Modern Threat Hunter Weapon

THOMAS HOFFMANN
CEO, MANAGING DIRECTOR SALES
& MARKETING

Radar Cyber Security

Who we are

2011
Year of Foundation

180
Employees

170
Countries with Customer Operations

5
Locations
Vienna (HQ), Munich, Frankfurt, Cosenza, Vaduz

2
Cyber Defense Centers
Vienna (HQ) & Vaduz

Our core competence is the early detection of IT security risks for corporations and public authorities.

”We use Radar Cyber Security‘s Managed Services to protect ourselves with the most modern tools against cyber threats. In addition to ongoing analyses of all assets in our networks, regular meetings with Radar Cyber Security‘s experts help us to assess the current situation and quickly take action when necessary.“

Adrian Baginski, BSc (WU) MSc
Data Security Manager with card complete Service Bank AG

Our Customers

An extract of our references

BY INDUSTRIES:

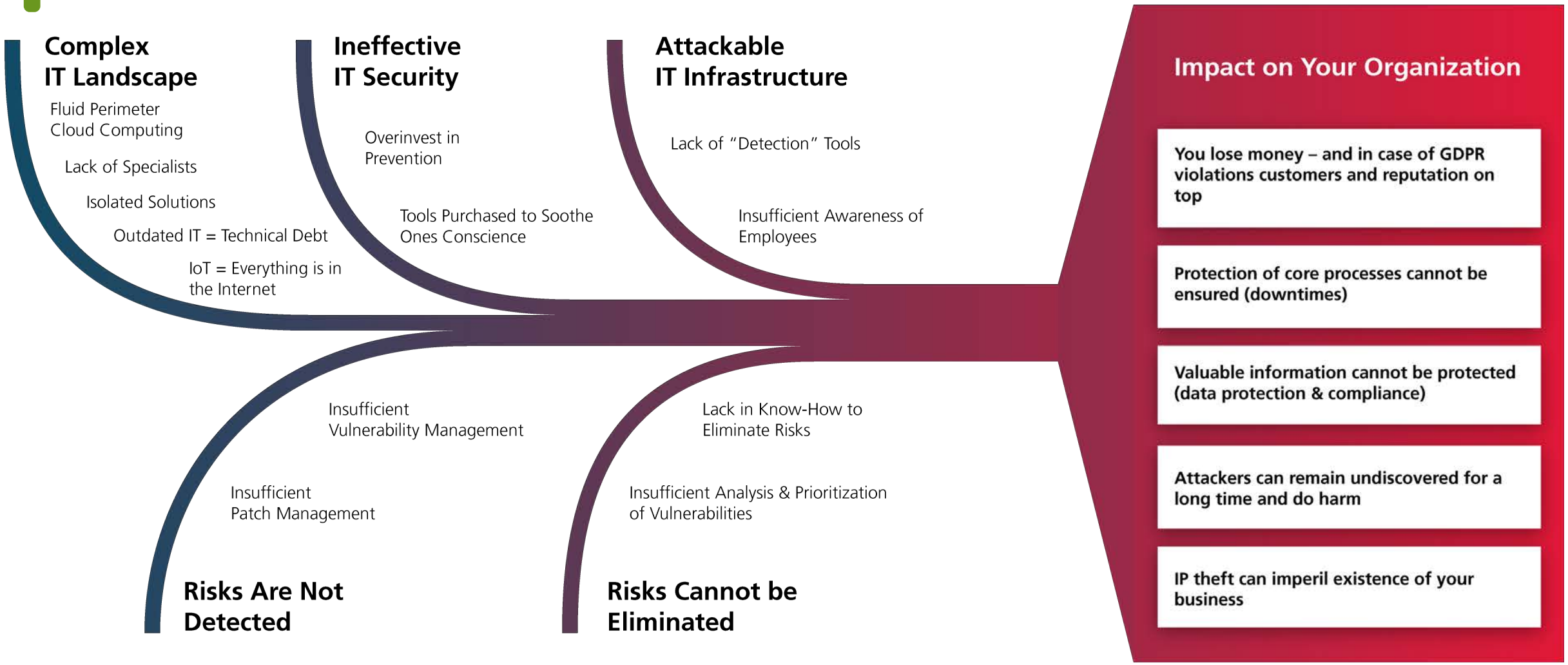
- 21% Manufact. Industry
- 16% Finance
- 16% CRITIS Companies
- 14% Commercial
- 14% Public Sector

WE PROCESS:

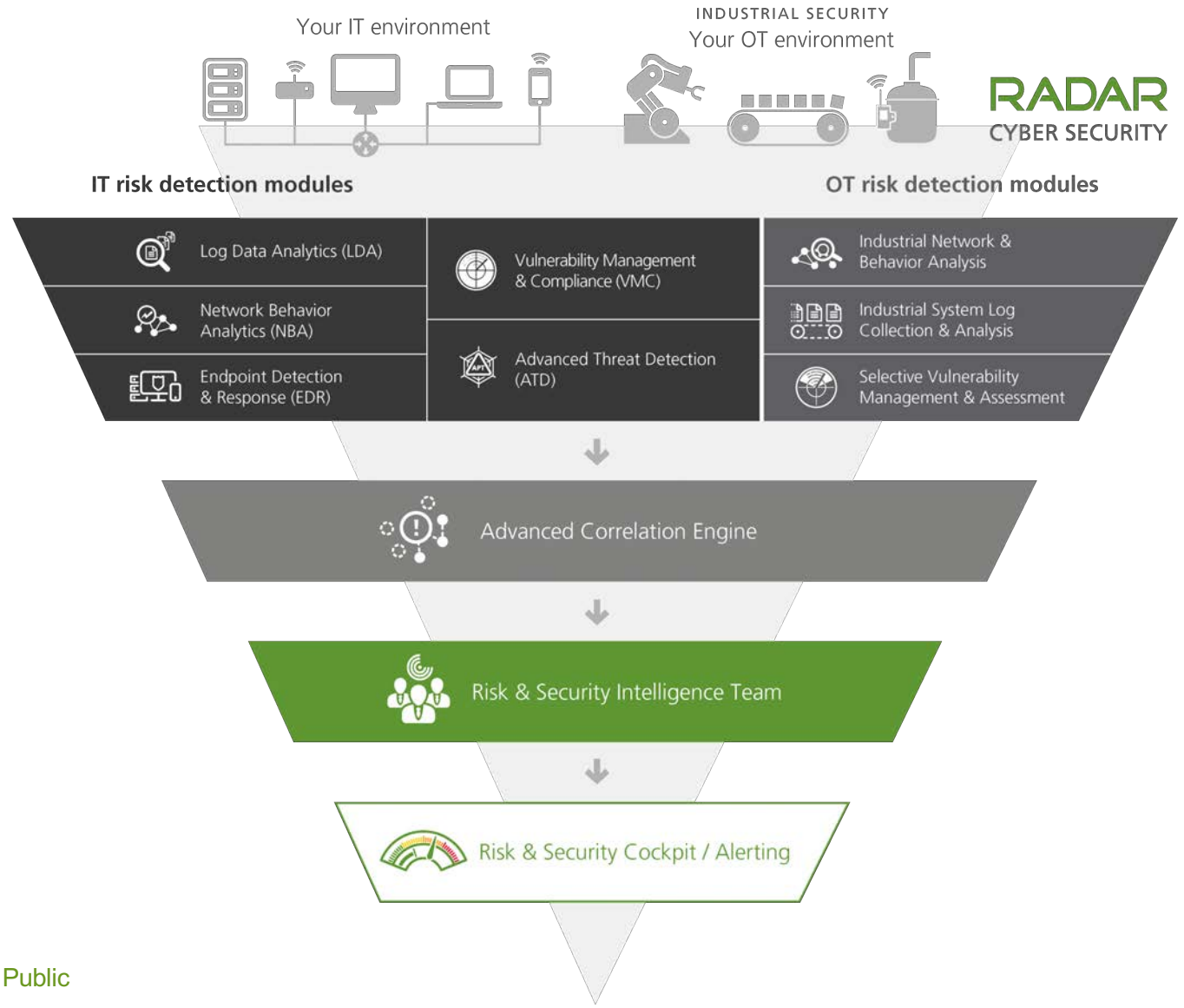
- 933 Petabyte of Data
- 99 Trillion Events
- 1,2 Billion Vulnerability Information
- 4,2 Million Incidents

Challenges in IT Departments

And Its Impact



Our System



RADAR CYBER SECURITY

RADAR CYBER SECURITY

Safeguard your digital journey.

Thank You

ISO 27001 CERTIFIED

FT 1000 Europe's Fastest Growing Companies 2018 statista

ECS EUROPEAN CYBER SECURITY ORGANISATION

Teilnehmer der Allianz für Cyber-Sicherheit

CYBER SECURITY EXCELLENCE AWARDS FINALIST 2017

2019 TOP 200 MSSPs

ПАНГЕО РАДАР

Оружие современного охотника за угрозами

Сергей Рублев

Директор по развитию Пангео Радар, CISSP

Что такое охота за угрозами

- РЕАГИРОВАНИЕ -

РЕАКТИВНЫЙ ПОДХОД

АЛГОРИТМЫ ВЫЯВЛЕНИЯ

ЧЕТКИЙ ПЛАН ДЕЙСТВИЙ

- ОХОТА -

ПРОАКТИВНЫЙ ПОДХОД

ПРОВЕРКА ГИПОТЕЗ

ПАНГЕО РАДАР

Подводные камни

ХАОС В ИНФРАСТРУКТУРЕ

КАК ВЫБРАТЬ ГИПОТЕЗУ

БОЛЬШИЕ ОБЪЕМЫ ДАННЫХ

ЧТО ЯВЛЯЕТСЯ «НОРМАЛЬНЫМ»

ПАНГЕО РАДАР

Требования к средствам хантинга

1. РАБОТА С БОЛЬШИМИ ДАННЫМИ
2. ПОМОЩЬ В ПОСТРОЕНИИ ГИПОТЕЗ
3. ПОМОЩЬ В ВАЛИДАЦИИ ГИПОТЕЗ
4. АВТОМАТИЗАЦИЯ РУТИНЫ
5. ИНТЕГРАЦИИ (SIEM, СИСТЕМЫ УПРАВЛЕНИЯ ИНЦИДЕНТАМИ)
6. СРЕДСТВА КОЛЛАБОРАЦИИ

ПАНГЕО РАДАР

Помощь в построении гипотез

ПРИОРИТИЗАЦИЯ ПО УРОВНЮ РИСКА

- Важность актива
- Опасность обнаруженной угрозы
- Достоверность техники обнаружения

СТАТИСТИЧЕСКИЕ ДАННЫЕ

- Агрегаты
- Аномалии

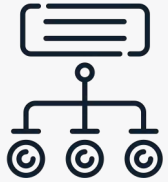
ФИЛЬТРАЦИЯ ДАННЫХ

- Схлопывание повторов
- Временной интервал
- Задействованные активы
- Источники данных
- Типы данных

Помощь в валидации гипотез

ОБОГАЩЕНИЕ

- Репутация
- Whois
- Корпоративные ресурсы



DRILL THROUG

- Выявление связанных объектов
- Добавление в рабочую среду

ИСТОРИЧЕСКИЙ КОНТЕКСТ

- Прошлые инциденты
- Заметки

СЕТЕВОЙ ГРАФ

- Отображение контекста на графе
- Выявление коммуникаций

ПАНГЕО РАДАР

Автоматизация

РЕТРОСПЕКТИВНАЯ КОРРЕЛЯЦИЯ

- Конструктор правил
- Выбор sope работы
- Запуск по расписанию

СОХРАНЕНИЕ ДАННЫХ ПО РАССЛЕДОВАНИЮ

- Конструктор инцидента
- Добавление данных в карточку по мере расследования

Workflow хантинга

THREAT INTELLIGENCE

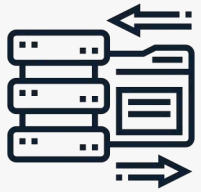
ВРЕМЕННОЕ ОКНО
SCOPE

ПОДГОТОВКА РЕЛЕВАНТНЫХ ГИПОТЕЗ

ВАЛИДАЦИЯ ГИПОТЕЗ

УПРАВЛЕНИЕ ИНЦИДЕНТАМИ

SIEM



КОРПОРАТИВНЫЕ ИСТОЧНИКИ

ПАНГЕО РАДАР

ПАНГЕО РАДАР

Доброй охоты!!!

Сергей Рублев

Директор по развитию Пангео Радар, CISSP

s.rublev@pangeoradar.ru

+7 (905) 528 74 18