
CAUTION
THIS FILE is PRINT ONLY VERSION
OF PRESENTATION

Keď sa z koristi stáva lovec...

alebo ako sa pripraviť na lov

Maroš Rajnoch, SOITRON, s.r.o., *maros@soitron.com*

SOITRON

Dôvernosť informácií:

Táto prezentácia je určená výhradne pre návštevníkov semináru

SOITRON DEFENSE 2018 (15. novembra 2018, Zochova chata)

Ako taká nesmie byť poskytovaná tretím stranám a to ani ako celok, ani žiadna jej časť. Mimo účel, na ktorý je určená nesmie byť rozmnožovaná a/alebo zasielaná mechanickou, fotochemickou alebo elektronickou cestou.

ISO 9001 LL-C (Certification) ISO 20000 LL-C (Certification) ISO 27001 LL-C (Certification) OHSAS 18001:2007 LL-C (Certification)

SOITRON

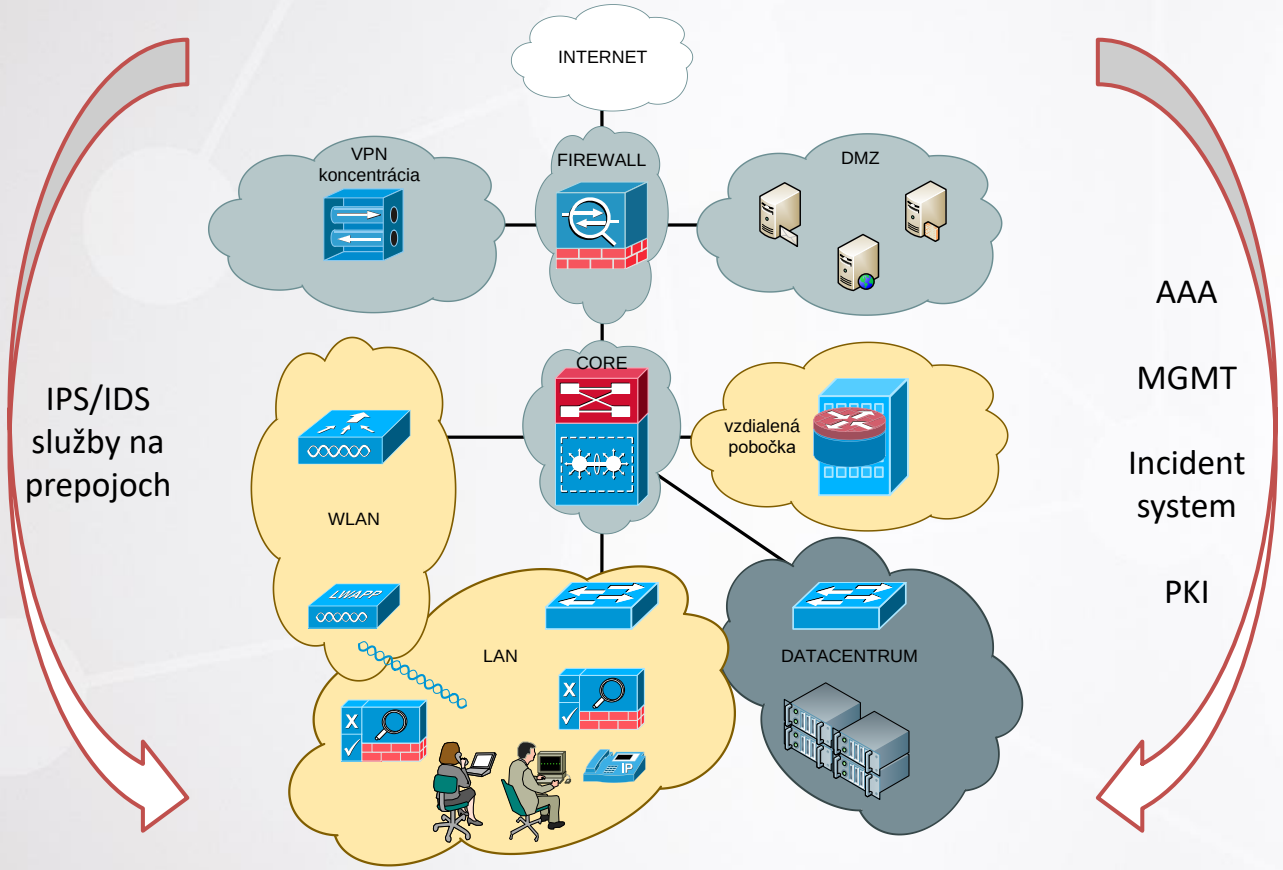
Dokument	Keď sa z koristi stáva lovec…
Podnázov	alebo ako sa pripraviť na lov
Verzia	1. X5BF27DFA
Klasifikácia	SELECTED AUDIENCE
OID	1.3.158.35955678.299039. X5BF27DFA

Vypracoval	Maroš Rajnoch
Konzultant	N/A
Preveril	N/A
Schválil	Stanislav Smolár

SOITRON

CISCO Self-Defending Networks (SDN)

is a CISCO concept of Security from ☞ **2004** ☜



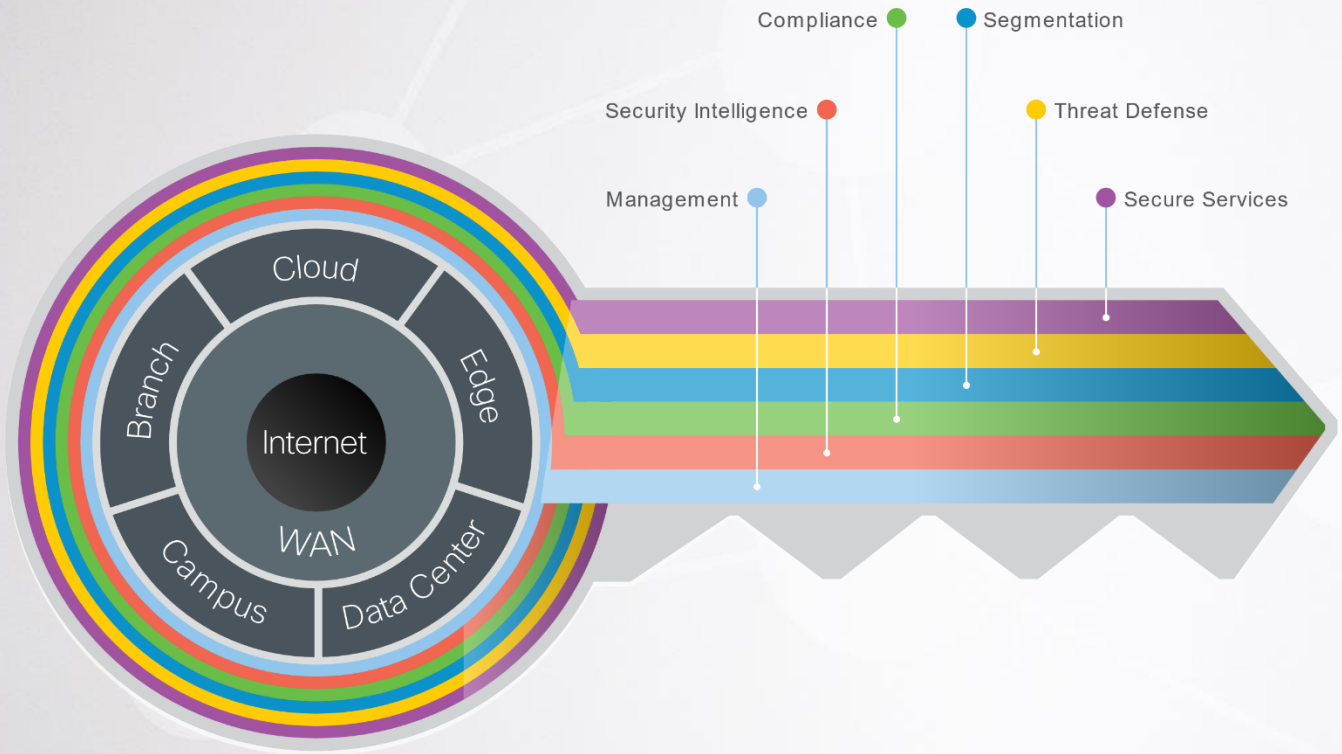
SDN uses 3 priciples:

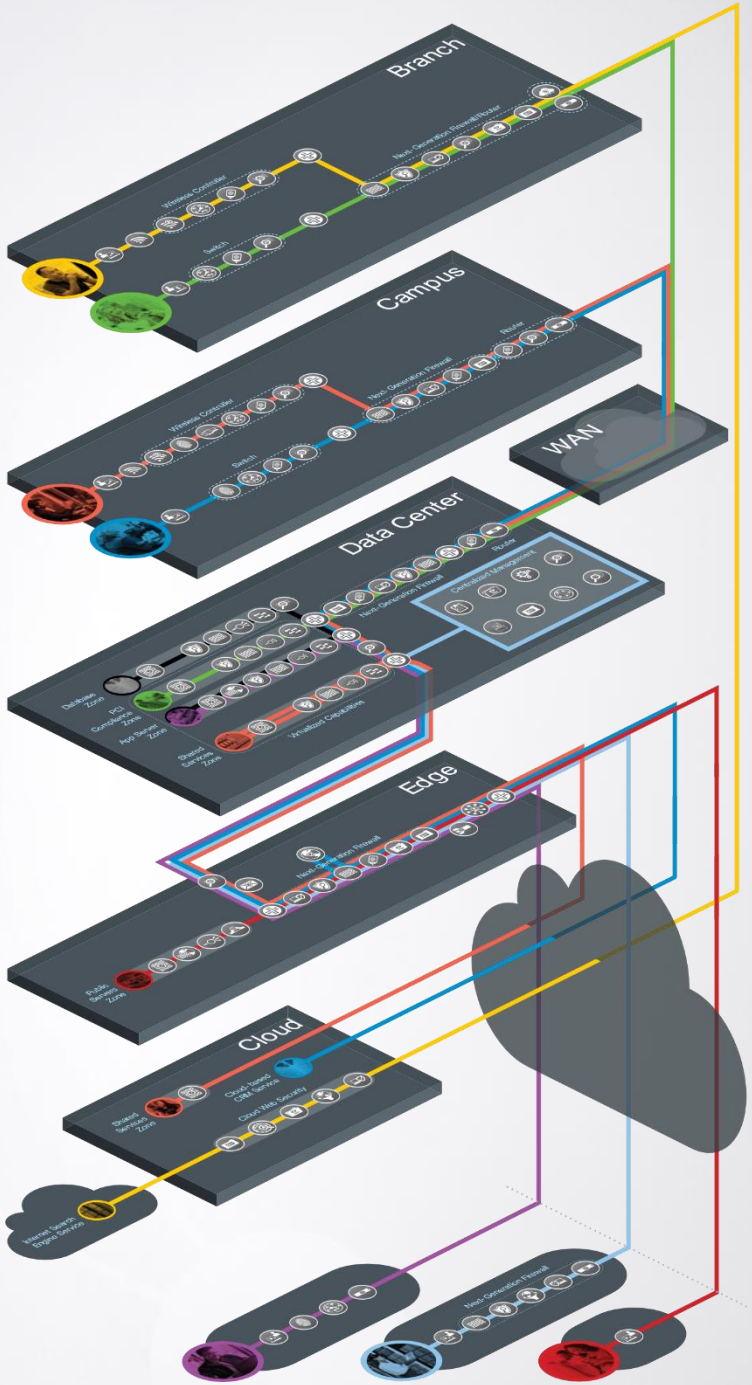
- **integration**
  every network element is a point of security

- **collaboration**
  different points of network cooperate to identify and mitigate threats

- **adaptation**
  adaptations for new threats

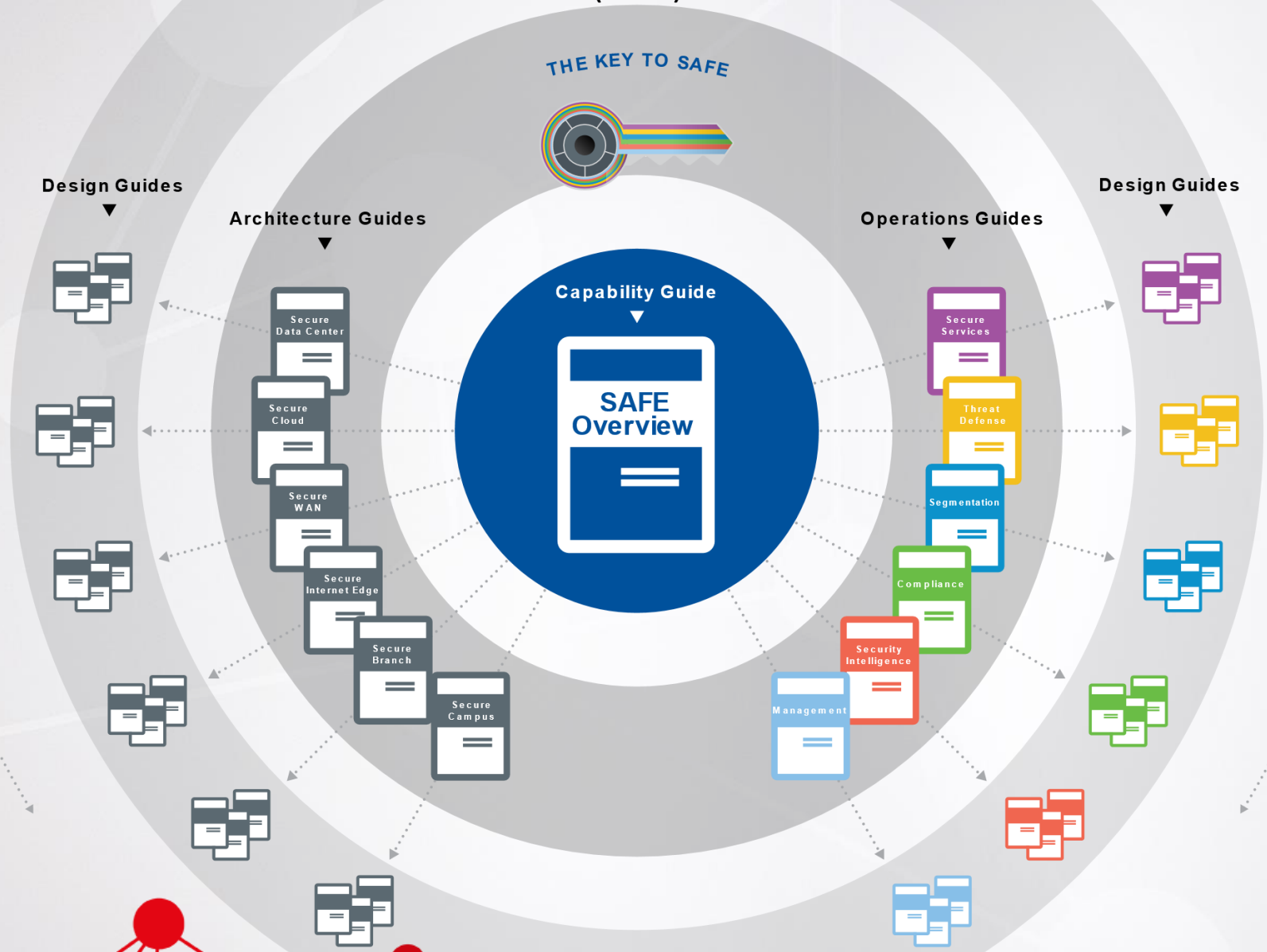
SAFE is a secure architectural framework example for business networks. Critical challenges have been deployed, tested, and validated at Cisco. These solutions provide guidance, complete with conguration steps, to ensure eective and secure deployments for our customers.





The SAFE Key organizes security by using two core concepts:
Places in the Network (PINs) and Secure Domains.

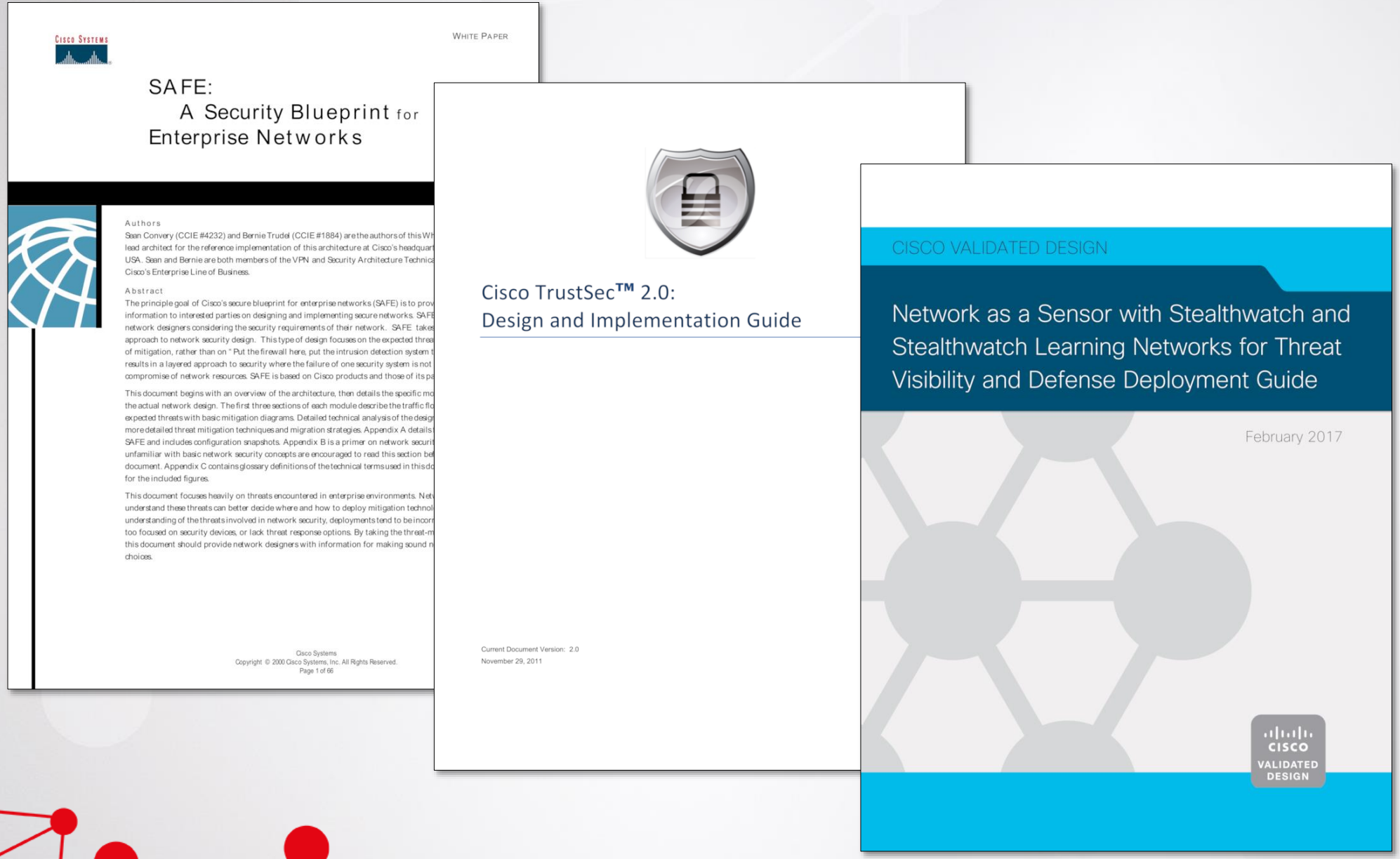
PIN:
- Data center
- Branch
- Campus
- WAN
- Internet edge
- Cloud



Secure Domains:
- Management
- Security intelligence
- Compliance
- Segmentation
- Threat defense
- Secure services

zdroj: cisco.com/go/safe

SOITRON


Cisco Systems
White Paper
SAFE:
A Security Blueprint for
Enterprise Networks
Authors
Sean Convery (CCIE #4232) and Bernie Trudel (CCIE #1884) are the authors of this Wh
lead architect for the reference implementation of this architecture at Cisco's headquart
USA. Sean and Bernie are both members of the VPN and Security Architecture Technica
Cisco's Enterprise Line of Business.
Abstract
The principle goal of Cisco's secure blueprint for enterprise networks (SAFE) is to prov
information to interested parties on designing and implementing secure networks. SAFE
network designers considering the security requirements of their network. SAFE takes
approach to network security design. This type of design focuses on the expected threa
of mitigation, rather than on " Put the firewall here, put the intrusion detection system t
results in a layered approach to security where the failure of one security system is not
compromise of network resources. SAFE is based on Cisco products and those of its pa
This document begins with an overview of the architecture, then details the specific mo
the actual network design. The first three sections of each module describe the traffic flo
expected threats with basic mitigation diagrams. Detailed technical analysis of the desig
more detailed threat mitigation techniques and migration strategies. Appendix A details
SAFE and includes configuration snapshots. Appendix B is a primer on network securit
unfamiliar with basic network security concepts are encouraged to read this section be
document. Appendix C contains glossary definitions of the technical terms used in this do
for the included figures.
This document focuses heavily on threats encountered in enterprise environments. Net
understand these threats can better decide where and how to deploy mitigation technol
understanding of the threats involved in network security, deployments tend to be incorr
too focused on security devices, or lack threat response options. By taking the threat-m
this document should provide network designers with information for making sound n
choices.
Cisco Systems
Copyright © 2000 Cisco Systems, Inc. All Rights Reserved.
Page 1 of 66
Cisco TrustSec™ 2.0:
Design and Implementation Guide
Current Document Version: 2.0
November 29, 2011
CISCO VALIDATED DESIGN
Network as a Sensor with Stealthwatch and
Stealthwatch Learning Networks for Threat
Visibility and Defense Deployment Guide
February 2017
CISCO
VALIDATED
DESIGN

SOITRON

Cisco Cyber Threat Defense v2.0

Design Guide

Last Updated: July 23, 2015

SAFE Design Guide

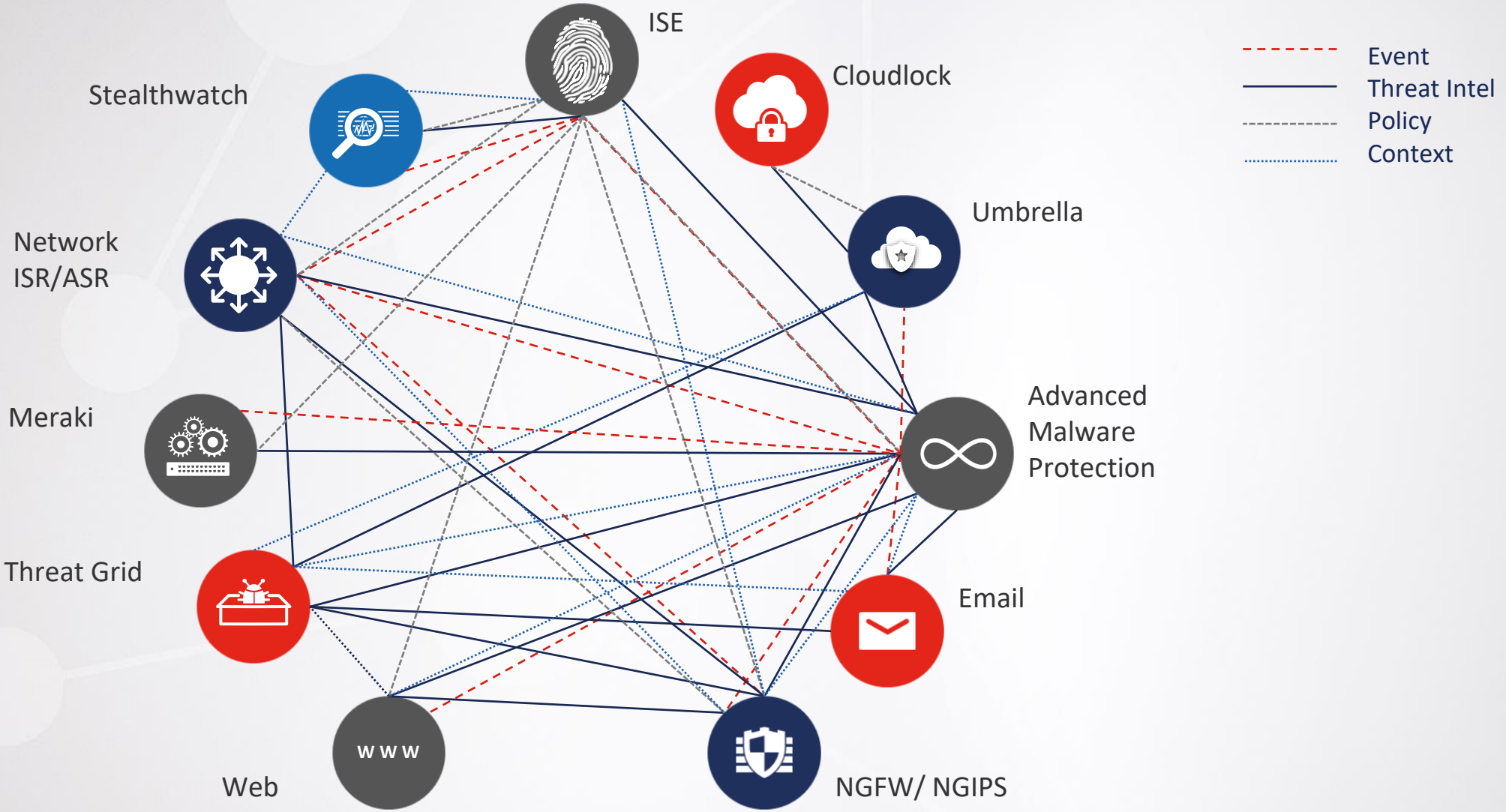
Security Domain: Threat Defense

Use Case: Cisco Ransomware Defense

Added Advanced - Updated August 2017

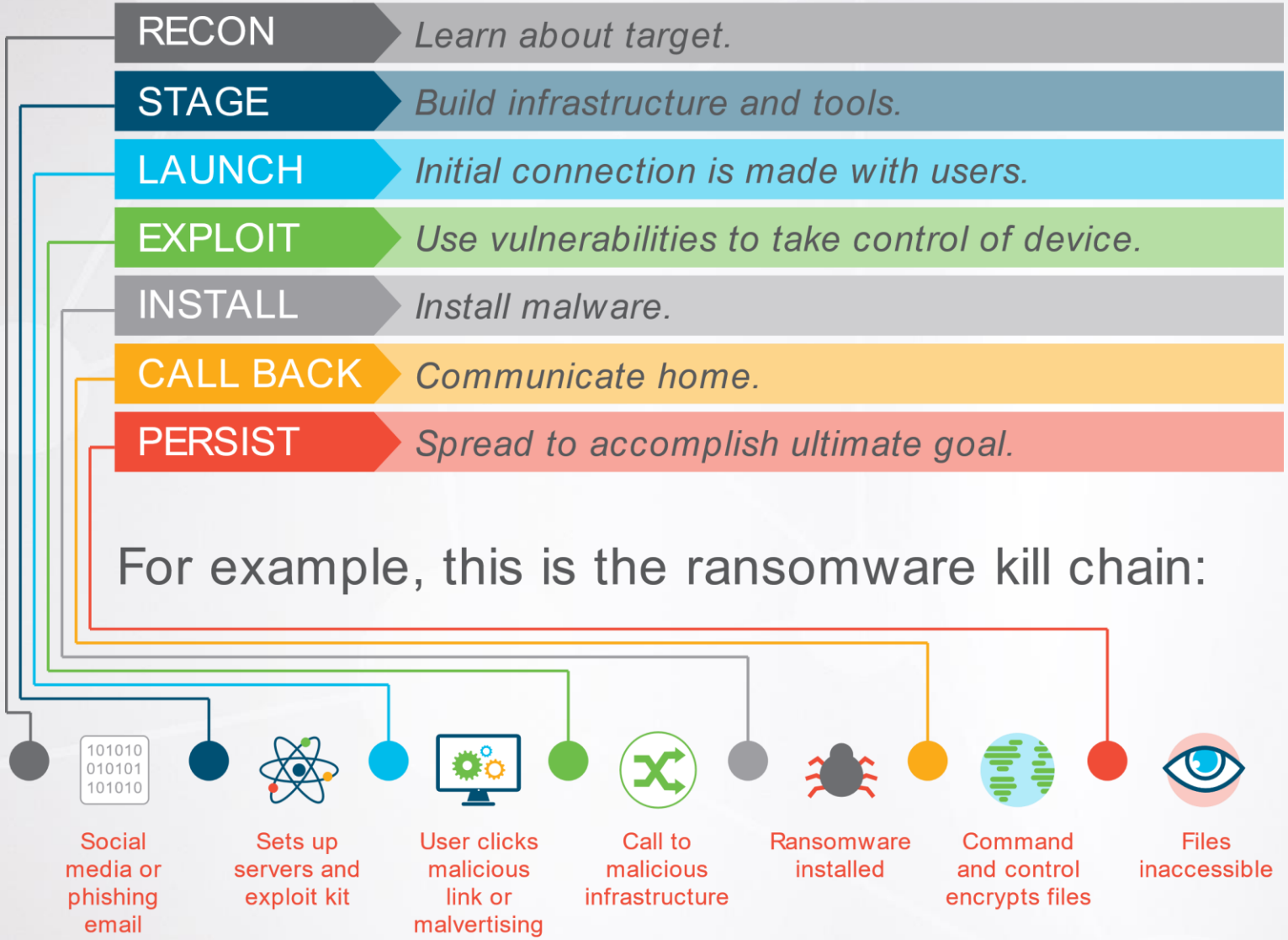
SOITRON

Summarizing Cisco Security Product Integration – **An integrated portfolio creates value for customer!**



SOITRON

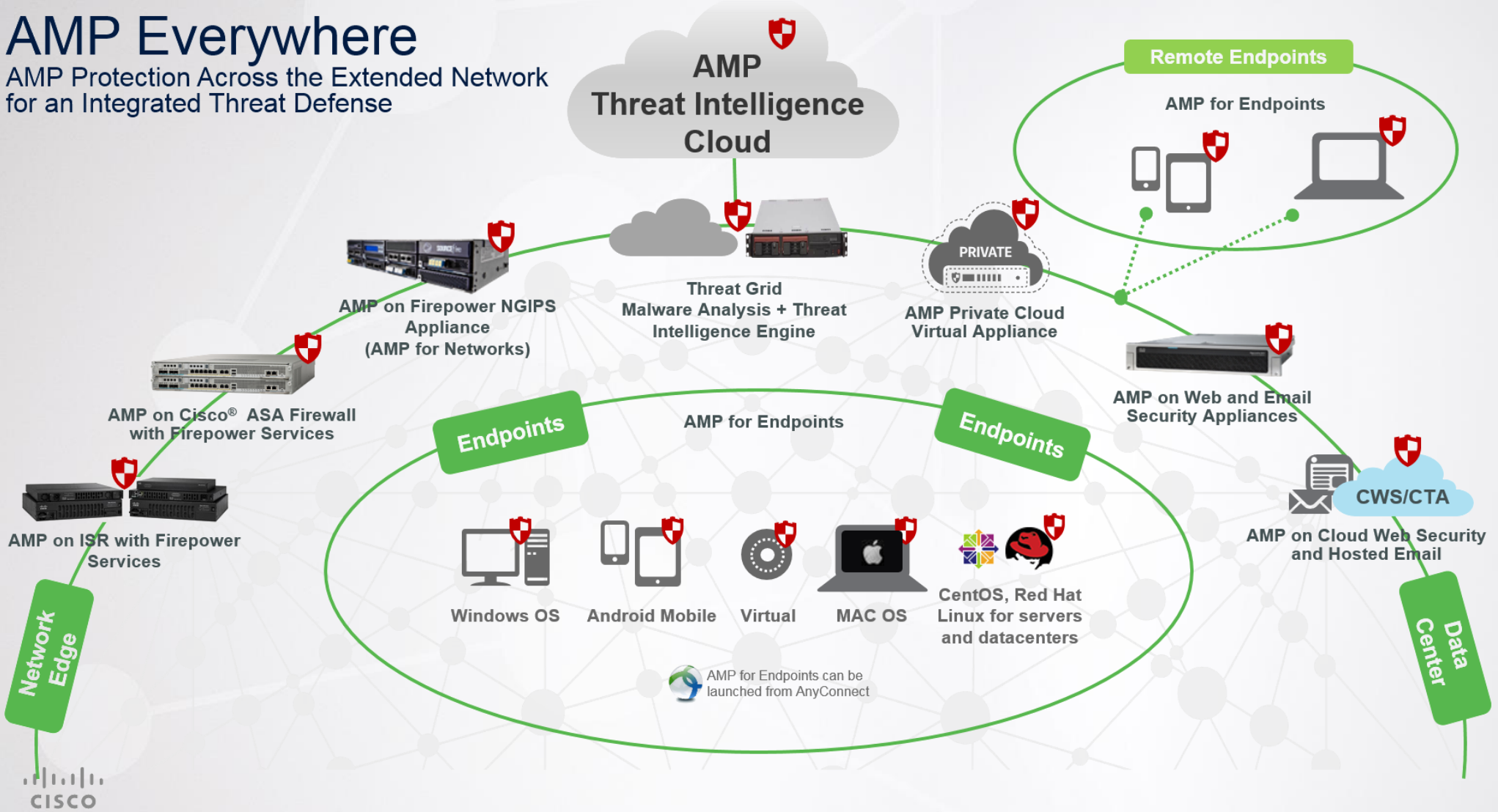
Most cyber attacks follow this general flow:



SOITRON

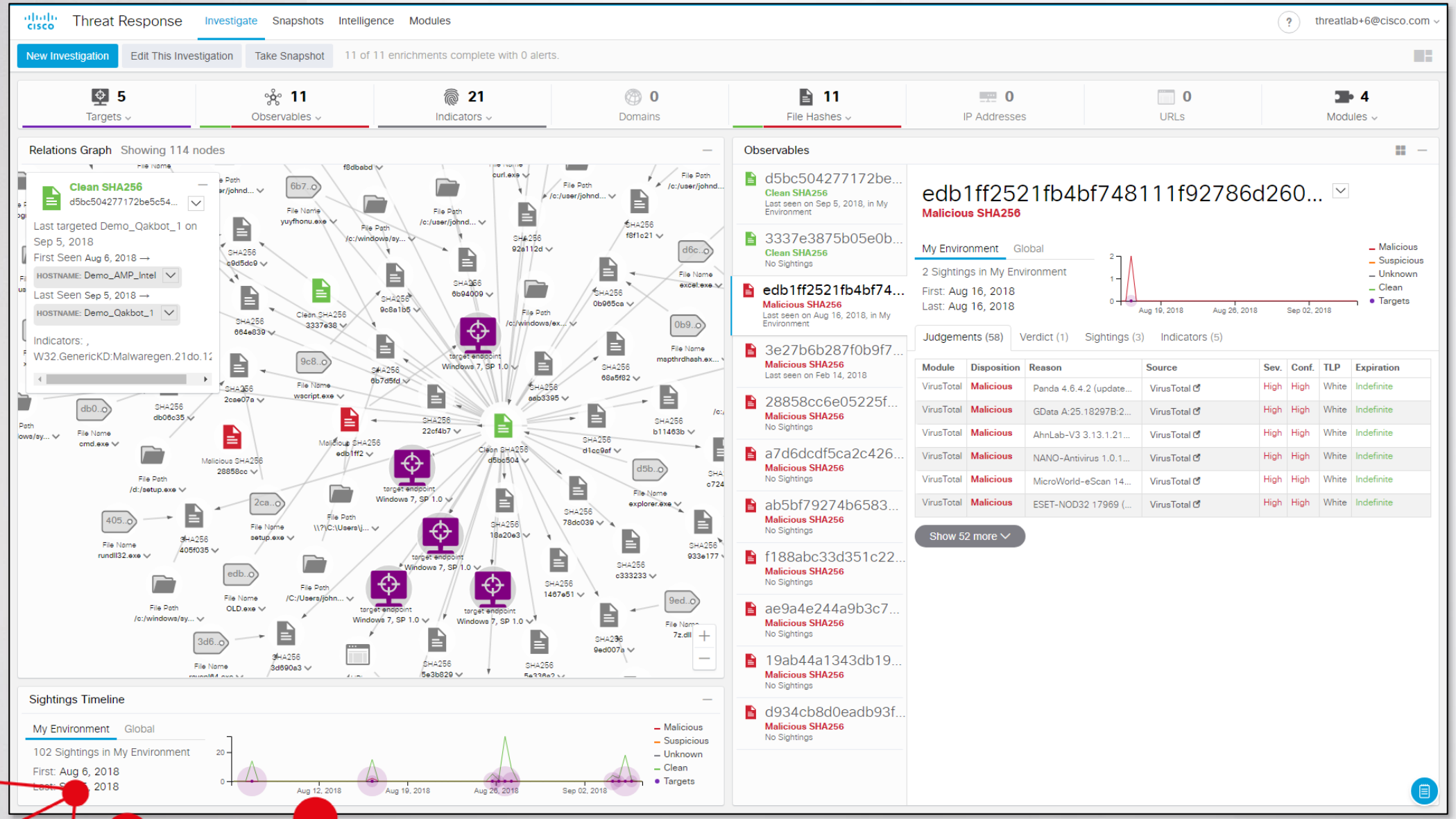
AMP Everywhere

AMP Protection Across the Extended Network for an Integrated Threat Defense



SOITRON

Cisco Threat Response – *detekcia*, *investigácia* a *remediácia* bezpečnostných incidentov



SOITRON

Cisco AMP dnes poskytuje širokú výbavu na boj s malwarom.
Je tak Vašou voľbou či sa z obete stane lovec – želám úspešný lov!

VS.

...nasleduje ukážka P. Mesjara...

SOITRON

Cyber Threat Response Lab v3.1

https://dcloud-cms.cisco.com/demo_news/cyber-threat-response-lab-v3-1

- *Scenario 1: HackMDs.com – Connectivity and Setup*
- *Scenario 2: Target Reconnaissance: Gathering Information about Vulnerabilities for a Future Attack*
- *Scenario 3: Smash and Grab: Attacking Your Public Network Services Through the Front Door*
- *Scenario 4: The Ransomware Scenario*
- *Scenario 5: Insider Threats: Moving Within to Obtain and Export Your Data*
- *Scenario 6: Compromised Hosts: Controlling Access and Monitoring for Malicious Threats*
- *Scenario 7: Centralized Defense*
- *Scenario 8: Cyber Threat Response Challenge*

SOITRON

SOITRON