

Al Virtuálny Bezpečnostný Analytik pre SecOps

Peter Kocik Systems Engineer CEE

> BMW i Motorsport Official Partner



One – Two Punch

Targeted Ransomware Attacks Data Exfiltration

Drop Destructive Payload



Incident Response Process



F

Traditional SecOps Approach

Human element that consist of SecOps analyst(s) that manage security technologies and drive threat resolution within a well defined process *Problem: InfoSec Shortage*

Products that provides threat visibility and response actions *Problem: Traditional Detection*



A systematic approach to detect, investigate and respond to threats *Problem: Manual Processes*



FortiAl

Virtual FortiGuard Analyst on your team

110





Virtual Security Analyst[™] powered by Deep Neural Networks that **identifies**, classifies, and investigates sophisticated threats in sub-second, and proactively blocks them.

Identify

Disrupt threats with subsecond detection and adapts to new threats instantaneously.

Solves

SecOps are facing increased volume, velocity and sophistication of threats

Dashboard	>	^ Discovery Date ♥	Infected Host IP 🌲	Device 🗢	VDOM 🗘	Malware Family
Security Fabric	>		40.40.00	C		
Attack Scenario	~	2020/06/23 13:53:06	10.10.10.23	Sniffer	Sniffer	PornoAsset
Attack Scenario Sun	nmary	2020/06/23 17:17:31	10.10.10.27	Sniffer	Sniffer	PornoAsset
Fileless	0	2020/06/23 13:04:20	10.10.10.57	Sniffer	Sniffer	Ruledor
Industroyer	0	2020/06/23 13:36:30	10.10.10.23	Sniffer	Sniffer	Small
Wiper	0	2020/06/23 13:36:30	10.10.10.23	Sniffer	Sniffer	Small
Ransomware	611	2020/06/23 13:37:10	10.10.10.23	Sniffer	Sniffer	Small
Worm Activity	374	2020/06/23 13:37:15	10.10.10.23	Sniffer	Sniffer	Small
Data Leak	444	2020/06/23 13:37:32	10.10.10.23	Sniffer	Sniffer	Small
Exploit	31	<				
Botnet	2	Attack Timeline at Host 10.10.10	.57			
Backdoor	906		Downloader	Downloader	Worm	
Banking Trojan	2k	40 40 40 4				
Rootkit	10	10.10.10.4			280	
Scenario Heuristic	8					
DoS	6					
Generic Trojan	2k		JS/Crypt.BBES!tr	W32/Waski.A!tr	W32/Palevo	p.BWC!worm.p2p
Sophisticated	14		O days 0 hours 0 minutes 0 seconds	O days 0 hours 0 minutes 1	seconds O days 0 hou	urs 0 minutes 3 seconds
Application	39		HTML Downloader Benjamin	PE Downloader Dinw	vod PE Worm	Ruledor
Cryptojacking	217					
					loss than a soor	

F



Virtual Security Analyst[™] powered by Deep Neural Networks that identifies, **classifies**, and investigates sophisticated threats in sub-second, and proactively blocks them.

Classify

Scientifically analyze IT and OT malware to accurately determine the type of threat and reduces false positives.

Solves

Masquerading malware evades security controls and prolongs mitigation effort.

			- Ranking Trojan Inf	netaalar Evoloit	Phiching and	many
FortiAI VM FA	IVMS00000	00000	Danking Hojan, ini		r morning, and	r mariy ≻_ ∷
🚯 Dashboard	> '	^				Family 🖨
🔆 Security Fabric						
Attack Scenario	~	2020/06/23 13:53:06	10.10.10.23	Sniffer	Sniffer	PornoAsset
• Attack Scenario Sur	nmary	2020/06/23 17:17:31	10.10.10.27	Sniffer	Sniffer	PornoAsset
Fileless	0	2020/06/23 13:04:20	10.10.10.57	Sniffer	Sniffer	Ruledor
Industrover	0	2020/06/23 13:36:30	10.10.10.23	Sniffer	Sniffer	Small
Wiper	0	2020/06/23 13:36:30	10.10.10.23	Sniffer	Sniffer	Small
Ransomware	611	2020/06/23 13:37:10	10.10.10.23	Sniffer	Sniffer	Small
Worm Activity	374	2020/06/23 13:37:15	10.10.10.23	Sniffer	Sniffer	Small
Data Leak	444	2020/06/23 13:37:32	10.10.10.23	Sniffer	Sniffer	Small
Exploit	31	<				
Botnet	2	Attack Timeline at Host 10.10.1	0.57			
Backdoor	906		Downloader	Downloader	Worm	
Banking Trojan	2k	10 10 10 4	\mathbf{A}	\mathbf{A}	\land	
Rootkit	10	10.10.10.4				
Scenario Heuristic	8					
DoS	6				W/22 /Dalaus	DM/Cluster # 2#
Generic Trojan	2k		JS/Crypt.BBES:tr	VV 32/ VVaski.A:tr	vv32/Palevo.	BvvC:worm.p2p
Sophisticated	14		O days 0 hours 0 minutes 0 seconds	O days 0 hours 0 minutes 1 seconds	s O days O hour	s 0 minutes 3 seconds
Application	39		HTML Downloader Benjamin	PE Downloader Dinwod	PE Worm	Ruledor
Cryptojacking	217					

2

Classify IT and OT threats: Industrover, Wiper, Fileless, Ransomware, Worm, Downloader, Dropper, Rootkit,



7



Virtual Security Analyst[™] powered by Deep Neural Networks that identifies and classifies, and investigates sophisticated threats in sub-second, and proactively blocks them.

3

Investigate

Speeds investigation by analyzing the entire threat movement and identifies patient zero and subsequent victims in real-time.

3

Solves

Manual investigation of a malware outbreak/lateral spread







Virtual Security Analyst[™] powered by Deep Neural Networks that identifies and classifies, and investigates sophisticated threats in sub-second, and proactively **blocks** them.

Automated Response

Quarantines these threats in real-time found in the network through the seamless integration with FortiGate.

Solves

Manual mitigation efforts to an on-going attack or an outbreak scenario

Dashboard	>	Quarantine Policies			
Security Fabric	~	Risk Level			
Enforcement Settings		Radio Field Critical Risk High Risk Medium Risk Low Risk			
Automation Framework Automation Log		Confidence Level			
Attack Scenario	>	Quarantine Confidence level equal and above 80 % Medium High			
Host Story	>	White List			
Virtual Security Analyst	>	Edit White List			
+ Network	>				
System	> > >	T Edit Delete			
🛔 User & Device		IP ≑			
🖹 Log & Report		172.16.77.45/32			
		10.10.4.0/24/24			
		192.168.110.0/24			
		4 · · · · ·			
		Apply			

FortiGate quarantine based on FortiAI risk & confidence levels



Example: WannaCry Response Life Cycle

The traditional approach with SecOps analysts only

Detect (1+ hrs)

- Assume out of 100's 1000's threats alerts on a SOC dashboard, threat selected happen to be ransomware or,
- Alerted directly by an affected user



Investigate (4+ hrs)

- Log into security product(s)
- Review logs/alerts
- Use built-in and external tools to validate ransomware
- Perform external research
- Log into security product(s) to search for WannaCry's lateral movement
- Create mitigation plan

Respond (2+ hrs)

- Quarantine devices(s), network segment
- Remediate device(s)/restore back-up
- Apply patches
- Close ticket

Example: WannaCry Response Life Cycle

SecOps analyst augmented with Deep Neural Networks (AI)



- Al: Ransomware validated in sub-second
- AI: Self-learns new ransomware features



- Al integrated with Security Controls:
 - Quarantine devices(s), network segment
- SecOps follow-up:
 - Remediate device(s)/restore backup
 - Apply patches
- Close ticket



Investigate (<5 mins)

- Al: Provides WannaCry kill-chain with contextual threat research
- AI: Identify WannaCry patient-zero & lateral movement
- SecOps: Create mitigation plan

FERTINET®

BMW i Motorsport Official Partner

