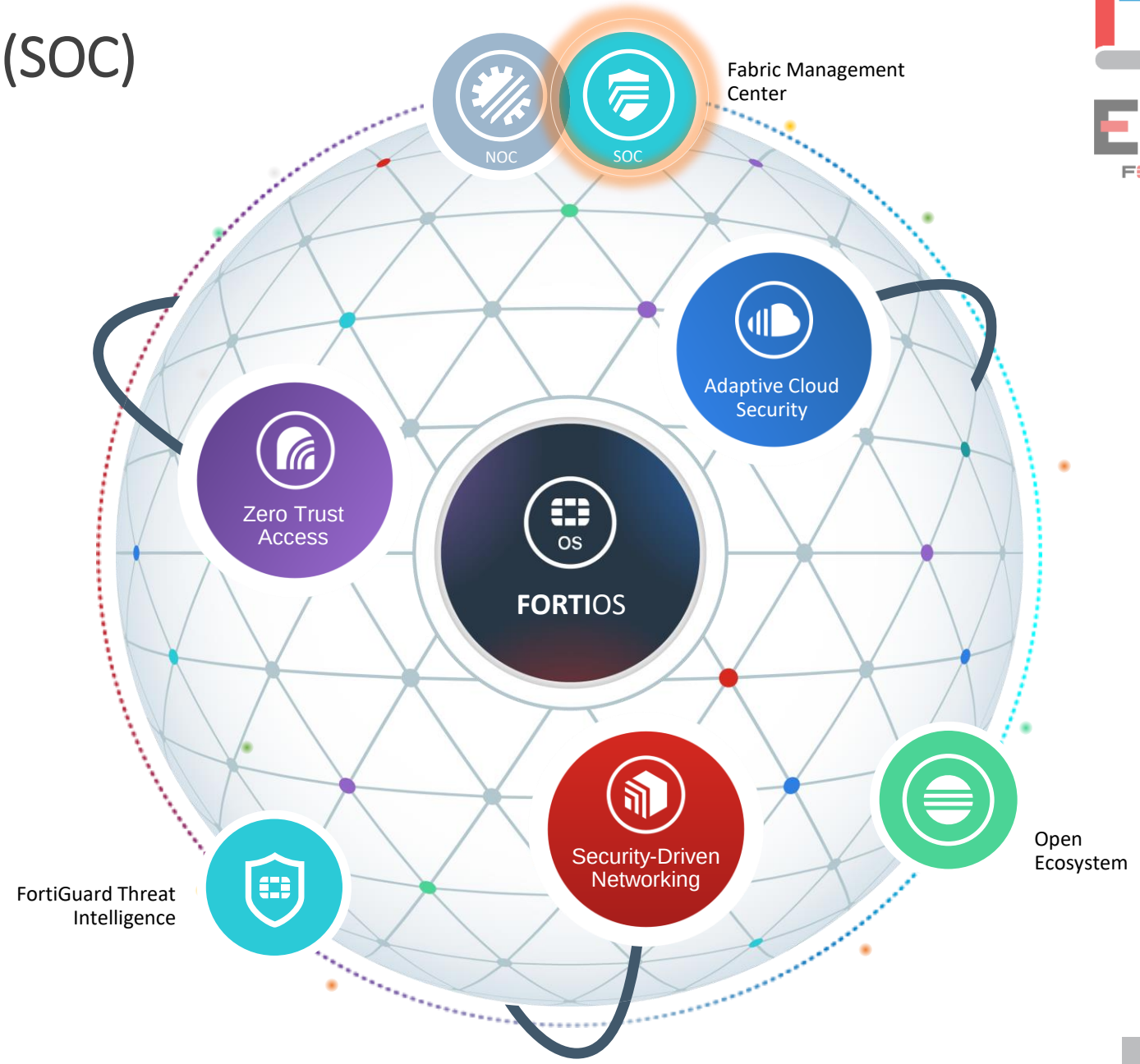
FORTINET

IT Solution FACTOR

FortiDeceptor

DECEIVE | EXPOSE | ELIMINATE THREATS

Security Operations (SOC)



IT Solution FACTOR

ENGAGE

FORTINET EXPERT PARTNER

Agenda

IT Solution FACTOR

ENGAGE

FORTINET EXPERT PARTNER

1 Dojrzałość SOC

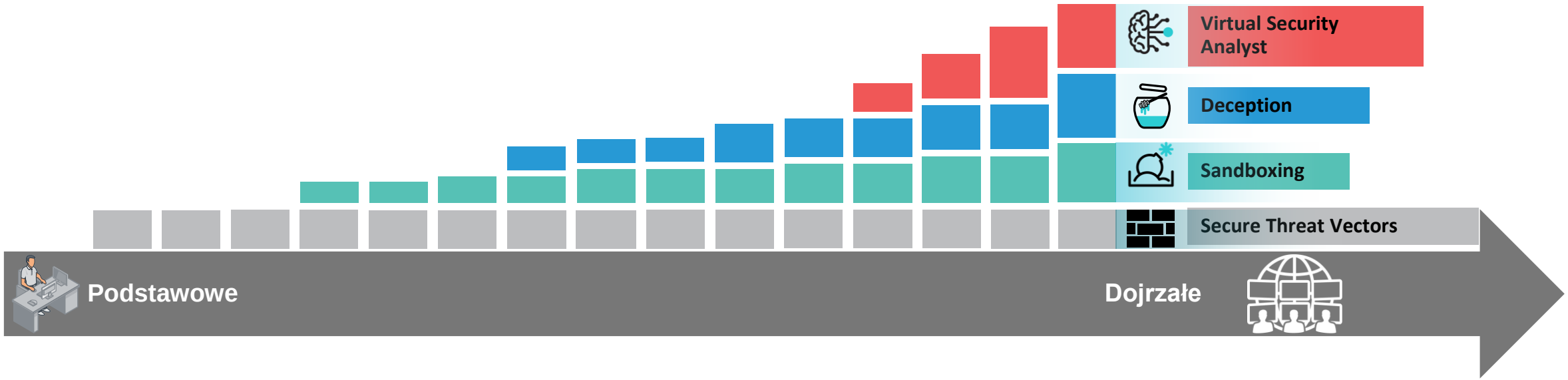
2 Ochrona przeciwko zagrożeniom

3 Weryfikacja rozwiązań

4 Ekosystem Security Fabric

Struktura Cyfrowego Bezpieczeństwa

SOC Maturity Model



Struktura Cyfrowego Bezpieczeństwa

Lockheed Martin Kill Chain

IT Solution FACTOR

ENGAGE

FORTINET EXPERT PARTNER

Struktura Cyfrowego Bezpieczeństwa

ATT&CK Matryca dla przedsiębiorstw

IT Solution FACTOR

ENGAGE

FORTINET EXPERT PARTNER

MITRE | ATT&CK®

ATT&CK Matrix for Enterprise

layout: side ▾ | show sub-techniques | hide sub-techniques

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery
10 techniques	7 techniques	9 techniques	12 techniques	19 techniques	13 techniques	39 techniques	15 techniques	27 techniques

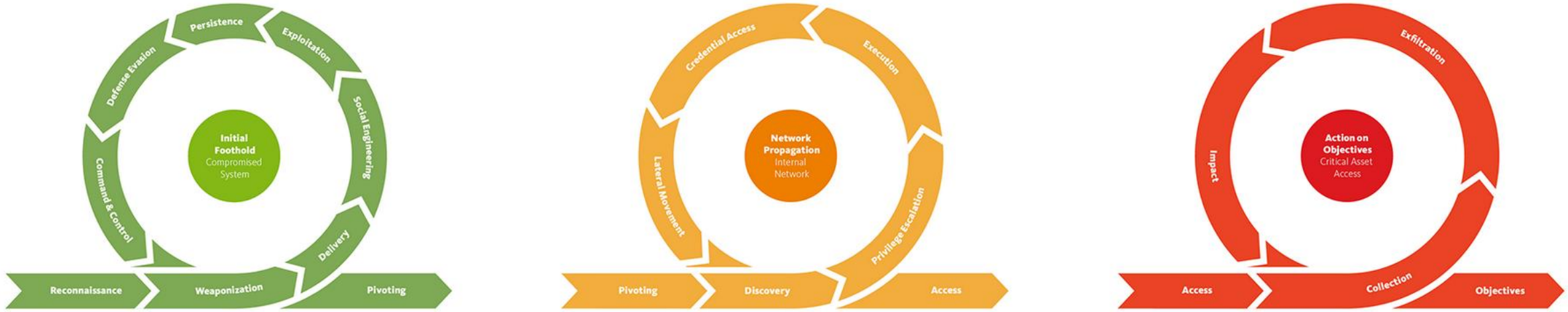
Struktura Cyfrowego Bezpieczeństwa

The Unified Kill Chain

IT Solution FACTOR

ENGAGE

FORTINET EXPERT PARTNER



Decepcja

Zakłócanie działań cyberprzestępców

Wyzwanie

zewnętrzne

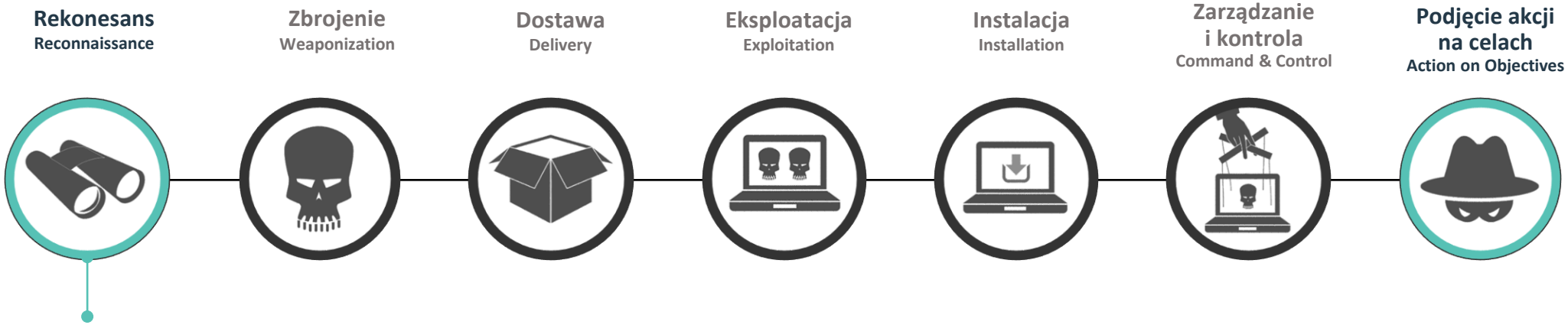
i wewnętrzne zagrożenia

minimalizacja kosztów

przełamania zabezpieczeń

Decepcja

Zakłócanie działań cyberprzestępców



Wyzwanie

Przeciwnie do tradycyjnego podejścia do bezpieczeństwa, gdzie chroniony musi zawsze mieć 100% racji, a atakujący musi mieć tylko raz trochę szczęścia, narzędzia zwodzące wywracają ten model do góry nogami**. Teraz to atakujący musi mieć 100% racji co do czasu ataku, albo w przeciwnym razie trafić na pułapkę, a obrońca musi mieć szczęście tylko raz, aby ta pułapka zadziałała.**

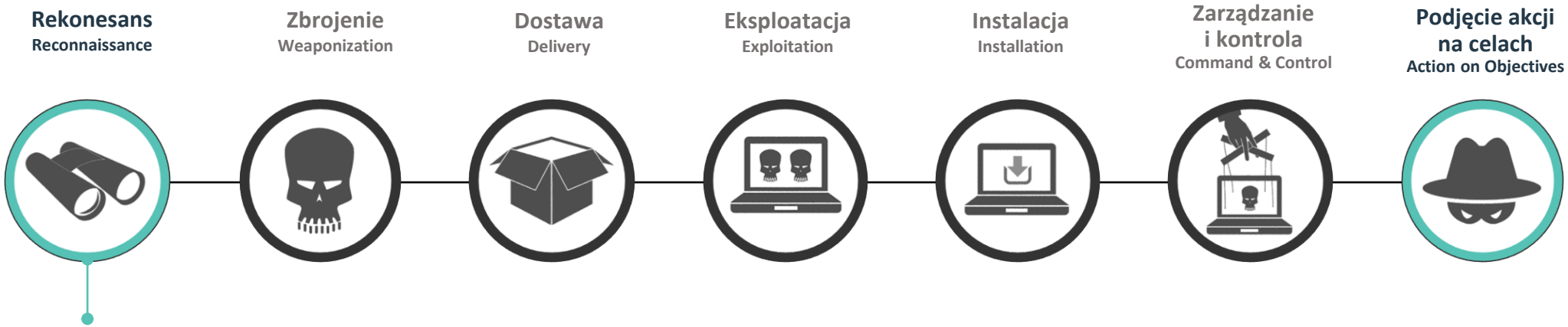
Zwodzenie

Zakłócanie działań cyberprzestępców

IT Solution FACTOR

ENGAGE

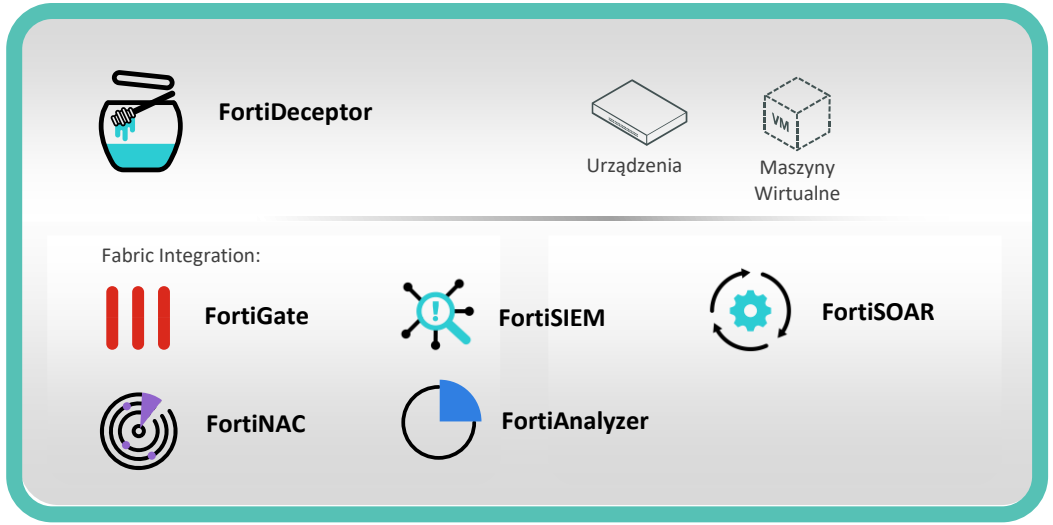
FORTINET EXPERT PARTNER



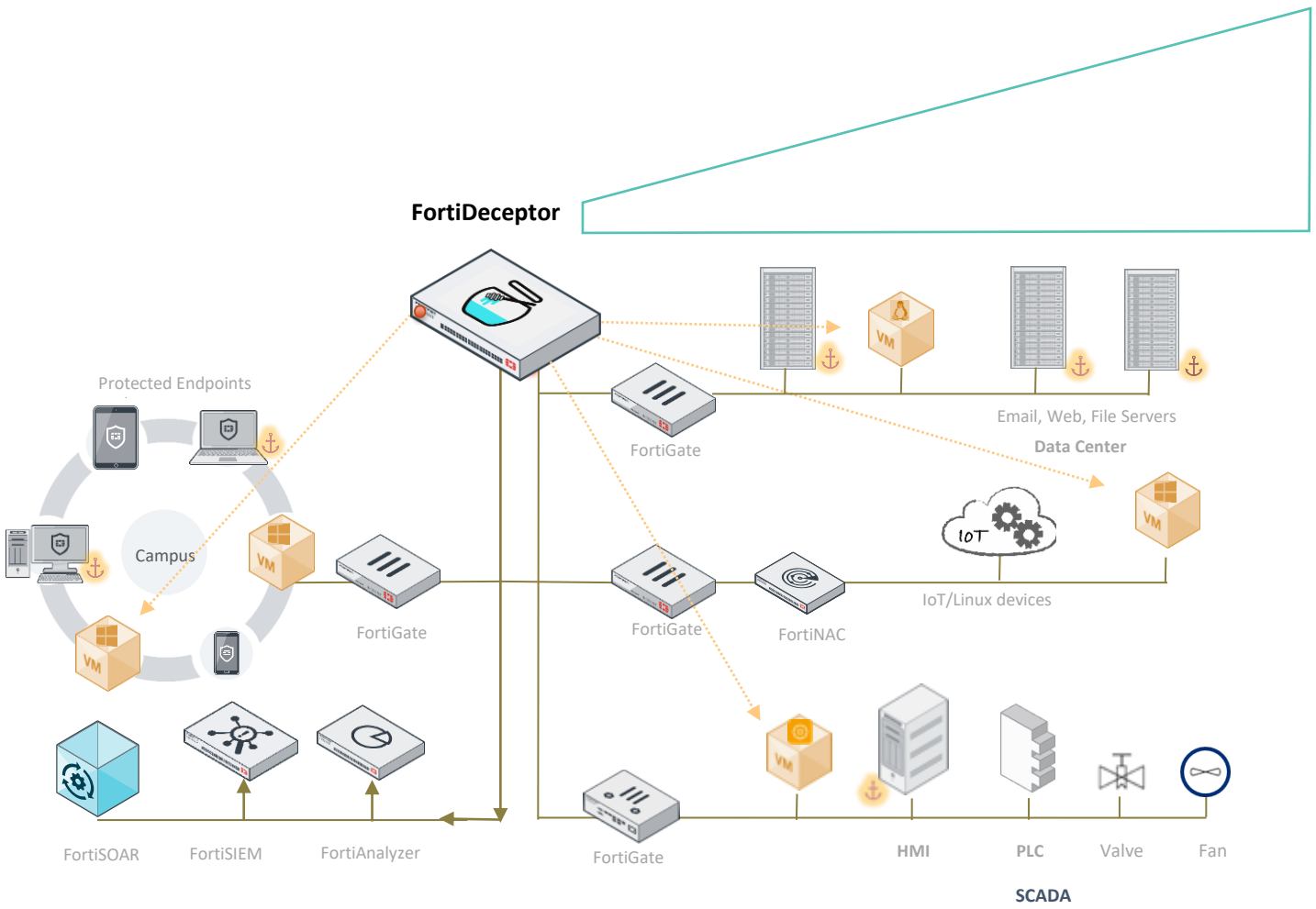
FortiDeceptor

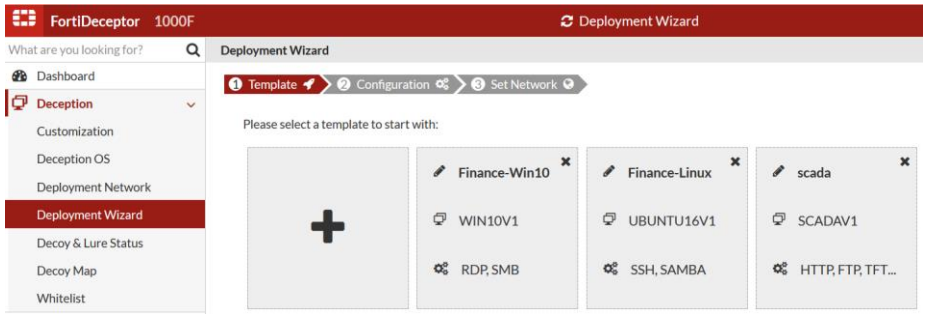
Rozwiązanie

Zaawansowany system FortiDeceptor zaprojektowany aby WYŁAPYWAĆ, UJAWNIAĆ i ELIMINOWAĆ zewnętrzne i wewnętrzne zagrożenia w początkowym kroku w łańcuchu ataku oraz proaktywnie blokować te zagrożenia zanim wyrządzą znaczne szkody.



FortiDeceptor: Cykl Życia



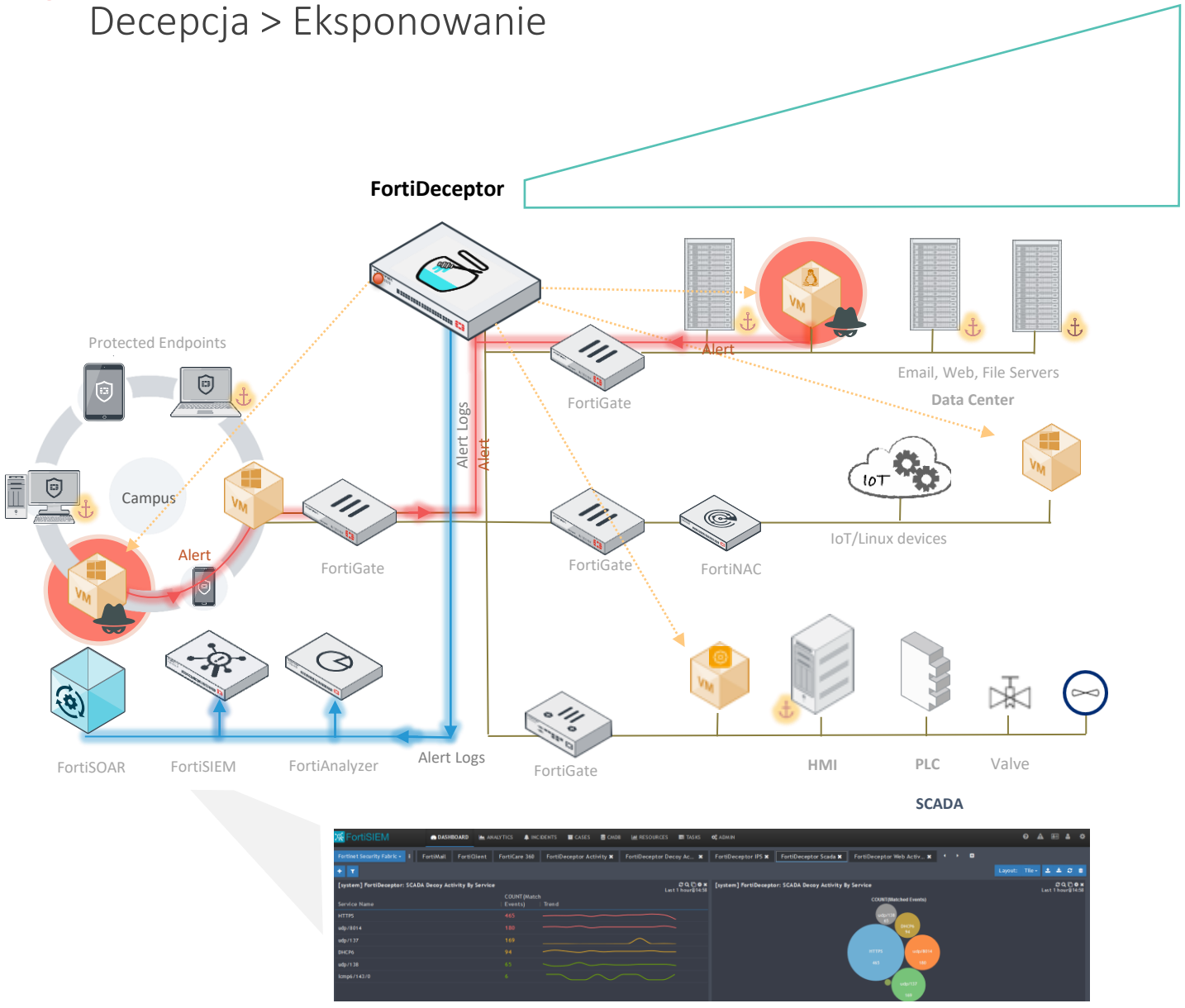


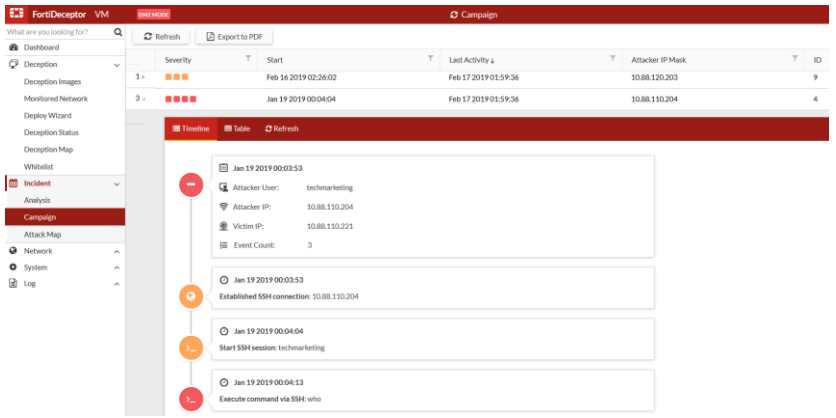
- Używa wabików na atakujących, które są niemożliwe do odróżnienia od prawdziwych zasobów IT oraz OT oraz umożliwiają wchodzenie z nimi w interakcję.
- Centralnie zarządzanie i zautomatyzowane uruchamianie wabików VM (Windows, Linux, ICS/SCADA) oraz generowanie przynęt (data, application /services*)

Przynęty OT: MODBUS, S7-200, IPMI, Bacnet, Triconex, Guardian-AST, IEC104, ENIP
Przynęty IoT: Medical PACS, DICOM, infusion pump, ERP, POS, GIT
Przynęty IT: SSL VPN, RDP, SMB, SQL, SSH, SAMBA, etc

FortiDeceptor: Cykl Życia

Decepcja > Eksponowanie

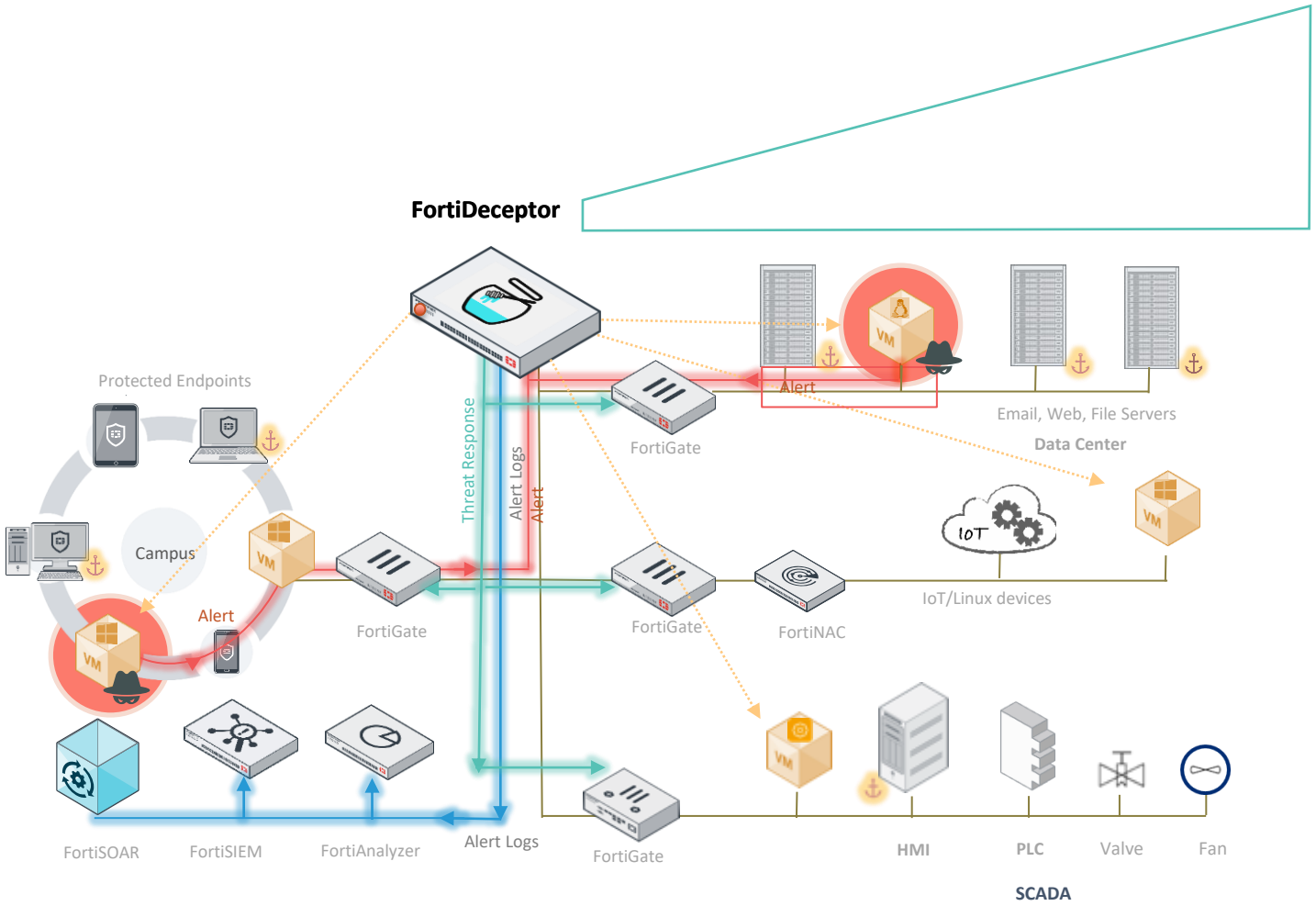


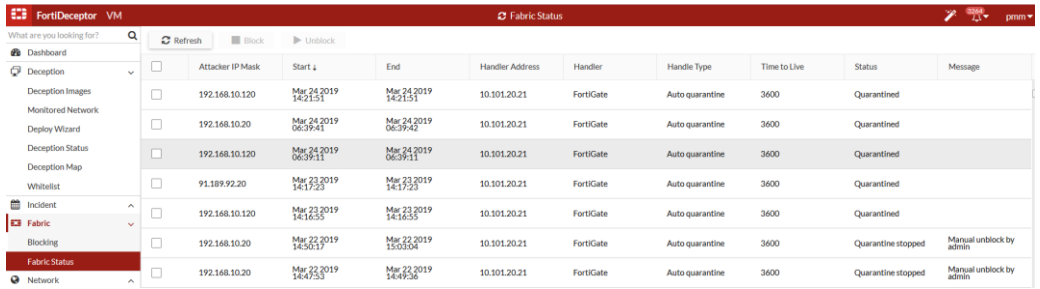


- Zachowuje się jak system wczesnego ostrzegania i generuje alerty pozwalające na dalszą analizę i podjęcie działań
- Konsoliduje wykrywanie i koreluje zewnętrzne i wewnętrzne podejrzane aktywności w jeden widok (single pain of glass)

FortiDeceptor: Cykl Życia

Decepcja > Eksponowanie > Eliminacja





- Manualne/Automatyczne blokowanie ataków oparte na wadze zagrożenia (severity-based) zanim nastąpią uszkodzenia.
- Integracja z Security Fabric
  - FortiGate: Kwarantanna adresu IP
  - FortiNAC: Izolacja Urządzeń
  - FortiSOAR: Uruchamianie Playbooków
  - FortiSIEM: Widoczność
  - Integracja z Systemami Trzecimi

FortiDeceptor: przykłady użycia

Wczesne wykrywanie w sieciach IT

Wykrywa atak na pierwszym etapie Kill Chain namierzając krytyczne zasoby IT

Uruchamia fałszywe zasoby IT

Zautomatyzowana odpowiedź

Integracja z Security Fabric pozwalająca na natychmiastową reakcję

FortiGate, FortiNAC, FortiSOAR, 3rd-party

Współpracuje z Purdue aby chronić zasoby OT

Wykrywa i odpowiada na ataki celowane w zasoby OT/IoT.

Uruchamia fałszywe zasoby OT

Wzbogacona odpowiedź na incydenty

Integracja z Security Fabric pozwala uwidocznić zdarzenia i zagrożenia

FortiSIEM, FortiAnalyzer, 3rd-party

FortiDeceptor: analiza zagrożeń

IT Solution FACTOR ENGAGE FORTINET EXPERT PARTNER

SECURED BY FORTIGUARD®

Podsumowanie

Deception-enabled Fabric

Obszerny

Sieć pułapek uruchomiona w segmentach IT oraz OT w celu ujawnienia ataków

Zintegrowany

Analityka i wykrywanie oparte na sztucznej inteligencji pełni funkcję wczesnego ostrzeżenia przed nachodzącą kampanią zagrożeń

Zautomatyzowany

Odpowiada na ataki przez integrację z systemami bezpieczeństwa in-line zanim nastąpią szkody niemożliwe do naprawienia

IT Solution FACTOR

ENGAGE

FORTINET EXPERT PARTNER

Demo

IT Solution FACTOR ENGAGE
FORTINET EXPERT PARTNER

Live: https://fortideceptor.fortidemo.com/ (demo/demo123)

Filmy:

1. **Deploy FortiDeceptor's Linux Decoy & Incident View:**
https://video.fortinet.com/products/fortideceptor/3.0/deploy-linux-decoy-incident-view

2. **FortiDeceptor ARAE & Fabric Integration in Action:**
https://video.fortinet.com/products/fortideceptor/3.0/fortideceptor-arae-fabric-integration-in-action

3. **FortiDeceptor SCADA Decoy Demonstration:**
https://video.fortinet.com/products/fortideceptor/3.0/fortideceptor-scada-decoy-demonstration

4. **FortiDeceptor integration with FortiNAC to Isolate end-device:**
https://www.youtube.com/watch?v=SfiEL7-F5Mo&t=128s

5. **FortiDeceptor integration with FortiSIEM for Incident Investigation and Response:**
https://www.youtube.com/watch?v=lVnjPiA4XzA

FORTINET®

IT Solution FACTOR

Zeskanuj kod QR

weź udział w quizie i zdobądź

szansę na wygranie atrakcyjnych nagród!

Dziękuję za uwagę

Andrzej Bajcar

Solutions Architect

andrzej.bajcar@itsf.com.pl

+48 886 648 727

IT Solution Factor

IT Solution Factor Sp. z o.o.
ul. Popularna 4/6
02-473 Warszawa
itsf.com.pl