Emirates
Tel: (+971) 5296-06471

SANGFOR PAKISTAN
44, Navy Housing Scheme, ZamZamma, Karachi, Pakistan
Tel: (+92) 333-3365967

SANGFOR ITALY
Sede Legale ed Operativa via E. Berlinguer, 920834 Nova
Milanese MB Italia
Tel: (+39) 340-061-6767

SANGFOR SPAIN
Calle de Ribadesella 7, 28250 Torrelodones,
Madrid (SPAIN)
Tel: (+34) 609-64-40-04

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

AVAILABLE SOLUTIONS

IAG	Simplify User & Network Management
NGAF	Smarter Security Powered By AI
Endpoint Secure	The Future of Endpoint Security
Cyber Command	Powerful Intelligent Threat and Detection Platform
HCI	Driving Hyperconvergence to Fully Converged
VDI	Ultimate User Experience that Beats PC
SD-WAN	Boost Your Branch Business With Sangfor
SIER	Simplify & Intelligence Your Branch Network
Access	Cloud-based SASE for Branch Offices & Remote Users
WANO	Enjoy a LAN Speed on your WAN

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

https://www.youtube.com/user/SangforTechnologies

Sangfor_BR_P_TIARA & Brochure_20210917