Intelligent Cyber Threat Detection and Response

Cyber Command Solution + MDR Service

Daniel See (Presales) daniel.see@sangfor.com
Agenda

PART 1
Background and Challenges

PART 2
Introduction

PART 3
Highlights & Benefits

PART 4
POC Campaign and Promotion
PART 1  Background
Unknown threats is everywhere in cyberspace

- C&C Hidden malicious traffic
- The new virus
- Struts2, webshell
- Virus variant
- Unknown malware
- Malicious link
- Variant easy
- Higher Percentage
- Destructive power

**Hacker groups**

Offense and defense are not equal. Commercialization of advanced tools of evasions.
Declaration From Anonymous Malaysia

Recently, Anonymous Malaysia has stepped out and claimed that they wanted to launched a new coordinated cyber-attack against the Malaysian Government. According to their previous footage, 91 of Malaysia Government websites have been compromised on June 15, 2011 and even more than 100 of websites in 2015.
Current Security Operation Issues - No security threat in sight

New unknown threats are hard to detect

- Zombies from internal network
- Ransomware attack
- Zero-day vulnerability attack

Root cause:

- Static signatures detection is difficult to deal with new threats and lack of continuous detection methods for Insider attacks

Insider threats are hard to detect

- A backdoor reserved by the hacker
- Disguise the illegal operation behavior of the legitimate user
- Outgoing exception data encapsulated in a normal protocol
Current Security Operation Issues - No security risk in sight

If you can't see the assets, you can't see the risk

- Lack of visibility for Botnet assets
- Weak password of Admin
- High-risk vulnerabilities in the system

Root cause:

*Lack of active assets and vulnerability identification, security equipment separation, difficult to in-depth correlation analysis, lack of global security perspective*

The perspective of security separation is difficult to operate efficiently

- Massive security logs, it is difficult to identify the effective alarm
- Professional logs, hard to understand
- Lack of correlation, hard to analyze
Can't see the status of global assets, risk assets can not be timely processing!

With so many alarms, how to find a real threat and respond quickly?

Can't analyze the logs and threats, security device is just a decoration!

Invisible proliferation of threats, not handled thoroughly!
Common Pain Points

✓ Hidden & Evolved Threats and Malware
✓ Powerless on Lateral Attacks (East-West Traffic)
✓ Afraid of second wave of infection or exploitation from cyber threats
✓ Lack of Visibility (Threats, Assets, Behaviors & Vulnerabilities)
✓ Immediate Response to on-going security incidents
✓ Lacking of professional security service and consultation
Security is upgraded from passive defense to Proactive defense

**Passive defense**
- Defensive first, passive response
  - Perimeter Protection
  - Intrusion Protection
  - Host Anti-Virus
- Reduce attack surface, increase attack cost

**Proactive defense**
- Comprehensive detection, quick response
  - Continuously monitor
  - Intelligent analysis
  - Synchronize correlation
- Shorten detection and response time

Build an active defense system integrating defense, detection and response, focusing on continuous monitoring and quick response
PART 2

Introduction of Intelligent Cyber Threat Detection & Response
Introducing Intelligent Cyber Threat Detection & Response

**Threat Detection**
- Monitors internal traffic. Correlates security events (logs)
- Artificial Intelligence. Behaviour Analysis, Neural-X (GTI) for Unknown and Never-Seen Threats
- Uncovers hidden/ghost assets
- Risks and Vulnerabilities

**Threat Hunting**
- Uncovers hacker’s point of entry & IOC
- Kill Chain Determination and Malware Behaviour Analysis
  (Prediction on Malware’s Next Action & Business Impact)
- Analyses impacts. Collects IOCs

**Threat Response**
- Remediation & Recommendation
- Correlates with network and endpoint countermeasures
Deployment

- Taps into core switches
- Compliments with your existing security controls (NGAF, Endpoint Secure, & SIEM)
- Monitors East–West & North-South traffic
- Will **not affect network architecture** and configuration, **No Downtime**, and **agentless** at the endpoint.

Components:
1. Cyber Command
2. STA (Stealth Threat Analysis)
3. SANGFOR Endpoint Secure
4. NGAF (Next-Gen Application Firewall)
### Scenarios of Cyber Command & SIEM

<table>
<thead>
<tr>
<th>Customers are advised to use the SIEM solution in the following two scenarios</th>
<th>Cyber Command is a better solution for customers needing</th>
</tr>
</thead>
<tbody>
<tr>
<td>◆ The essential needs of customers are to meet compliance, obtain and maintain ISO certificates and log management and storage. SIEM solutions meet the above customer requirements perfectly.</td>
<td>◆ Strong security monitoring functions, better threat detection and response capabilities.</td>
</tr>
<tr>
<td>◆ The customer is large with enough personnel to carry out security operation and maintenance and correlation analysis of multi-brand security products. SIEM can be used as the core management platform of SOC to meet high-standard security operation requirements.</td>
<td>◆ To streamline SOC operations and maximize use of security personnel.</td>
</tr>
<tr>
<td></td>
<td>◆ To reduce O&amp;M costs by maximizing deployment and utilization of existing security products.</td>
</tr>
</tbody>
</table>
PART 3

Highlights & Benefits of Intelligent Cyber Threat Detection & Response
Our solutions: high synergy level automation

**Before**
- EDR
- NGFW
- Threat Intelligence
  - Inquire
  - Confirm
- Data
- Action

**After**
- core switch data
- EDR data
- NGAF data
- **Correlation**
- CC
- Security Analyst
- Automatic response
- other teams

- Business team
- System team
- CISO
- Security Engineer

Sangfor Technologies
Our solutions: continuous full traffic detection with AI technology

Before:
- Internet
- Malware
- Virus variants
- Perimeter Protection
- Compromised remote worker
- Virus bypass FW
- Data exfiltration
- Malicious user

After:
- Advanced threats
- Compromised hosts
- Malicious users
- UEBA
- Engine Zero
- Neural X
- Other AI models

Remove virus
Quarantine high risk user
Block lateral attacks
Our solutions: Reduce incident risk and remove the root-cause

Before

- Product line (Industrial control devices)
- Shadow IT
- Data Center
- Office network

After

- Proactive approach as protection (disable unsafe ports, vulnerabilities etc.)
- Assets auto-discovery and management
- Built-in threat hunting help admin find out root-cause

- DMZ
- Data Center
- Office network
Accurate detection capability - Neural X continuous empower security capability

Sangfor Neural-X
- Autonomous Evolution Architecture
- Multi Engine Analysis
- Comprehensive Data Support
- Large Algorithm Resource Pool
- AI Big Data

Security Capability
- Attack Traceability
- Linkage Disposal
- File Cloud Lookup
- Hacker portrait
- Threat Analysis
- Virus Fingerprints
- Tactical Intelligence
- Traffic Signature
- Etc.

Capacity Delivery
- Security Threat Information
- Abnormal File Recognition
- Security Analysis Ability
- Unknown Threat Protection
- Alarm Information Push
- Security Equipment Linkage

Service Delivery
- Cloud Protection
- Cloud Monitor
- Cloud Shield
- Cloud Mirror

Sangfor Cyber Command
Sangfor Engine Zero

Coverage
Both known and zero-day attacks.

Efficacy
In recent tests our malware detection rate scored the highest in terms of accuracy among other vendors.

Fast
Extremely efficient, utilizing very few resources while efficiently providing malware inspection on the network gateway with very little performance impact.
Cooperation with Virustotal

VirusTotal += Sangfor Engine Zero

THURSDAY, NOVEMBER 28, 2019  BERNARDO.QUNTREO  LEAVE A COMMENT

We welcome the Sangfor Engine Zero to VirusTotal. In the words of the company:

"Sangfor Engine Zero (a.k.a SAVE engine in China) is an AI-powered malware inspection engine developed by the Sangfor Security Team and in use at some of the most influential and forward thinking enterprises globally. Engine Zero utilizes machine learning technology to analyze and synthesize input data. The combined power of Sangfor’s dedicated R&D and Security teams, comprised of data scientists, security analysts and white hat researchers, has produced Engine Zero’s unique, multi-dimensional features, able to detect and classify malicious files, sight unseen. Engine Zero surpasses traditional detection engines (feature/hash based) in its ability to: 1. Ability to identify new and unknown malware with no updates to the AI model; 2. Proven industry-leading ransomware detection capabilities (successfully detected WannaCry, Globelmposter, GandCrab, CrySiS and their families); 3. Integrate and work in conjunction with the highly-automated Neural-X. Sangfor’s AI-enabled cloud platform for threat intelligence & analytics, to self-evolve and self-teach without human intervention."

Sangfor has expressed its commitment to follow the recommendations of AMTSO and, in compliance with our policy, facilitates this review by SKD Labs, an AMTSO-member tester.

Detection - Complete Coverage

Complete Network Coverage
- North-South traffic
- East-West traffic
- Network Gateways logs
- Endpoint logs & Files
- User Authentication

Advanced Detection Coverage
- Known and Unknown Attacks & Assets
- Malware & Attack Event Analysis and Prediction
- Attacks that bypassed your existing controls
- Insider threats
- Uncover Evolved Virus or Malware
- Able to detect latest C&C Domains

Threat Intelligence
- Sangfor Neural-X

Artificial Intelligence Based Detection Engines
- Expected Behaviour
- Abnormal Behaviour (UEBA)
Track Patient Zero
Simplified Threat Hunting

Impact Analysis

Track down “Patient Zero”

Golden Eye
Behavior of compromised assets

Security Incidents by Severity
Discovery of Asset and Vulnerabilities

Compromised Asset: Botnet
Attack surface: High risk port open
Vulnerability for key assets
Weak passwords for key assets
Lack of encryption protection for key assets

Global assets visualization
Asset Vulnerability visualization

Active identification of assets

Potential risk
Response – Visualized Incident Investigation via Attack Chain

![Visualized Incident Investigation via Attack Chain](image_url)
2.12 The host suffered MS08-067 vulnerability exploit attacks from the Internet.

**Impacts:**
As long as the host is turned on, if the user does not perform any operations, the target host is still directly intruded and injected virus samples, it indicates that the host is controlled by hackers, and there may be the following risks:

1. Confidential information may be stolen, such as important files, usernames and passwords of key assets, etc.
2. The host, as a zombie, attacks other organizations on the Internet and violates the cyber security law, which may cause it to be notified and punished by regulatory authorities.

**Proof:**
Taking User Segment (10.251.188.88) as an example, this event occurred on the host during the report period. Detailed proof is as follows.

**Description:** The host suffered MS08-067 vulnerability exploit attacks from the Internet.

**Forensics:** The host suffered 4 MS08-067 vulnerability exploit attacks from 1 host. The following are top 10 attackers:
1. 2020-07-23 14:54:26-15:19:15, the host suffered 4 MS08-067 vulnerability exploit attack(s) from 10.251.3.232 (Beijing).

**Verification:** You can paste screenshots of verification material here and take screenshots as follows:
Event detailed proof > Virus removal result > System file.

**Suggestions:**
1. If the attack is successful, it indicates that the host has an MS08-067 vulnerability and can be successfully exploited by an attacker, but there is no proof that the host has been implanted with a virus by the attacker. We recommend to use Sangfor Endpoint Security Client for virus scan and removal: [https://www.sangfor.com/product/sfx-network-security-endpoint-secure.html](https://www.sangfor.com/product/sfx-network-security-endpoint-secure.html)
2. If the above tool cannot solve problems, [KidoKiller](http://edr.sangfor.com.cn/tool/Kidokiller.zip) can be used.
3. If the attack fails, it indicates that there is no MS08-067 vulnerability on the host. You can keep monitoring.

**Security Enhancement Suggestions:**
1. If there is a vulnerability, download and install the patch: [https://docs.microsoft.com/en-us/security-updates/securitybulletins/2008/ms08-067](https://docs.microsoft.com/en-us/security-updates/securitybulletins/2008/ms08-067)

**Daily maintenance:**
1. It is recommended to disable ports 139 and 445 that are used for file sharing if they are not necessary for business.
2. Update the system patch in time. You can use Windows to update automatically or Tencent PC Manager to update.
3. Back up critical data regularly to other hosts or storage devices.
Comprehensive Visibility

Overall security posture

Cyber attack posture

Asset posture

Vulnerability posture
Response

Remediation & Recommendations
- Patching, hardening
- Block a user
- Further investigation

Network Correlation
- Shut down C&C Connections
- Block open ports and IP
- Set ACL policies

Endpoint Correlation
- Scan for other malware
- Stop processes
- Quarantine
Overview of Advantages

Detect Unknown Threats & Vulnerabilities
That potential risk or vulnerable point to the organization might be the loop holes of attacks

Active Prevention
By using sophisticated and advanced detection method, user able to be notified before attack happen. Able to predict the suspicious activities

Business Impact Analysis
Helps IT to understand what is already compromised and what needs to be prioritized. Visualize all traffic flows.

Faster Response
Faster response to improve overall security control. To avoid attack when something abnormal being detected

Professional Security Consultation
Sangfor team able to provide long term remediation plan for user and respond for the security incident in time.
Expert Security Consultants

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

Cyber Command

MDR
Managed Detection and Response
Benefits of SANGFOR MDR Service

✓ Continuous 24*7 Protection and Managed Service for Customer

✓ No need to have dedicated manpower to learn CC from scratch

✓ Recurring Service (Monthly or Quarterly), will communicate with client to improve the security posture.

✓ MDR Service Report will integrate with Recommendations and Mitigations Plans for discovered threats and vulnerabilities.
Components of MDR Service

- **Vulnerability and Threat Analysis**: Quarterly Basis
- **Attack Event Analysis**: Monthly Basis
- **Long Term Remediation Suggestion**: Quarterly Basis
- **SANGFOR Care Services**: Continuously Basis
- **Incident Response**: On Demand Basis
Case Study - GLC

Customer Pain Points:
• Experienced Attacks and Hidden Threats
• To identify their asset’s vulnerabilities
• SIEM unable to integrate with their Firewalls

Solution:
-Cyber Command’s Golden Eyes help to track IOC and Patient Zero (Real Culprit behind the zombie)
-Cyber Command’s Risk and Vulnerabilities Assessment
-Cyber Command able to correlate with their NGAFs to collect logs and perform Response
Case Study - Government

Customer Pain Points:

- Crypto mining Incident Occurrence Regularly
- To ensure all assets are all secure and well-aligned with security best practice standard
- To have Continuous detection and response service

Solution:

- Cyber Command with UEBA, Threat Intelligence and A.I based Detection Engines for Unknown/ Hidden Threats
- Risk and Vulnerabilities assessment and recommendation Provided
- MDR service provided
THANK YOU

Intelligent Threat Detection and Response Platform

Daniel See (Presales Manager @Sangfor Malaysia)

www.sangfor.com

Sangfor Technologies Inc.