SANGFOR

A New Strategy to Combat Ransomware

Paul Tsang | Senior Regional Solution Architect, CISSP

paul.tsang@sangfor.com

SANGFOR Technologies Inc.

Agenda

PART 1 Threat Landscape

PART 2 The Stages of Ransomware Attack

PART 3 Tactics to Combat Ransomware

PART 4 Takeaways

SANGFOR

PART 1 Threat Landscape

Colonial Pipeline Ransomware Attack

- On 2021 May 7th , Colonial Pipeline, the largest pipeline system was hit by DarkSide Ransomware.
  - 4.4M USD had been paid to DarkSide group.
  - Fuel rose by $3 per gallon
    - Compromised VPN accounts

Ransomware Threat Map

Based on our vast experience from 24 months of Incident Response offerings in APAC, below are the key summary data we have observed.

Regional Perspective

APAC

China / Hong Kong region recorded the largest number of security incidents requesting our Incident Response investigations.

Other major countries (i.e. MY, IN, TH) had a notable increase in ransomware cases during that period.

SANGFOR

Ransomware Threat Map

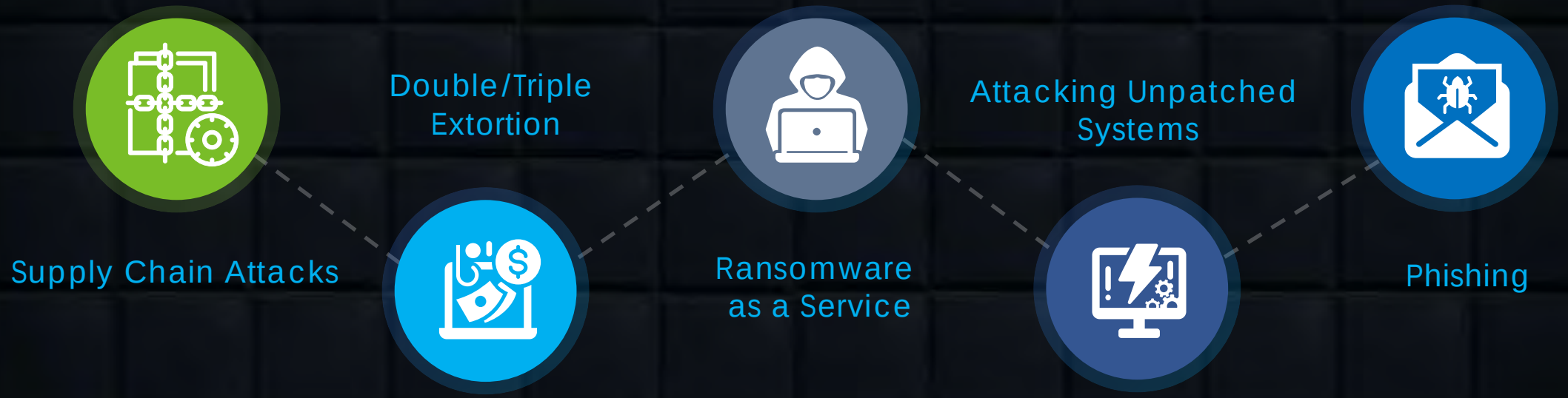
Top Industries on Ransomware Threat Landscape in APAC Region

The ransomware attack is no longer a question of "if"; but "when" !

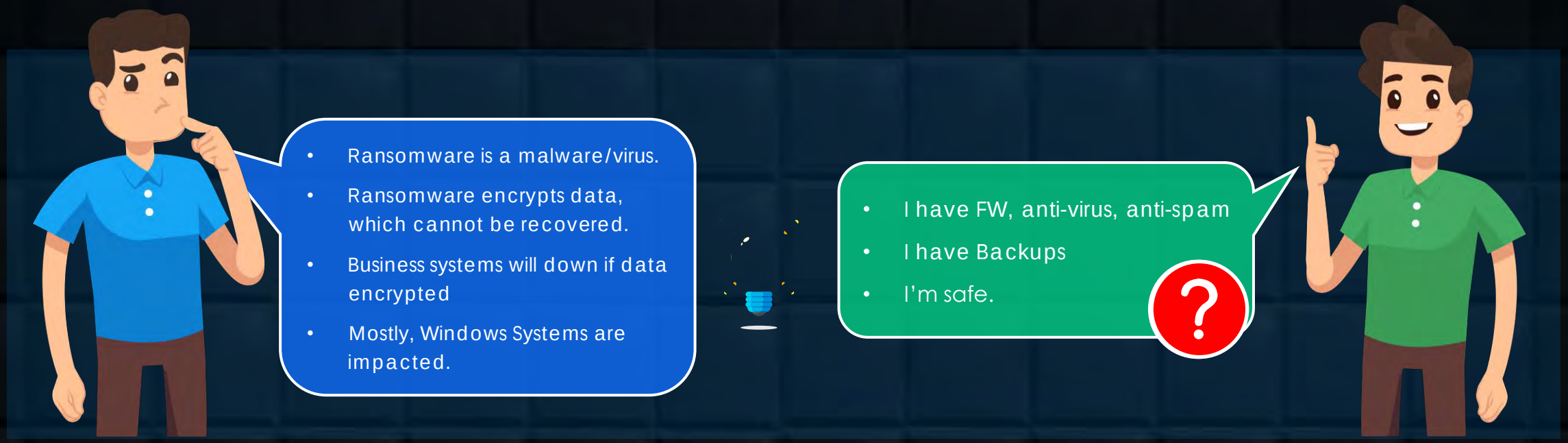
* Based on Sangfor Internal IR Statistics as of 1st May 2022

SANGFOR

Ransomware Trends of 2021



What Do You Think About Ransomware



The Fact

- No single product can provide a 100% detection rate. And even 0.1% miss may cause a lot impact.
- 75% of businesses infected with ransomware were running up-to-date endpoint protection.

SANGFOR

PART 2

The Stages of Ransomware Attack

Overview of a Ransomware Lifecycle

- The Ransomware arrives at the victim's machine

- Propagate itself through the file system
- Steal the data
- Delete the existing shadow copies
- Encrypt the specific extension file

Victim receives phishing email containing a link to infected website

- Receive decryption key if pay the ransom via TOR
- The decryption key will be destroyed if not pay the ransom during the certain period

Victim is given a ransom notice with a deadline

SANGFOR

Stages of Ransomware Attack

Lockheed Martin Cyber Kill Chain (CKC)

Intrusion | Post-Access | Exploit

MITRE ATT&CK

Reconnaissance	Execution	Lateral Movement	Exfiltration
Resource Development	Persistence	Collection	Impact
Initial Access	Privilege Escalation	Command & Control	
	Defense Evasion		
	Credential Access		
	Discovery		

SANGFOR

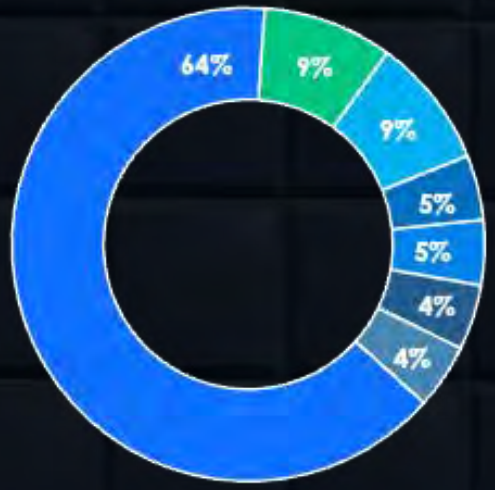
Stage 1: Intrusion

Objective: to get a foothold in the network

Stage 1: Intrusion – Brute force Attack

SSL VPN, RDP, SMB, IoT and **more...**

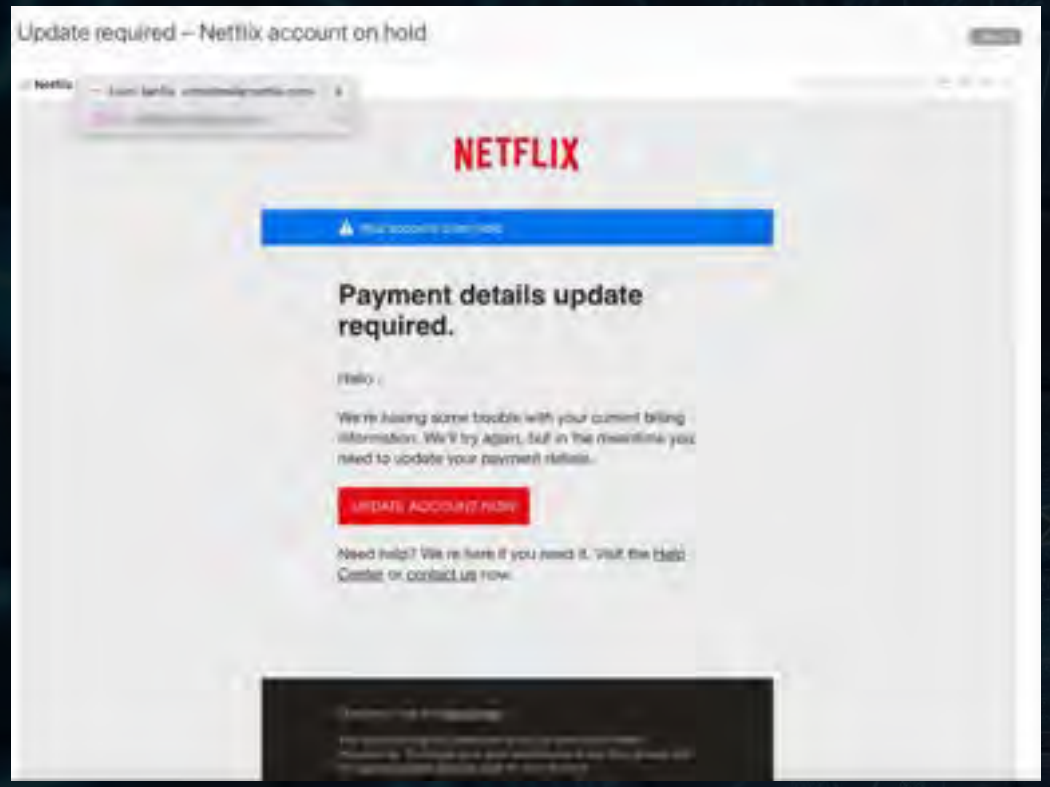
Compromise Root Causes



- 64% I Bruteforce (e.g. VPN, RDP, SMB)
- 9% I Phishing / Spam
- 9% I Web or application server vulnerabilities
- 5% I SSL VPN
- 5% I No result(Customer self-formatted etc)
- 4% I From Endpoint(USB, user neglience etc)
- 4% I FW configuration change

SANGFOR

Stage 1: Intrusion – Social Engineering



Phishing (Spoofing)

Spear Phishing (Targeted phishing attack)

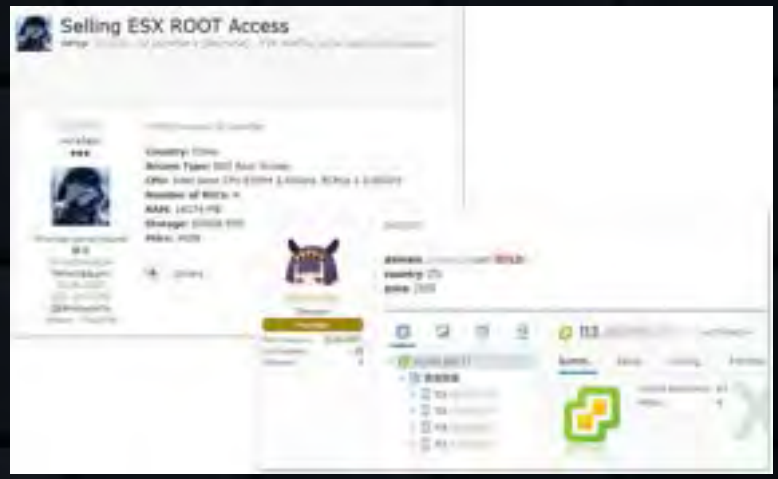
Stage 1: Intrusion – Vulnerabilities Attack

- Internet
Applicatio

Stage 1: Intrusion – Initial Access Brokers (IAB)

We don't sell rdp,we sell access to RMM (remote monitoring and management) software of the companies.

1- File transfer
2- CMD on all systems with
3- Deploy file on all systems
4- Run file on all systems
5- Uninstall AV from systems
6- Monitor Your process
7- Access to Domain controller + File Server + Some Backup Devices
8- Full access to registry
9- Deploy firewall rule on all pc and take it off
10- Change Wallpaper of all systems



Stage 2: Post Access

Ransomware is not only encrypting your data, but it is stealing your data too!!!

Stage 2: Post Access - Evasion

- Malware Sandbox Evasion Techniques

Malware

- Delaying Execution
- Hardware Detection
- CPU Detection
- User Detection
- Environment Detection

SANGFOR

Stage 2: Post Access - DGA

- DGA Algorithm Techniques

DGA Characteristics:

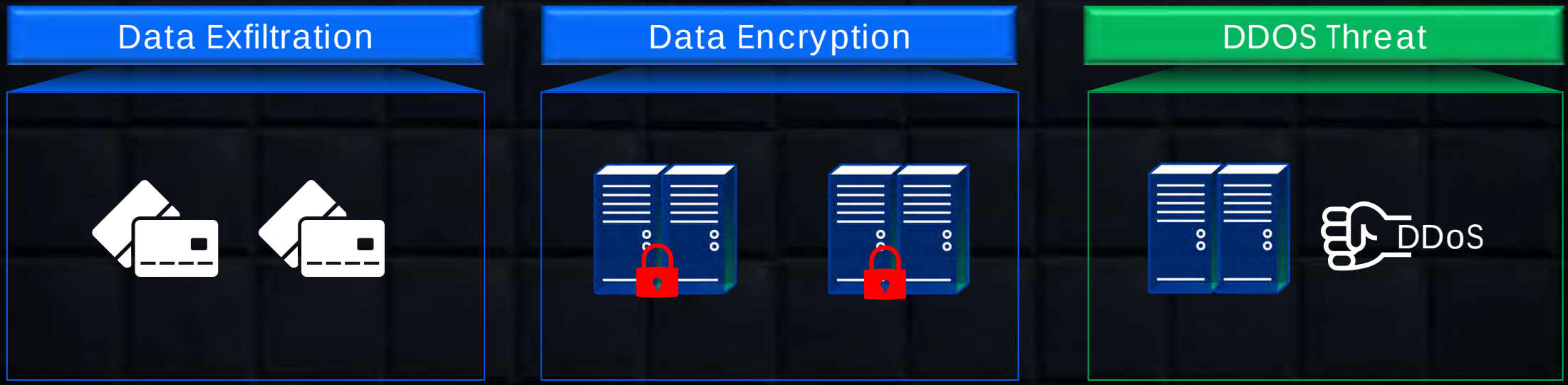
1. Resolve to the same IP
2. >90% can't be resolved
3. Human unreadable
4. Single use

Typical DGA: randomly generated, and uncreadable to humans	Variant 1: Joining words and random letters	Variant 2: Joining words
rhpmt.ws ciscqq.ws	speeh4ab5893940.me	fallcity.ru strengthbright.net
qckjqqel.ws wotybgr.ws	speeh062e9c0b96.cloud	fiftytold.net verygrow.net
qqjyfit.ws dhlfqaegj.ws	speeh062e9c0b96.vip	favorleft.ru callwear.net
mcoenfeoy.ws lhtryk.ws	speehe34a33001b.cloud	wellthirteen.net picturestream.ru

SANGFOR

Stage 3: Exploit

- Exfiltration and Impact



We Must Change Our Security Mindset

NIST Cybersecurity Framework

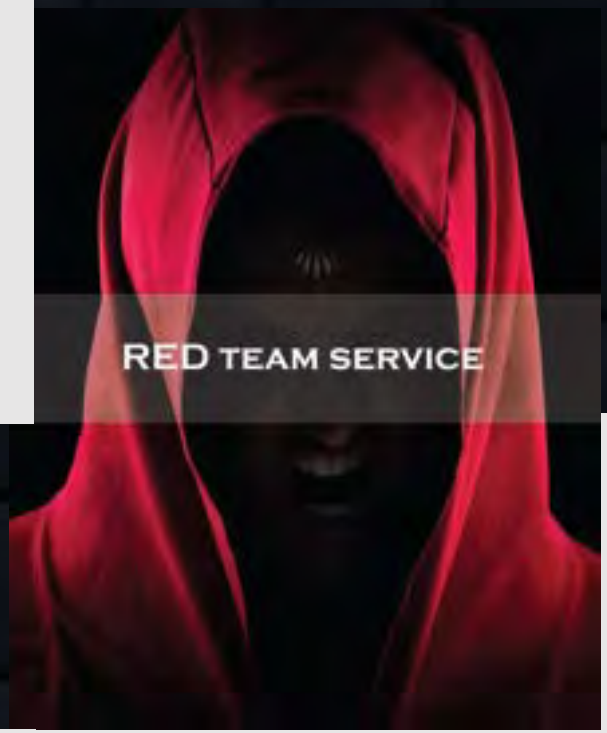
Assume attackers already inside

SANGFOR

PART 3

Tactics to Combat Ransomware

#1 | Risk Assessment



Know when you've lost your key

SANGFOR

#2 | Prevent Social Engineering Attack

- Email Security Gateway
- Security Awareness Guideline
- Security Ongoing Awareness Training

	Phase One: Initial Baseline Phishing Security Test Results			Phase Two: Phishing Security Test Results Within 90 Days of Training			Phase Three: Phishing Security Test Results After One Year-Plus of Ongoing Training		
	BASELINE			90 DAYS			1 YEAR		
Organization Size	1-249	250-999	1000+	1-249	250-999	1000+	1-249	250-999	1000+
REGION: North America	28.7%	30.2%	35.8%	17.4%	17.9%	17.4%	3.5%	4.6%	6%
		TOTAL: 32.4%			TOTAL: 17.5%			TOTAL: 4.7%	
Africa	30.2%	27.4%	32.4%	24.8%	21%	17.9%	8.1%	12.7%	4%
		TOTAL: 31.4%			TOTAL: 18.8%			TOTAL: 5.4%	
APAC (Asia, Oceania & Australia)	30.2%	32.6%	36.7%	21.1%	19.2%	15%	4.4%	6.2%	5.2%
		TOTAL: 34.5%			TOTAL: 16.9%			TOTAL: 5.4%	
Europe	27.8%	28.2%	31.1%	17.9%	18.2%	18.9%	4.2%	6.7%	8%
		TOTAL: 29.9%			TOTAL: 18.5%			TOTAL: 6.3%	
South America	30.9%	30%	45.6%	24.7%	22.2%	19.3%	1.8%	9.8%	0.8%
		TOTAL: 39.9%							
United Kingdom & Ireland	26.2%	27.7%	32.7%	16.7%	16.3%	17.5%	3.9%	4.3%	8.3%
		TOTAL: 30%			TOTAL: 17%			TOTAL: 5.5%	

Source: KnowBe4 Phishing by Industry Benchmarking Report 2022

#3 | 3-2-1 Backup Rule

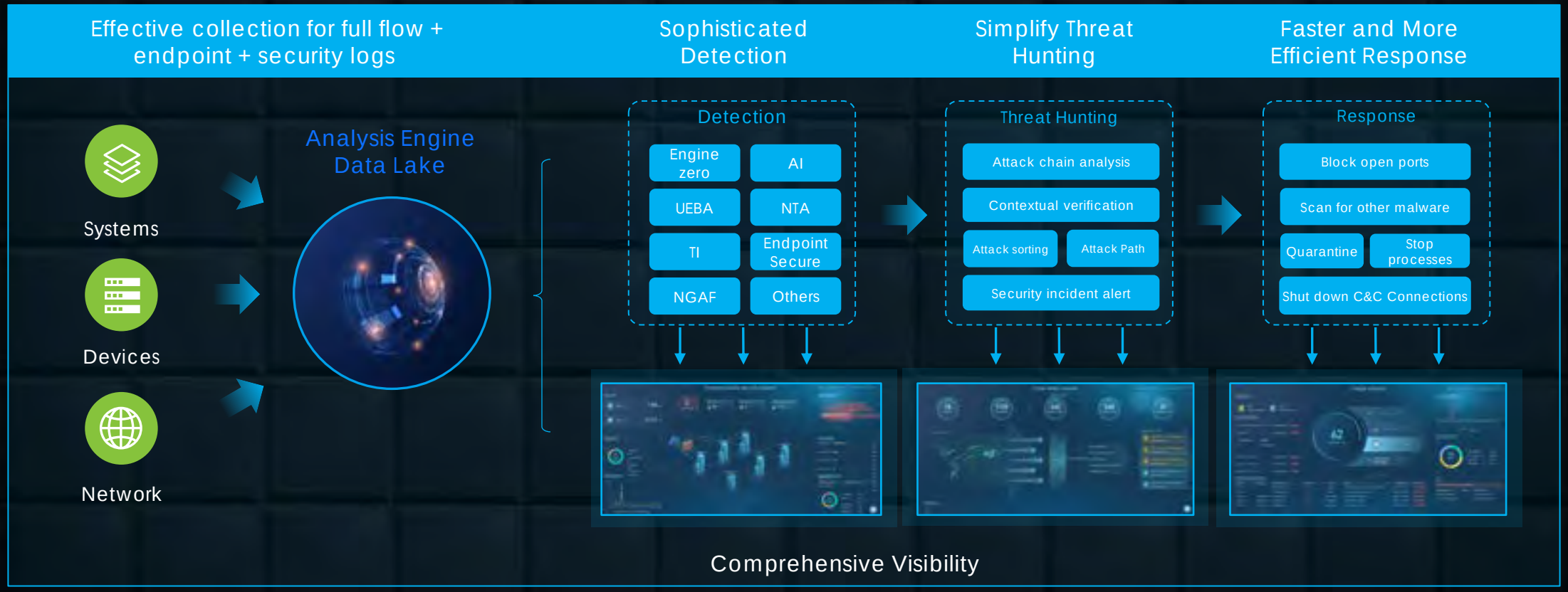
Maintain at least 3 copies of your data

Keep 2 copies stored at separate locations

Store 1 copy at an off-site location

SANGFOR

#4 | AI-based Continuous Threat Detection and Response



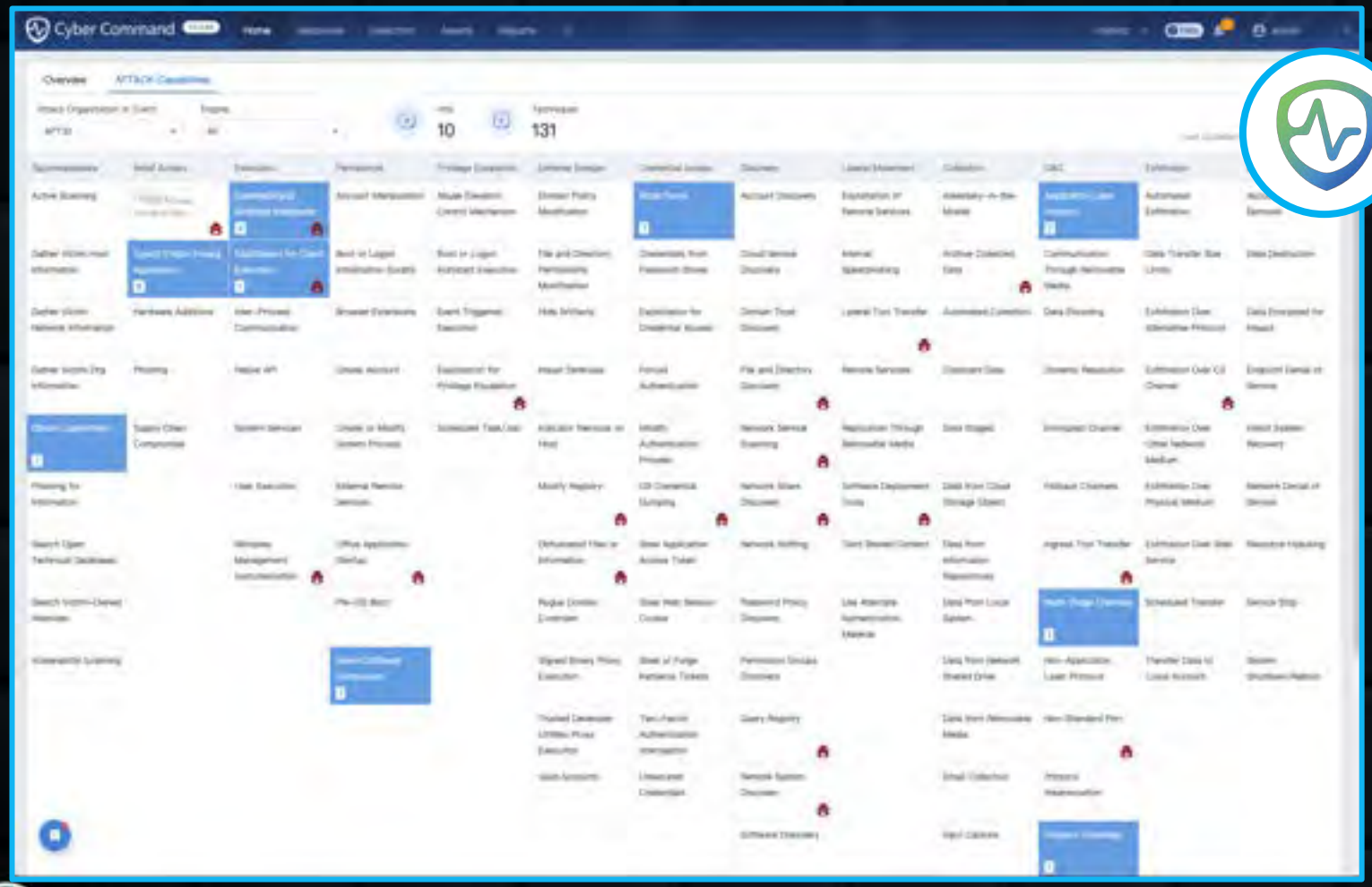
#4 | AI-based Continuous Threat Detection and Response

Purpose-built AI Detection Engines

Scenarios	Data	Main Characteristic	Algorithm	Types	Sangfor Products
DNS hidden tunnel	DNS log	The entropy of valid information in a domain name、access behavior	Random forests	supervised	Cyber Command, NGAF, Endpoint Secure
DGA domain name	DNS log	The entropy of valid information in a domain name、access behavior	NLP、graph analysis	supervised	Cyber Command, NGAF, Endpoint Secure
New malicious domain name	DNS log	The entropy of valid information in a domain name、access behavior	NLP、Anomalies detection	supervised + unsupervised	Cyber Command, NGAF, Endpoint Secure
Botnet family variant tracking	DNS log	Host-domain name - resolve IP graph structure information	graph analysis	semi-supervised	Cyber Command, NGAF, Endpoint Secure
HTTPS C&C	HTTPS log	TLS Handshake/certificate /background flow characteristics	Random forests	supervised + unsupervised	Cyber Command, NGAF
Encrypt RDP and SSH slow brute force	RDP log、SSH log	Access frequency, login status characteristics	Random forests	supervised	Cyber Command, NGAF, Endpoint Secure
Website defacement	web access log	Syntactic features of web content	NLP	supervised	Cyber Command, NGAF
Engine-Zero files anti-virus	files	Static file characteristics	XGBOOST	supervised	Cyber Command, NGAF, Endpoint Secure
webshell	HTTP log	URL grammar characteristics, traffic behavior characteristics	NLP	supervised	Cyber Command, NGAF
Abnormal outbound behavior	session	traffic behavior characteristics	Anomalies detection	unsupervised	Cyber Command
Abnormal login behavior	login log	Login behavior characteristics	Anomalies detection	unsupervised	Cyber Command
Attack path recovery	multiple log	multiple logs correlation characteristics	Knowledge mapping	unsupervised	Cyber Command

#4 | AI-based Continuous Threat Detection and Response

MITRE ATT&CK Capabilities

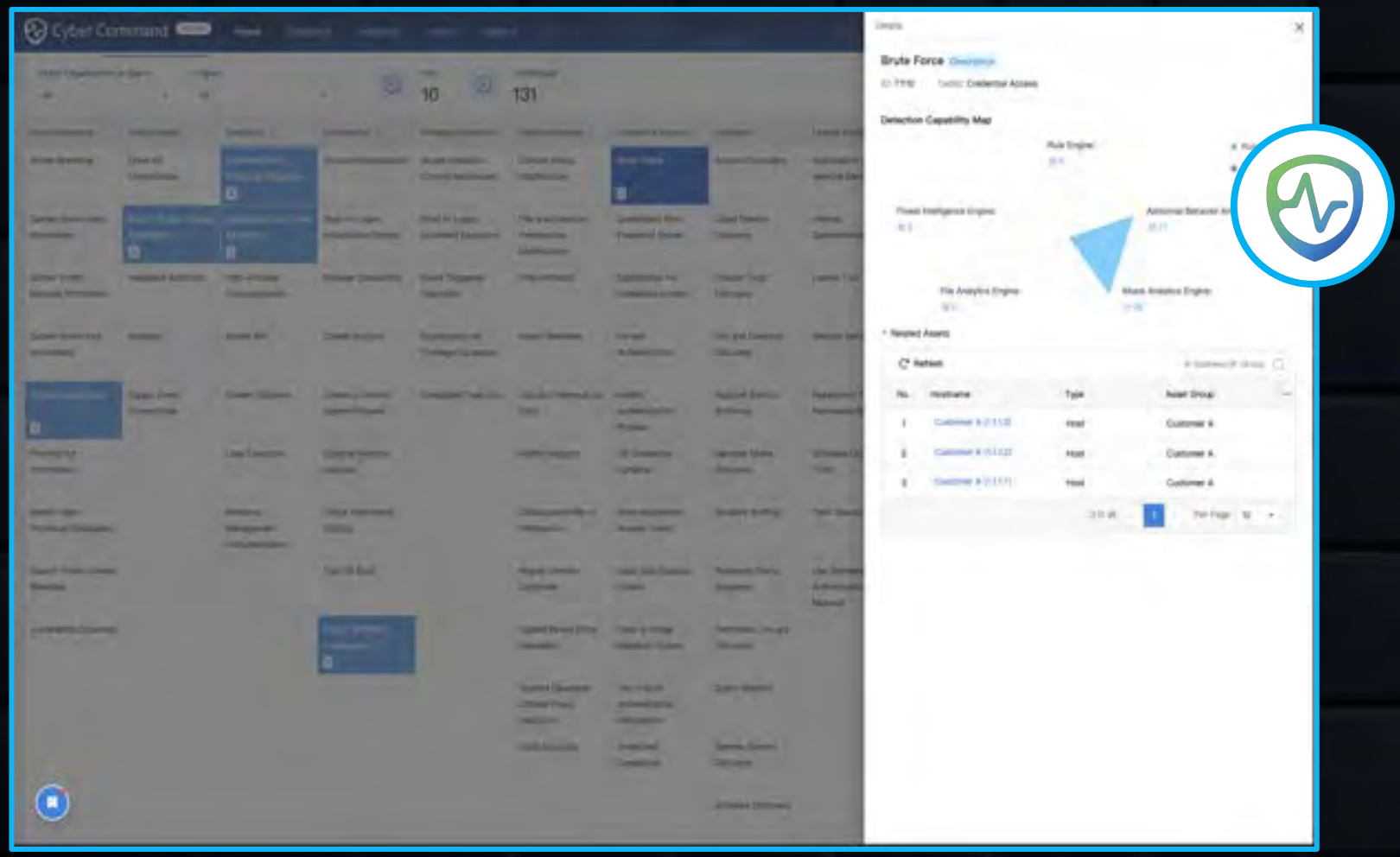


Complete coverage for MITRE ATT&CK tactics and techniques

- 100% coverage for network techniques
- APT organizations intrusion methods insight
- Security awareness for your own environment

SANGFOR

#4 | MITRE ATT&CK Capabilities



Comprehensive insight for the specific technique

- 5 detection engines mapping for each technique
- Correlate risk assets for the specific technique
- Support drill down to further investigate

SANGFOR

#4 | Integrated SOAR with Existing Security Ecosystem

- Automate response
- Integrate with existing processes

SIEM

QRadar

ArcSight An HP Company

splunk>

LEEF

Forward events

CEF

Cyber

Security Orchestration

Firewall

paloalto NETWORKS | SOPHOS | FORTINET | Check Point SOFTWARE TECHNOLOGIES LTD | CISCO | JUNIPER NETWORKS | Coming Soon

Endpoint

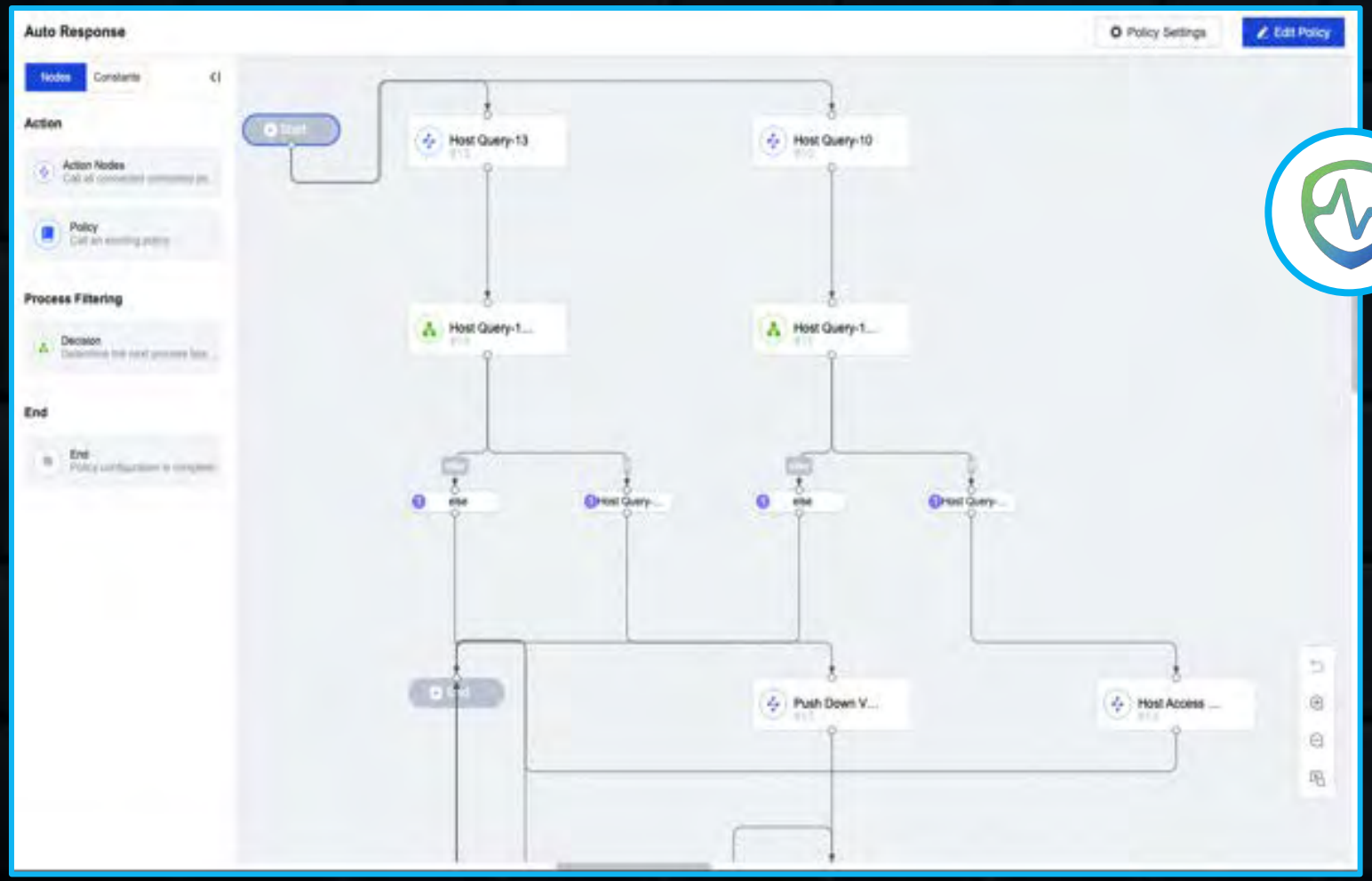
Bitdefender | Windows Defender ATP | SOPHOS | Symantec | McAfee | kaspersky | TREND MICRO | F-Secure | Coming Soon

Other

macmon | vmware | Coming Soon

SANGFOR

#4 | WYDIWYG SOAR Module

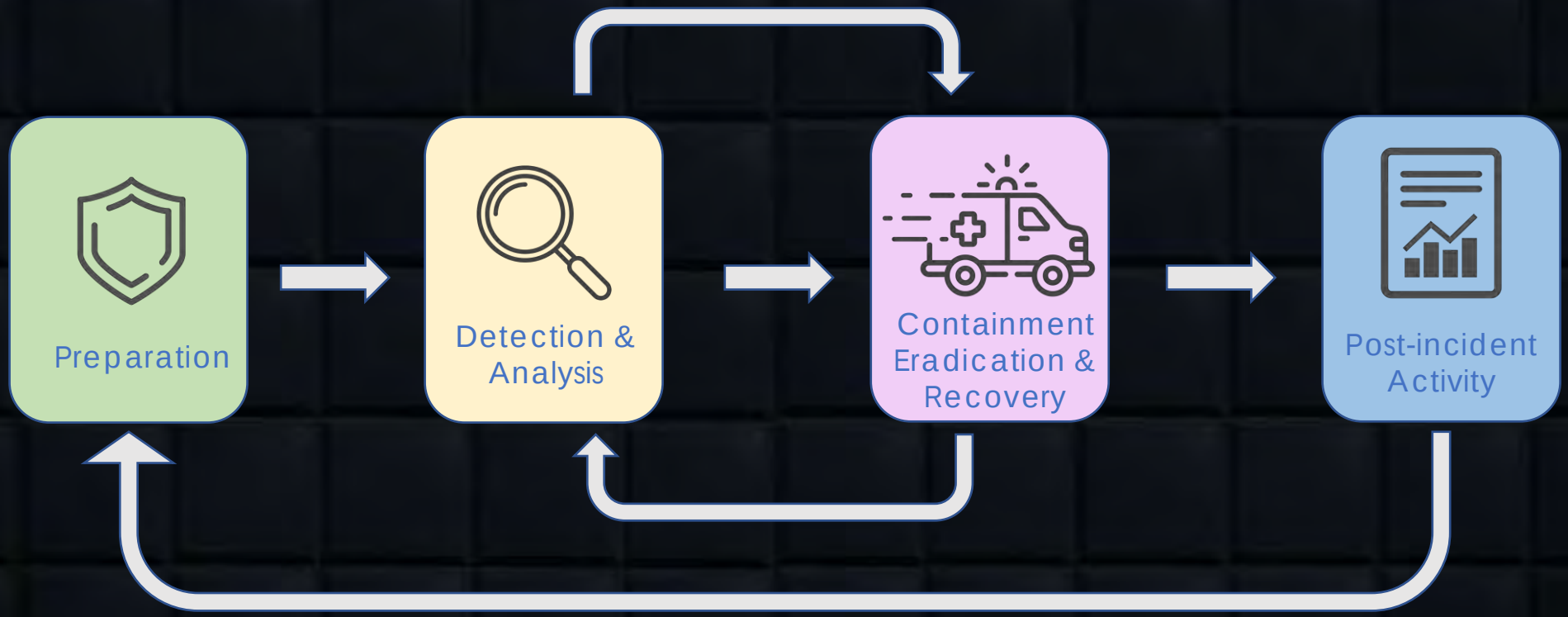


Cyber Command SOAR is a workflow Automation engine

- Flexible integrate with 3rd party security devices
- Built-in playbook template to support common scenarios
- Intuitive, visual playbook editor


“Nothing is 100 % Secured”
What if I’m still being attacked
by Ransomware?

Incident Response



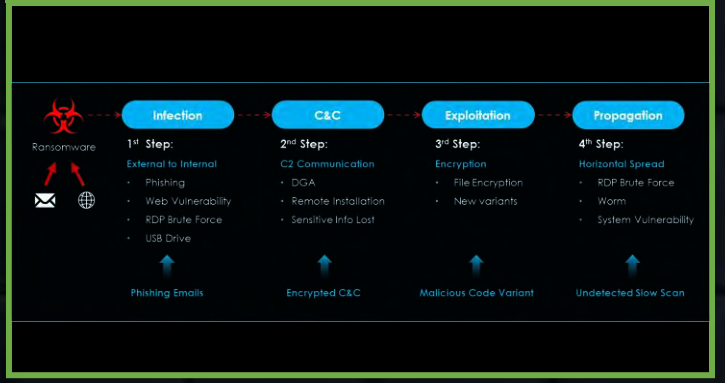
PART 4 Takeaways

Takeaways

We Must Change our Security Mindset

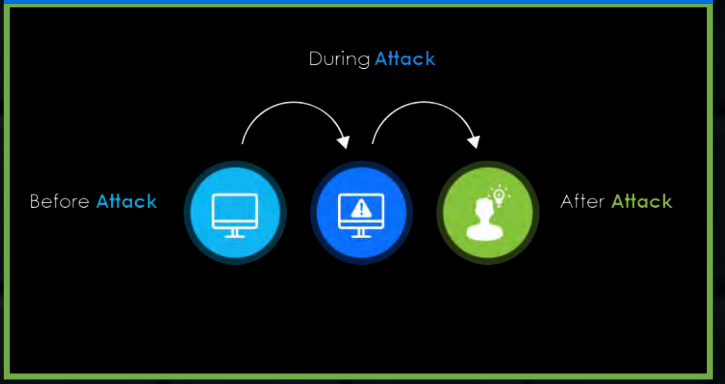
- Assume attackers are already inside
- Start threat hunting looking for signs of breach
- Assessment, Assessment, Assessment!!!

Continuous Threat Detection



- Use purpose-built AI to combat AI
- Block every step in the kill chain and leverage NDR solution

Leverage IR and post attack assessment services



- IR services contain ransomware impact
- Threat hunting services find root-cause and provide customized remediation solutions

SANGFOR

SANGFOR

THANK YOU!

Paul Tsang | Senior Regional Solution Architect, CISSP
paul.tsang@sangfor.com
SANGFOR Technologies Inc.