



Автоматизація інформаційної безпеки

Alexander Kulakovskiy

Sales Representative ITOM/ADM and SRG Solution



Трохи цифр

Ці ризики мають вартість

За період Січень- Червень 2020, було виявлено....

2,037 зламів та виставлено в DarkNet

27,000,000,000 записів



Статистика

80%

Споживачів змінювали
постачальника сервісів у разі
витоку їх даних

Source: [IDC Research \(as reported by Varonis\)](#)

93%

Користувачів подавали до суду на
постачальника сервісу у випадку витоку
їх даних

Source: [Gemalto Survey \(as reported by Tech Wire Asia\)](#)

\$3,86 М

Середня вартість наслідків кібер-атак

Source: [Ponemon Institute, 2020](#)



280 днів

Середній період
виявлення зламу

Source: [Ponemon Institute, 2020](#)



Arcsight SIEM

Що таке SIEM?

Комплексна платформа виявлення та аналізу загроз в режимі реального часу, яка значно скорочує час на виявлення та реагування на загрози.



1: Збір

Технічних даних з усіх активних елементів ІТ інфраструктури, таких як: Firewall, IPS, Сервери, ПЗ, анти-віруси, тощо.



2: Стандартизація

Форматів, протоколів та виду даних з пристроїв різних виробників в загальноприйнятій формат подій



3: Збагачення

Зібраних даних артефактами, таксономією, первинною аналітикою з урахуванням деталей мережі та об'єктів



4: Зберігання

Зібраних даних у захищеному вигляді з компресією 10:1, яке зменшує витрати, навіть для лог-записів за декілька років



5: Пошук та аналіз

З використанням текстового інструменту з інтуїтивним інтерфейсом та локалізацією



6: Виявлення та запобігання

В режимі реального часу будь-якій загрозі чи порушенню



Автоматизація за допомогою ArcSight SOAR



Автоматичне сортування

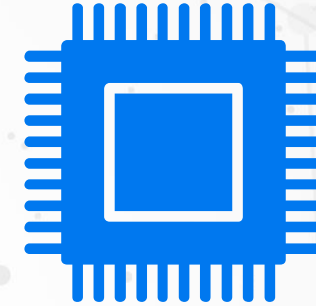
- Критичність події
- Консолідація подій в інциденти
- Робота з карткою інциденту

Повна автоматизація роботи 1 рівня підтримки



Збір даних

- Кінцеві пристрої, Сервери, Мережа
- HR, СКУД
- SIEM, Логи
- Програмне забезпечення
- Хмари



Обмежувальні дії

- NAC/Поміщення в карантин
- Блокування на рівні Firewall, Web-шлюзів, тощо
- Блокування або видалення облікових записів
- Фізичне блокування на рівні СКУД
- тощо*

3
можливістю узгодження

*ініціація або зупинка будь-якого технологічного процесу



Приклад #1: компрометація користувача





Приклад #2: виток інформації





Приклад #3: Розслідування фішингу





Приклад #4: Взаємодія з CERT



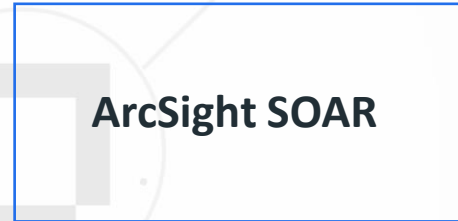
National
CERT

1. CERT sends IPs,
Hashes and
URLs to block



SMTP

2. Receive
Email



ArcSight SOAR

3. Extract all IPs,
hashes,
URLs etc.

4. Block URLs on
Web Gateway(s)



Web Gateway

5. Block hashes on EPP

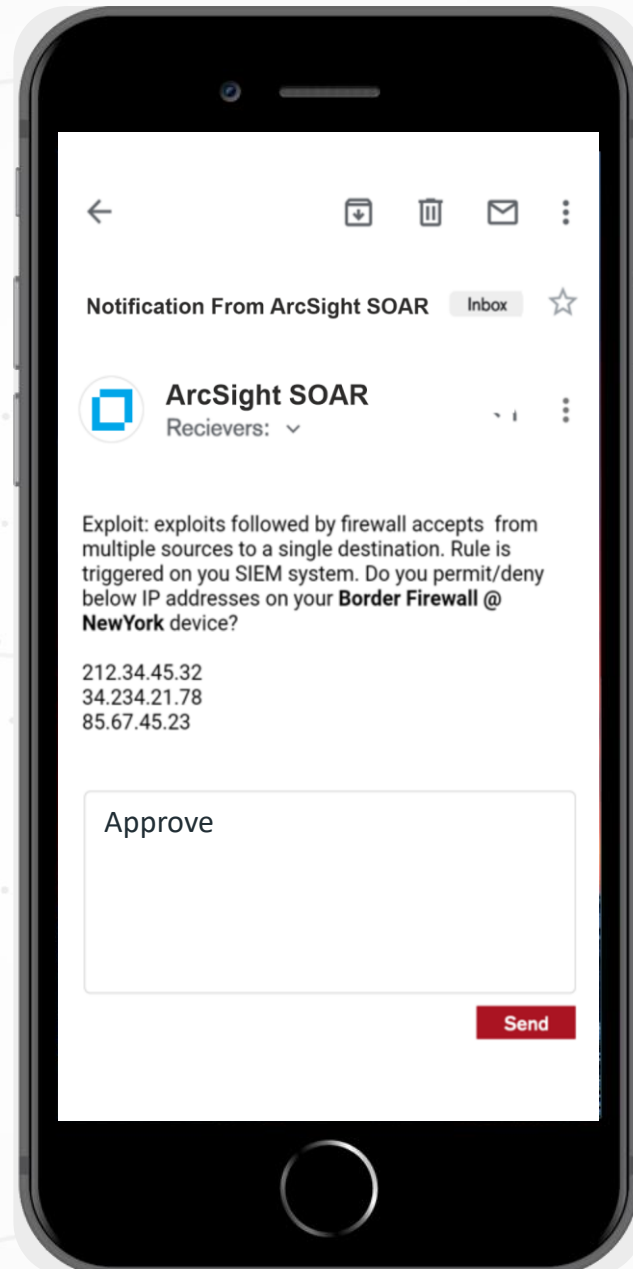


6. Block IPs on firewall(s)



Border Firewalls

Швидка реакція



з узгодженням дій



Створення алгоритмів ArcSight SOAR

Workflow Playbook Editor

Playbook Name: Lateral Movement Investigation

Advanced Playbook Editor

Name: Incident Search Label

Matching Mode: All conditions

Rollback Mode: Permanent (no rollback)

Incident auto-close: Don't close

Script language: Javascript

Create Conditions

ID	Type	Parameters
1	var incidents = atar.incidentSearch().label("High").execute();	
2		
3	for(var index = 0 ; index < incidents.length ; index++){	
4	print(incidents[index].getProject().getName());	
5	print(incidents[index].getSerial());	
6	}	

Test Playbook

No selected alert source | Offender | Impact | Test

Close Save

ArcSight SOAR 2.22.4 (20200817191552) - © Copyright 2020 - Licensed to: MicroFocus



120+ Інтеграцій

Threat Intelligence



SIEM & Analytics



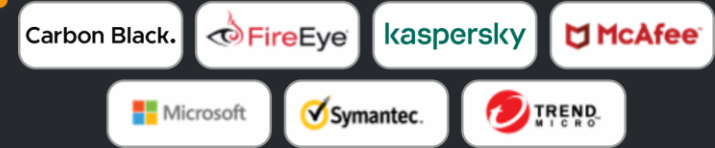
Security Testing



Mail Security



Endpoint Protection / EDR



Web Gateway



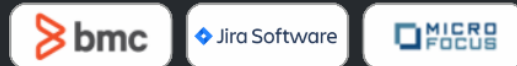
Network Security



Others



Service Desk



Micro Focus має власний MITRE ATT&CK

MICRO FOCUS Layered Analytics (All) Real-Time Machine Learning Search and Hunt Partner

Layered Analytics
ArcSight's three analytics solutions can seamlessly be combined to form a "Layered Analytics" approach. This 'best of br... [Read more](#)

Initial Access 8	Execution 11	Persistence 15	Privilege Escalation 11	Defense Evasion 24	Credential Access 11	Discovery 22	Lateral Movement 8	Collection 13	Command and C... 14	Exfiltration 7	Impact 6
Drive-by Compromise	Command and Scripting...	Account Manipulation	Abuse Elevation...	Abuse Elevation...	Brute Force	Account Discovery	Exploitation of Remote S...	Archive Collected...	Application Layer Pro...	Automated Exfiltration	Data Encrypted for Impact
Exploit Public-Fac...	Exploitation for Client...	BITS Jobs	Access Token Manipulation	Access Token Manipulation	Credentials from Passw...	Application Window Disc...	Remote Service S...	Audio Capture	Communication Through Remo...	Data Transfer Size Limits	Inhibit System Recovery
External Remote Serv...	Inter-Proces s Communi...	Boot or Logon Aut...	Boot or Logon Aut...	BITS Jobs	Credentials from Web...	Browser Bookmark DI...	Remote Services	Clipboard Data	Data Encoding	Exfiltration Over Alterna...	Network Denial of...
Hardware Additions	Dynamic Data Exc...	Authenticat ion Package	Authenticat ion Package	Deobfuscate / Decode File...	Exploitation for Credent...	Cloud Service Discovery	Replication Through Remo...	Data Staged	Data Obfuscation	Exfiltration Over C2 Chan...	Resource Hijacking
Phishing	Native API	Kernel Modules...	Kernel Modules...	Exploitation for Defense...	Forced Authentication	File and Directory...	Shared Webroot	Data from Information...	Dynamic Resolution	Exfiltration Over Other N...	Service Stop
Replication Through Remo...	Scheduled Task / Job	LSASS Driver	LSASS Driver	Hide Artifacts	Input Capture	Network Service Sc...	Software Deployment...	Data from Local System	Encrypted Channel	Exfiltration Over Physica...	System Shutdown / R...
Trusted Relationship	Scheduled Task	Registry Run Keys / ...	Registry Run Keys / ...	Hidden Files and...	Modify Authenti...	Network Share Discovery	Taint Shared Content	Data from Network Sha...	Fallback Channels	Scheduled Transfer	
Valid Accounts	Shared Modules	Security Support...	Security Support...	Hidden Window	Network Sniffing	Network Sniffing	Use Alternate...	Data from Removable M...	Ingress Tool Transfer		
	Software Deployment...	Shortcut Modific...	Shortcut Modific...	NTFS File Attributes	OS Credentia...	Password Policy Dis...		Email Collection	Multiband Communication		
	Source	Time Providers	Time Providers	Hijack Execution...	Steal or Forge Ker...	Peripheral Device Disc...		Input Capture	Non-Applicatio n Layer Prot...		
	System Services	Winlogon Helper DLL	Winlogon Helper DLL	Impair Defenses	Two-Factor Authentica...	Permission Groups Disc...		Man in the Browser	Non-Standard Port		
	User Execution	Boot or Logon Initializa...	Boot or Logon Initializa...	Indicator Removal on...	Unsecured Credentials	Process Discovery		Screen Capture	Proxy		
	Windows Management...	Browser Extensions	Create or Modify Sy...	Indirect Command Exe...		Query Registry		Video Capture	Remote Access Software		
		Create Account	Event Triggered...	Masquerading		Remote System Discovery			Web Service		
		Create or Modify Sy...	Exploitation for Privil...	Modify Authenti...		Software Discovery					

Legend

- Technique covered in Real-Time
- Technique covered in Machine Learning
- Technique covered in Search and Hunt
- Technique covered in Partner
- Not covered in content

Arcsight – лідер ринку Інформаційної Безпеки



\$4B

інвестиції компанії Micro Focus в інновації продуктів Інформаційної Безпеки



81

Центрів
Кіберзахисту
створено
«під ключ»



485+

патентів у сфері
Інформаційної
Безпеки



75PB

найбільша
«Приватна
Хмара» у світі



450M+

пристроїв та ПЗ



2000+

сертифікованих
спеціалістів



10/10

Найбільших
банків світу

65TB

даних для
розслідувань
у форензиці



9/9

платіжних систем



145M

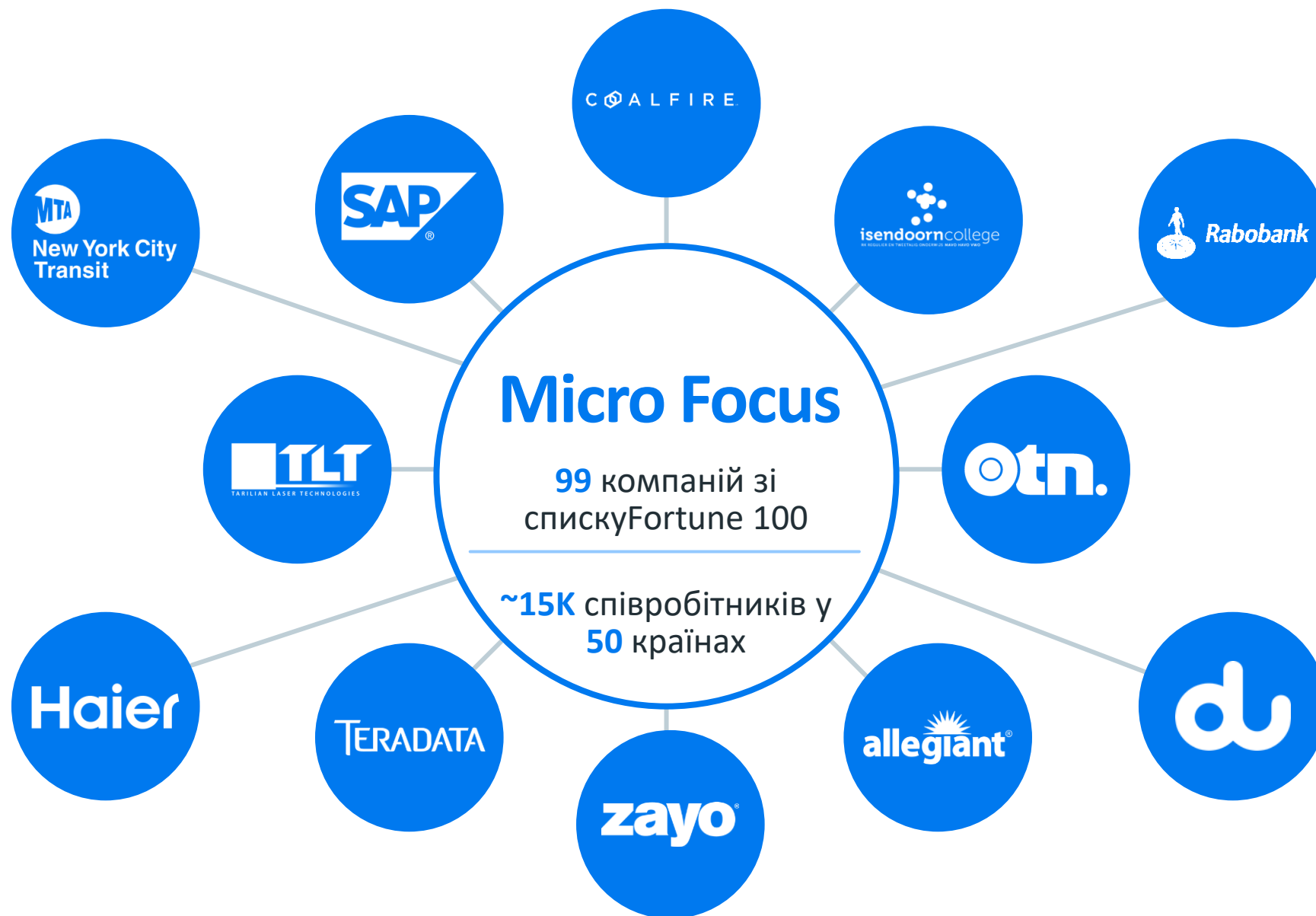
документів 1100
адвокатів
захищено



20+

досвіду в
Інформаційній
Безпеці

Глобальні Клієнти





Дякую!

Alexander.Kulakovskiy@microfocus.com