MODERN CYBER DEFENSE

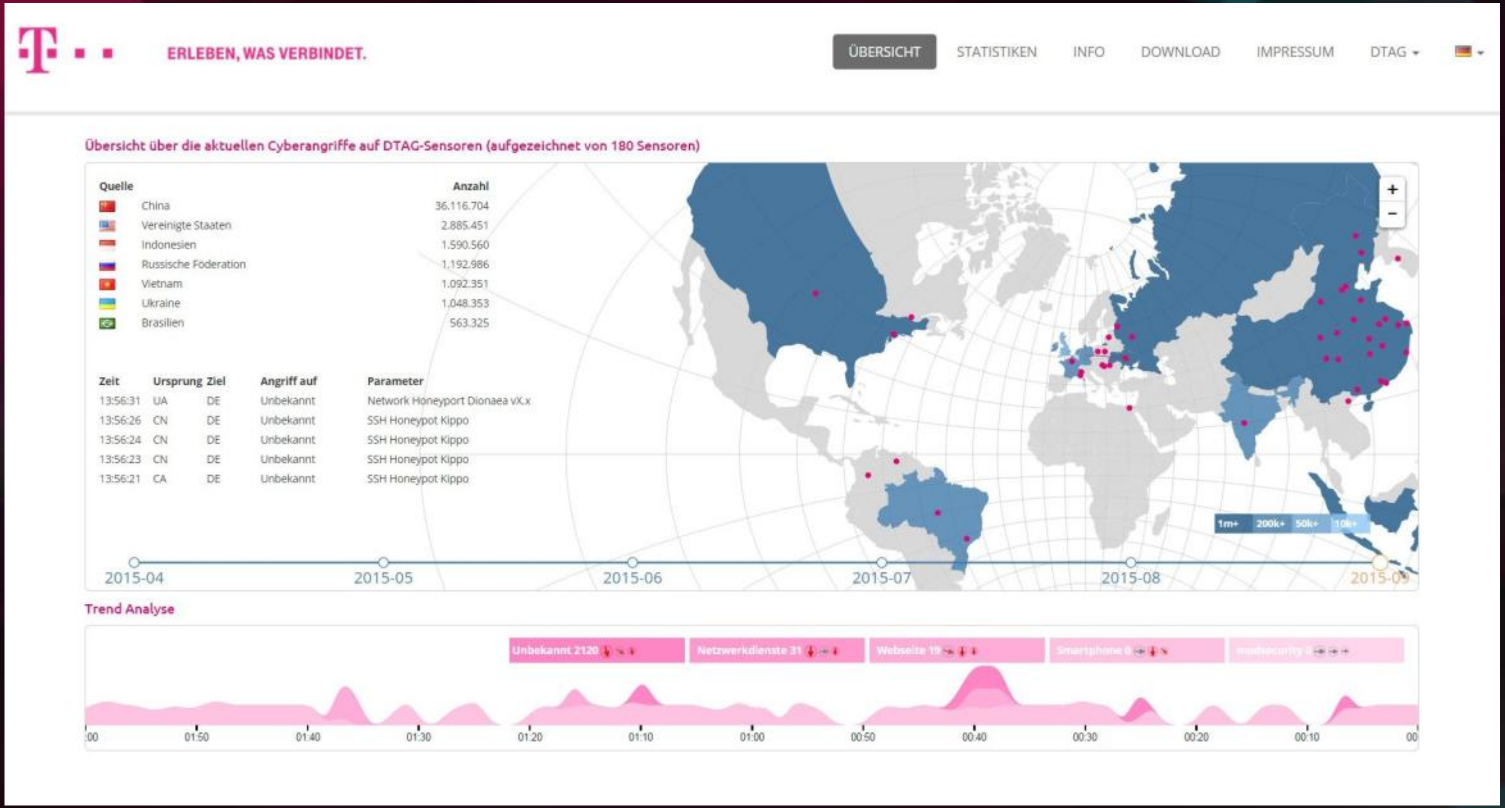
DR. RÜDIGER PEUSQUENS

VP CYBER DEFENSE RESPONSE

October 5 2017

LIFE IS FOR SHARING.

MORE THAN 4‘000‘000 CYBER ATTACKS – EVERY DAY!



Übersicht über die aktuellen Cyberangriffe auf DTAG-Sensoren (aufgezeichnet von 180 Sensoren)

Quelle		Anzahl
🇨🇳	China	36.116.704
🇺🇸	Vereinigte Staaten	2.885.451
🇮🇩	Indonesien	1.590.560
🇷🇺	Russische Föderation	1.192.986
🇻🇳	Vietnam	1.092.351
🇺🇦	Ukraine	1.048.353
🇧🇷	Brasilien	563.325

Zeit	Ursprung	Ziel	Angriff auf	Parameter
13:56:31	UA	DE	Unbekannt	Network Honeyport Dionaea vX.x
13:56:26	CN	DE	Unbekannt	SSH Honeypot Kippo
13:56:24	CN	DE	Unbekannt	SSH Honeypot Kippo
13:56:23	CN	DE	Unbekannt	SSH Honeypot Kippo
13:56:21	CA	DE	Unbekannt	SSH Honeypot Kippo

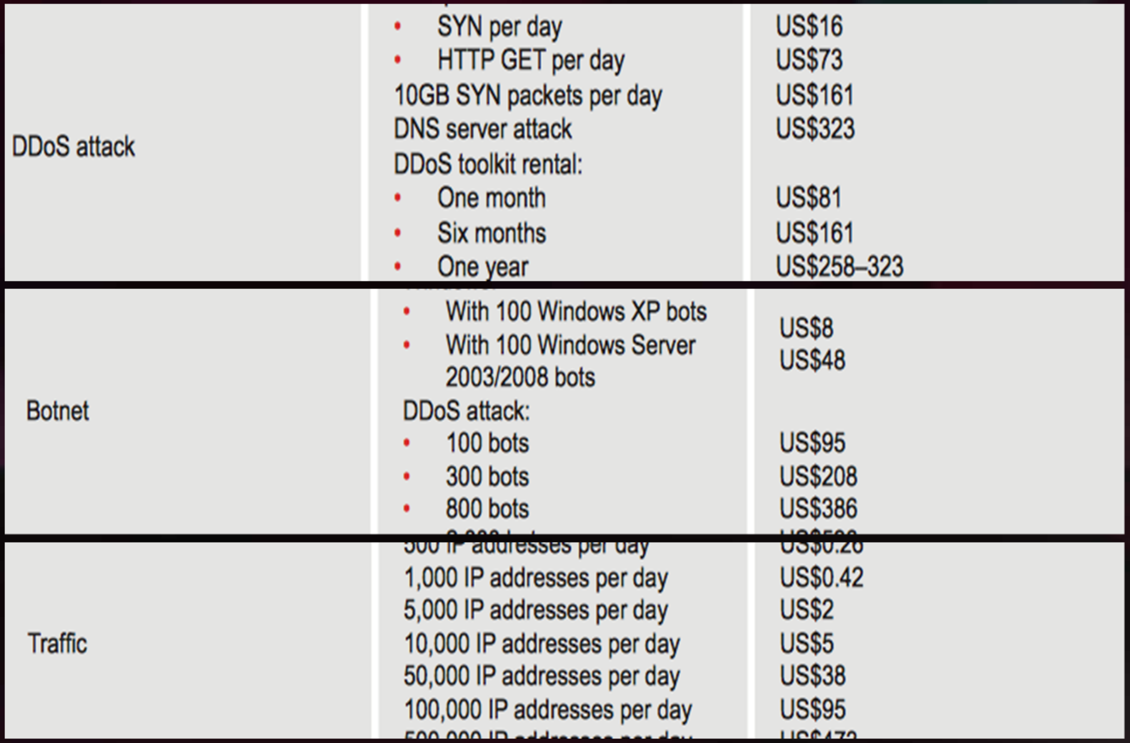
Trend Analyse

sicherheitstacho.eu

LIFE IS FOR SHARING.

BOTNET BUSINESS CASE: CYBER-BLACKMAIL

BOT-NETS
&
DENIAL OF SERVICE
ATTACKS
AVAILABLE
ON THE DARKNET



DDoS attack	• SYN per day • HTTP GET per day 10GB SYN packets per day DNS server attack DDoS toolkit rental: • One month • Six months • One year	US$16 US$73 US$161 US$323 US$81 US$161 US$258–323
Botnet	• With 100 Windows XP bots • With 100 Windows Server 2003/2008 bots DDoS attack: • 100 bots • 300 bots • 800 bots	US$8 US$48 US$95 US$208 US$386
Traffic	500 IP addresses per day 1,000 IP addresses per day 5,000 IP addresses per day 10,000 IP addresses per day 50,000 IP addresses per day 100,000 IP addresses per day 500,000 IP addresses per day	US$0.26 US$0.42 US$2 US$5 US$38 US$95 US$472

LIFE IS FOR SHARING.

MIRAI BOTNET ATTACK 11/27/2016 SUCCESSFULLY STOPPED

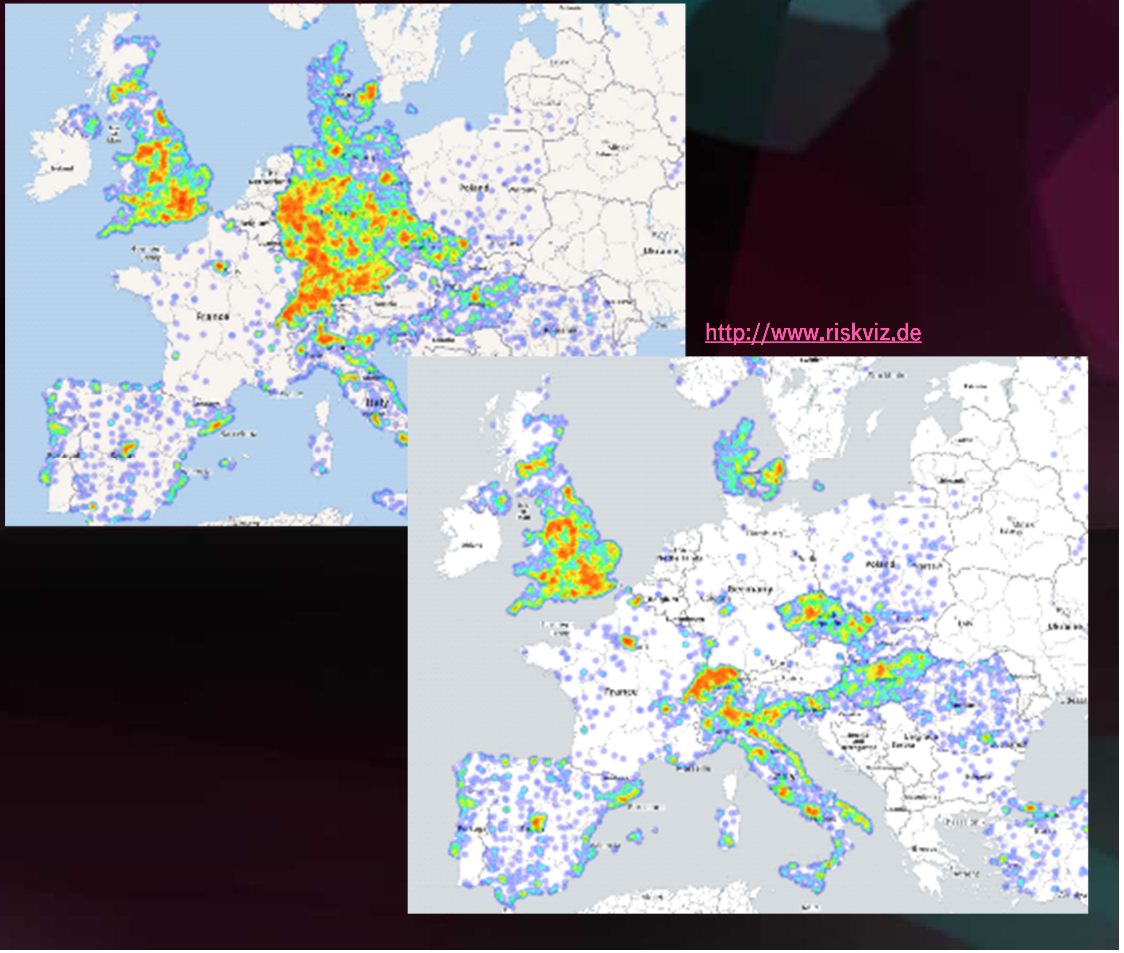
DEVICES ATTACK DEVICES

Worldwide Target:

Take control of end-user IAD / home routers

Collateral damage at Deutsche Telekom:

Internet usage down for 900‘000 customers



http://www.riskviz.de

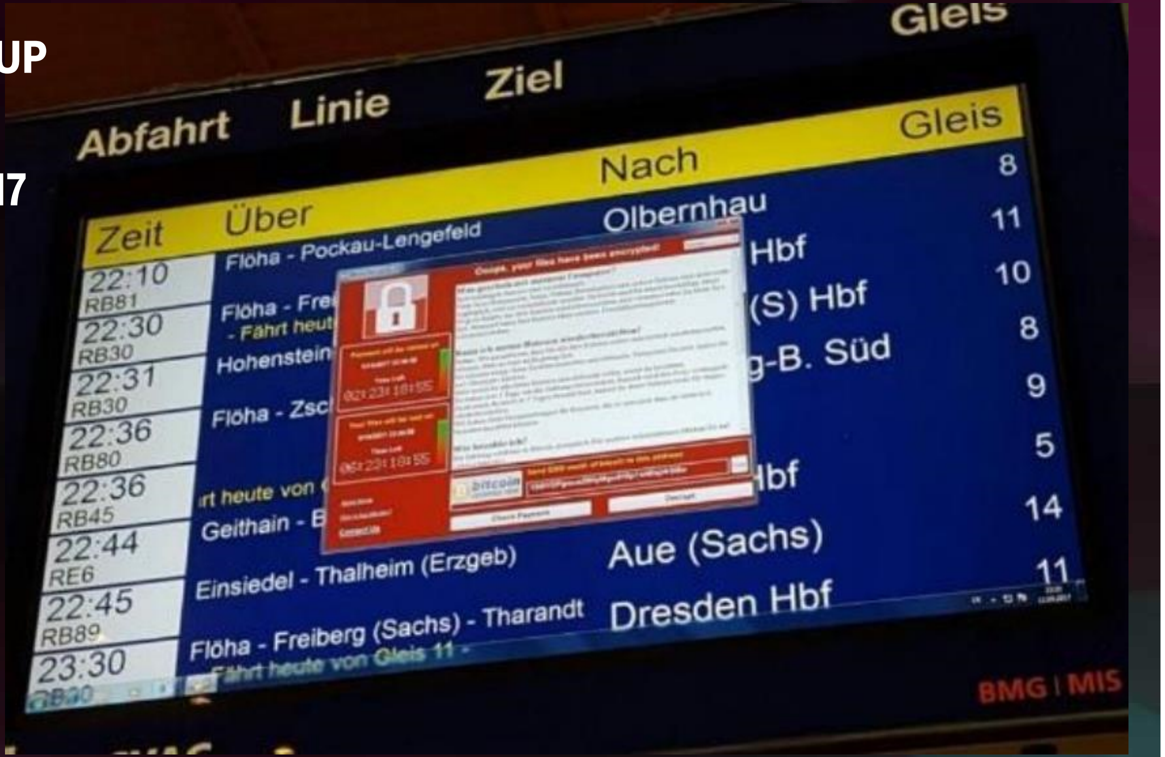
LIFE IS FOR SHARING.

WANNACRY OUTBREAK 05/12/2017

KNOWN VULNERABILITY
IN WINDOWS SMB SERVICE

KNOWN FROM NSA EQUATION GROUP
LEAK 2016

PATCH AVAILABLE SINCE 03/14/2017



TARGETS

- SERVER
- WORKSTATIONS
- PC-BASED DEVICES

LIFE IS FOR SHARING.

EVERY ORGANIZATION IS A POTENTIAL VICTIM

SONY

100 million customer data records stolen - PSN offline for one month

The New York Times

Over months, attackers accessed computers in NYT's editorial offices

ebay

Up to 145 Mio. customer data records stolen

Networks of the German Bundestag infiltrated with persistent Malware

YAHOO!

Up to 500 Mio. customer information stolen

JPMorganChase

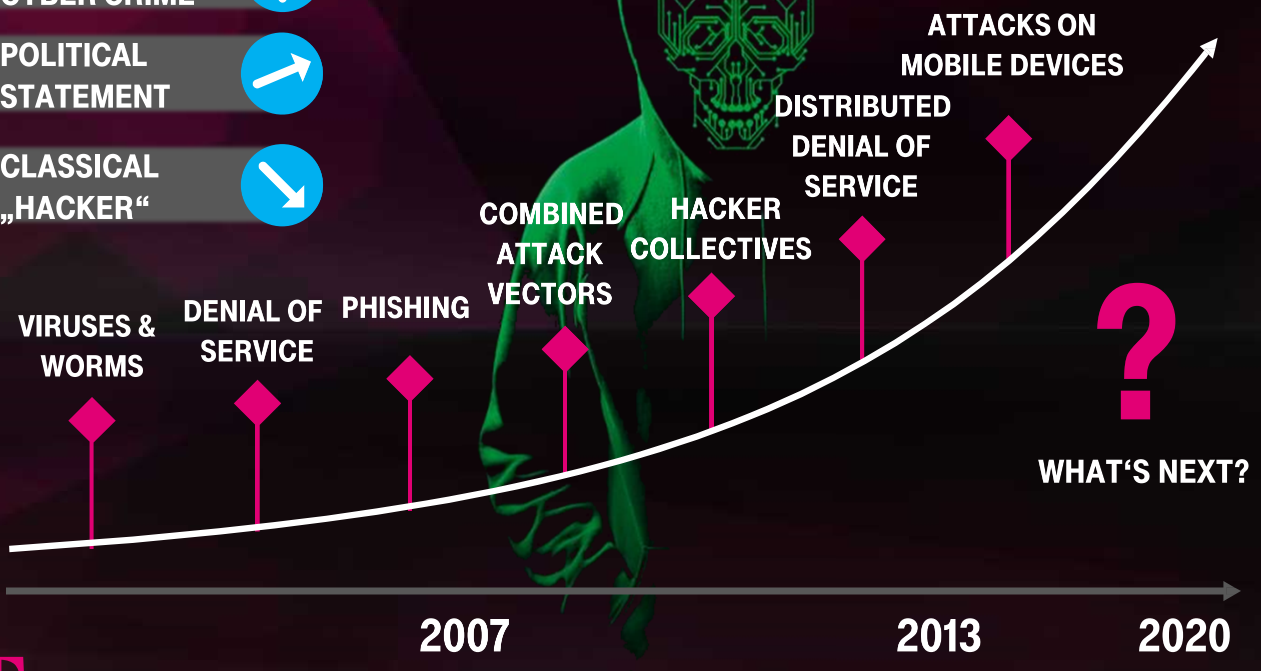
76 million customer data records stolen, attack was revealed after 2 months

HBGary DETECT DIAGNOSE RESPOND

Theft of internal & confidential customer documents (e.g. from the FBI & NSA)

ATTACKS ARE GETTING MORE PROFESSIONAL, CAUSING GREATER DAMAGE

- ORGANIZED CYBER CRIME ↑
- POLITICAL STATEMENT ↗
- CLASSICAL „HACKER“ ↘



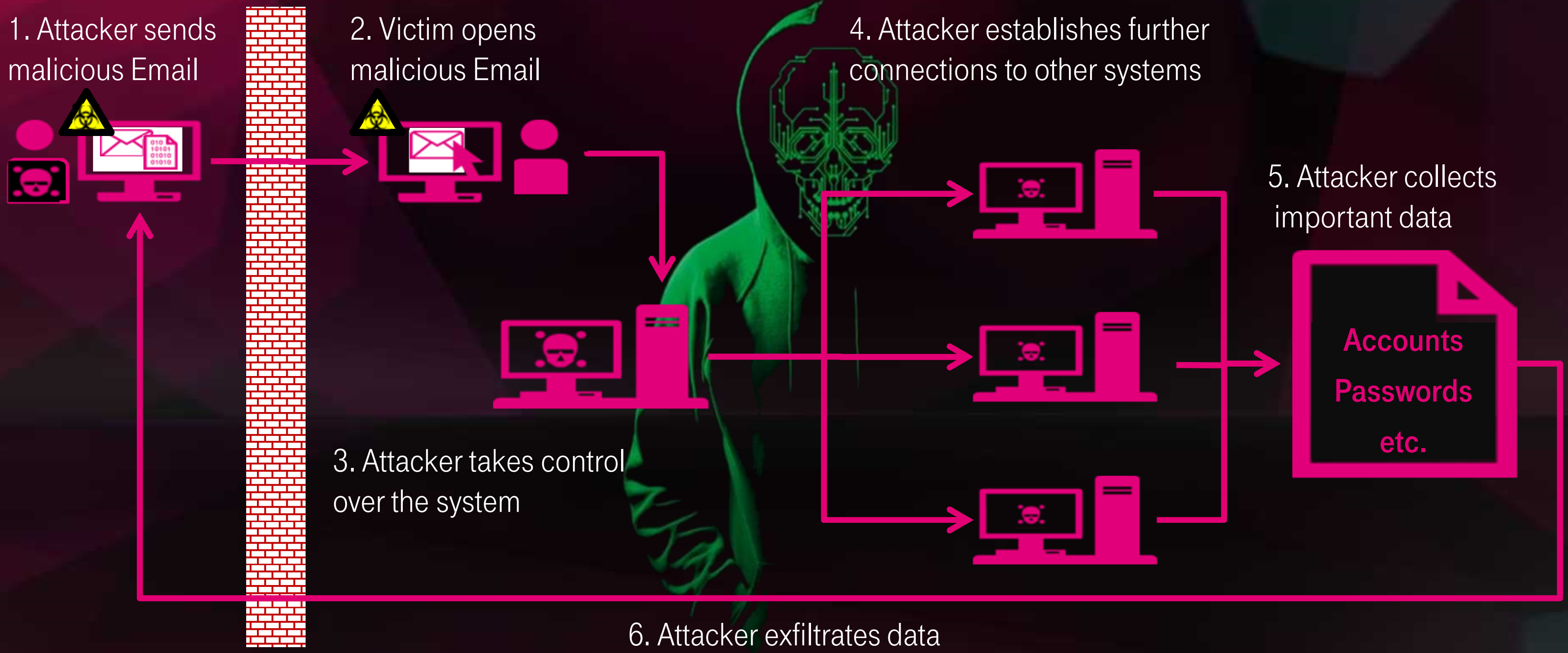
ATTACK SURFACE IS GROWING

INCREASING PROFESSIONALITY

HIGHER SEVERITY OF DAMAGE

FAST EXPLOITS

TARGETED CYBER ATTACK COME IN THROUGH THE DOOR



1. Attacker sends malicious Email

2. Victim opens malicious Email

3. Attacker takes control over the system

4. Attacker establishes further connections to other systems

5. Attacker collects important data

6. Attacker exfiltrates data

LIFE IS FOR SHARING.

THE EVOLUTION OF ATTACKS CHANGES THE RULES

“Arms race”

TARGETED ATTACKS

PERSISTENT

FLEXIBLE

UNDER THE RADAR

ASYMMETRIC

PREVENTION ?

RESILIENCE !

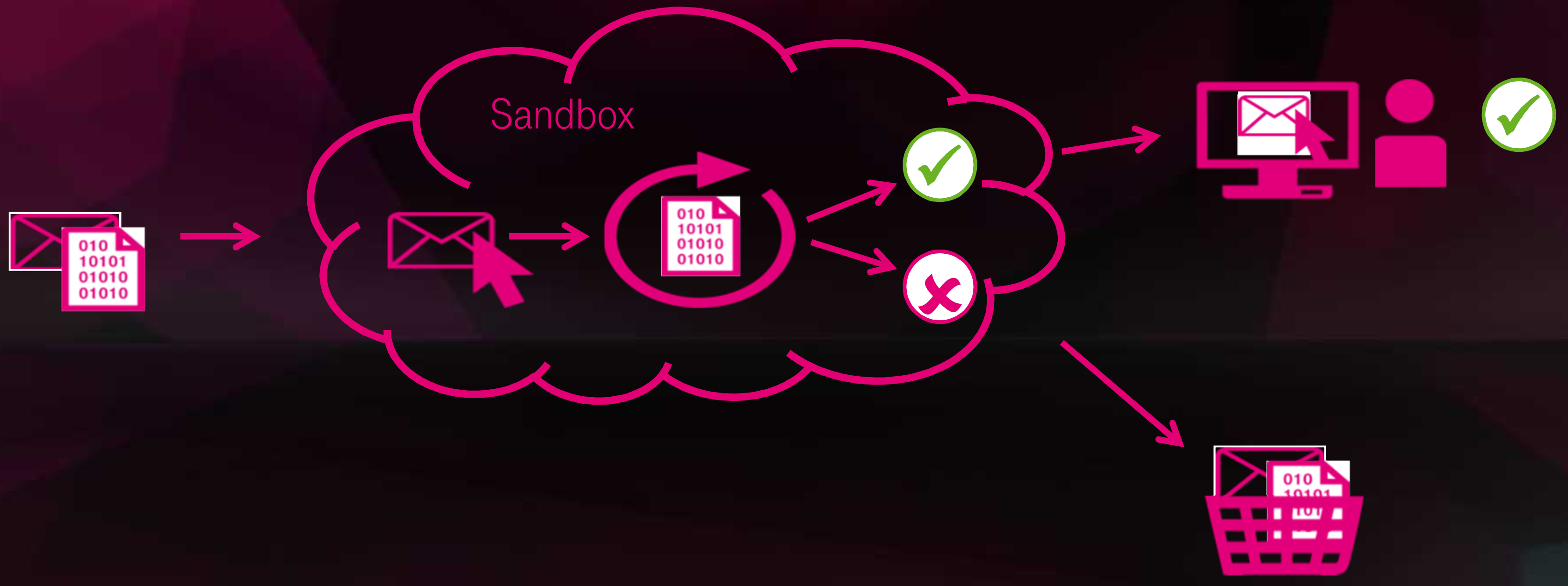
PREVENT

DETECT

RESPOND

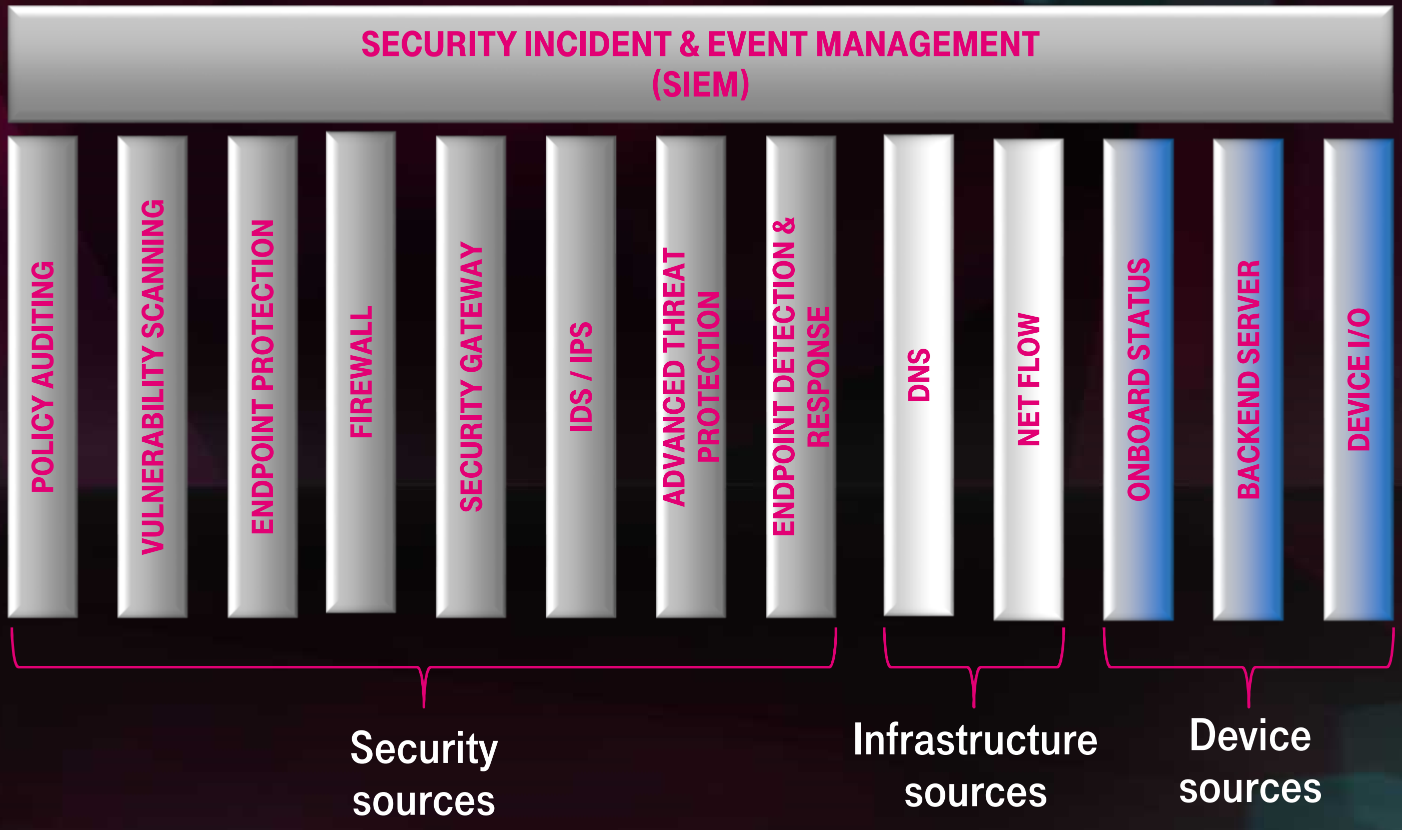
LIFE IS FOR SHARING.

EXAMPLE - EMAIL: RECOGNIZING MALICIOUS ATTACHMENTS WITHOUT OPENING THE EMAIL



CYBER DEFENSE COLLECTS MONITORING INPUT

SOURCES OF ANOMALY DETECTION ARE COLLECTED AND CORRELATED TO GENERATE PRECISE ALARMS



SECURITY INCIDENT & EVENT MANAGEMENT (SIEM)

POLICY AUDITING

VULNERABILITY SCANNING

ENDPOINT PROTECTION

FIREWALL

SECURITY GATEWAY

IDS / IPS

ADVANCED THREAT PROTECTION

ENDPOINT DETECTION & RESPONSE

DNS

NET FLOW

ONBOARD STATUS

BACKEND SERVER

DEVICE I/O

Security sources

Infrastructure sources

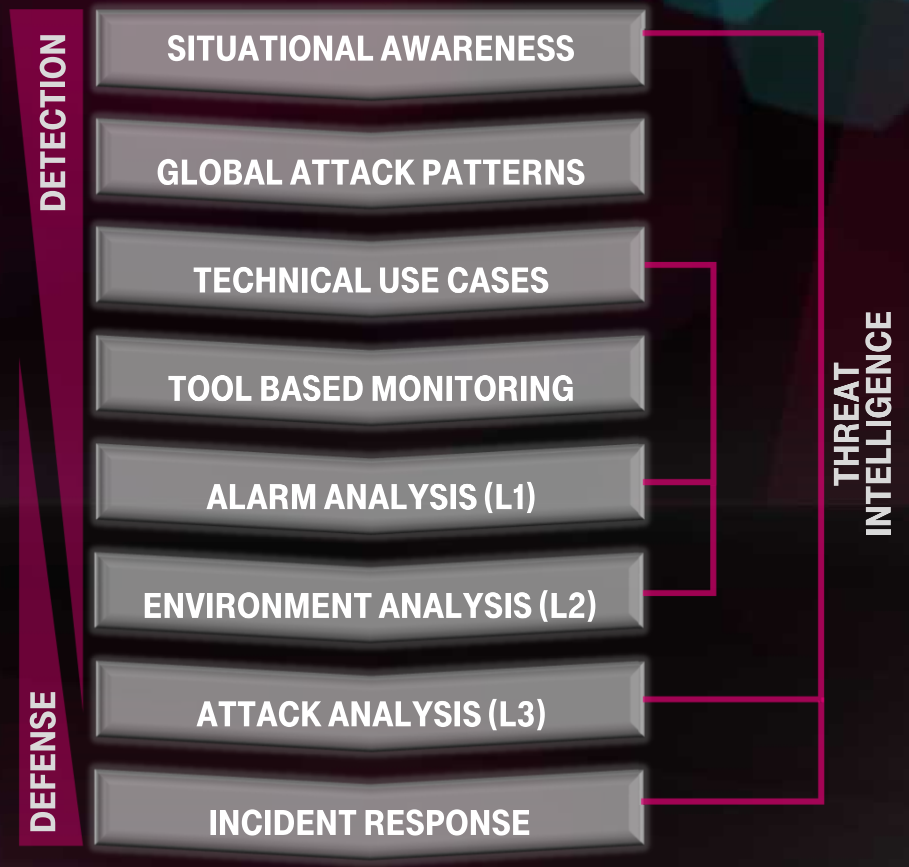
Device sources

CYBER DEFENSE PROVIDES DETECTION AND RESPONSE

THREAT INTELLIGENCE

SIEM MONITORING SERVICE

INCIDENT RESPONSE & FORENSICS



DETECTION

DEFENSE

SITUATIONAL AWARENESS

GLOBAL ATTACK PATTERNS

TECHNICAL USE CASES

TOOL BASED MONITORING

ALARM ANALYSIS (L1)

ENVIRONMENT ANALYSIS (L2)

ATTACK ANALYSIS (L3)

INCIDENT RESPONSE

THREAT INTELLIGENCE

LIFE IS FOR SHARING.

CYBER DEFENSE NEEDS HUMAN INTELLIGENCE

REQUIREMENT OF

- SECURITY EXPERTS AND
- 24/7 DUTY

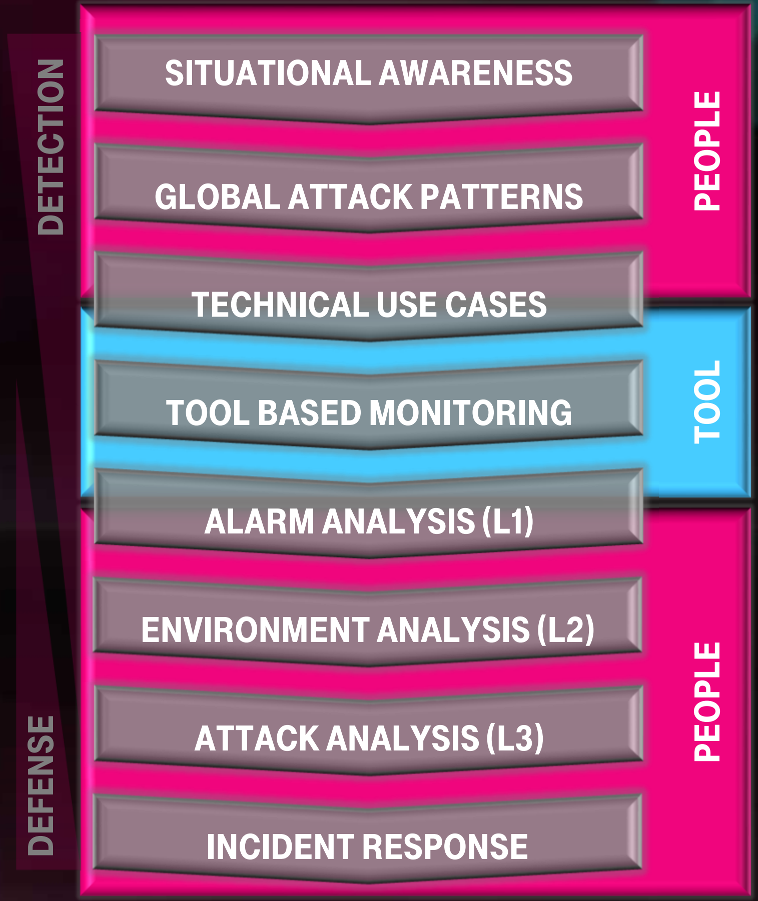
DRIVES

NEED FOR PEOPLE AND SKILL DEVELOPMENT

→

CYBER SECURITY PROFESSIONAL TRAINING PROGRAM

DTAG & COLOGNE CHAMBER OF COMMERCE



DETECTION

DEFENSE

SITUATIONAL AWARENESS

GLOBAL ATTACK PATTERNS

TECHNICAL USE CASES

TOOL BASED MONITORING

ALARM ANALYSIS (L1)

ENVIRONMENT ANALYSIS (L2)

ATTACK ANALYSIS (L3)

INCIDENT RESPONSE

PEOPLE

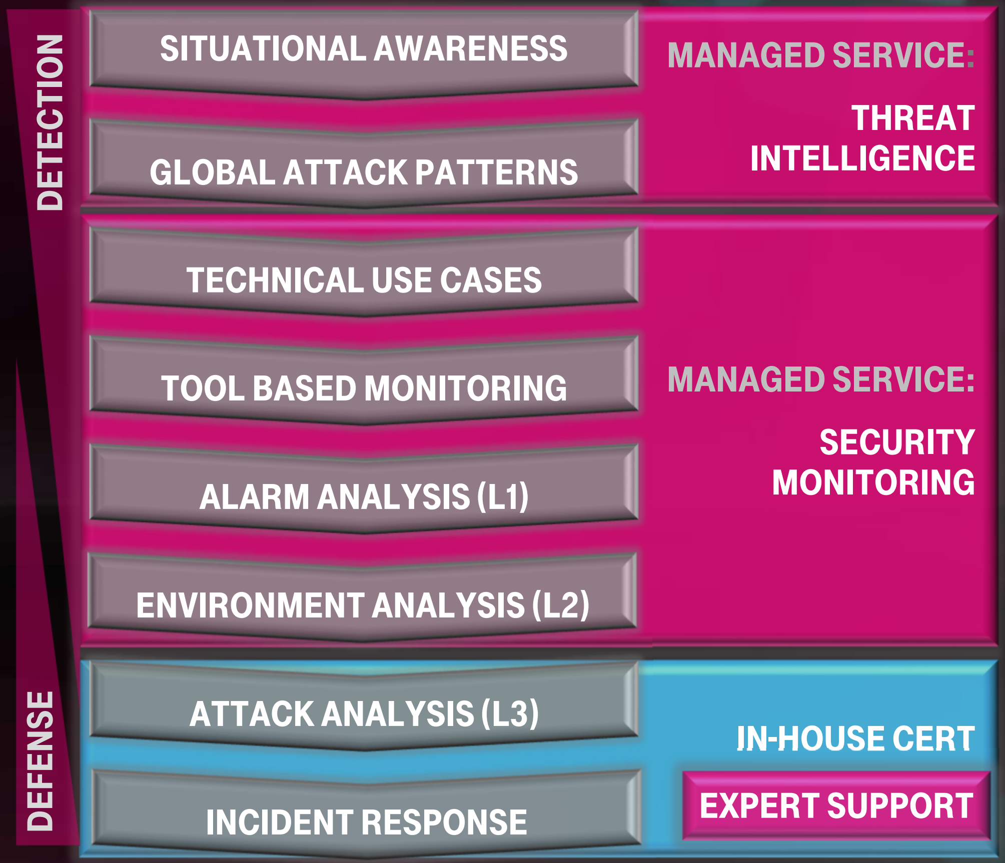
TOOL

PEOPLE

LIFE IS FOR SHARING.

CYBER DEFENSE IS A MANAGED SERVICE

A STRONG OUTSOURCING PARTNER HELPS TO ESTABLISH EFFICIENT CYBER DEFENSE



DETECTION

SITUATIONAL AWARENESS

GLOBAL ATTACK PATTERNS

MANAGED SERVICE:

THREAT INTELLIGENCE

TECHNICAL USE CASES

TOOL BASED MONITORING

ALARM ANALYSIS (L1)

ENVIRONMENT ANALYSIS (L2)

MANAGED SERVICE:

SECURITY MONITORING

DEFENSE

ATTACK ANALYSIS (L3)

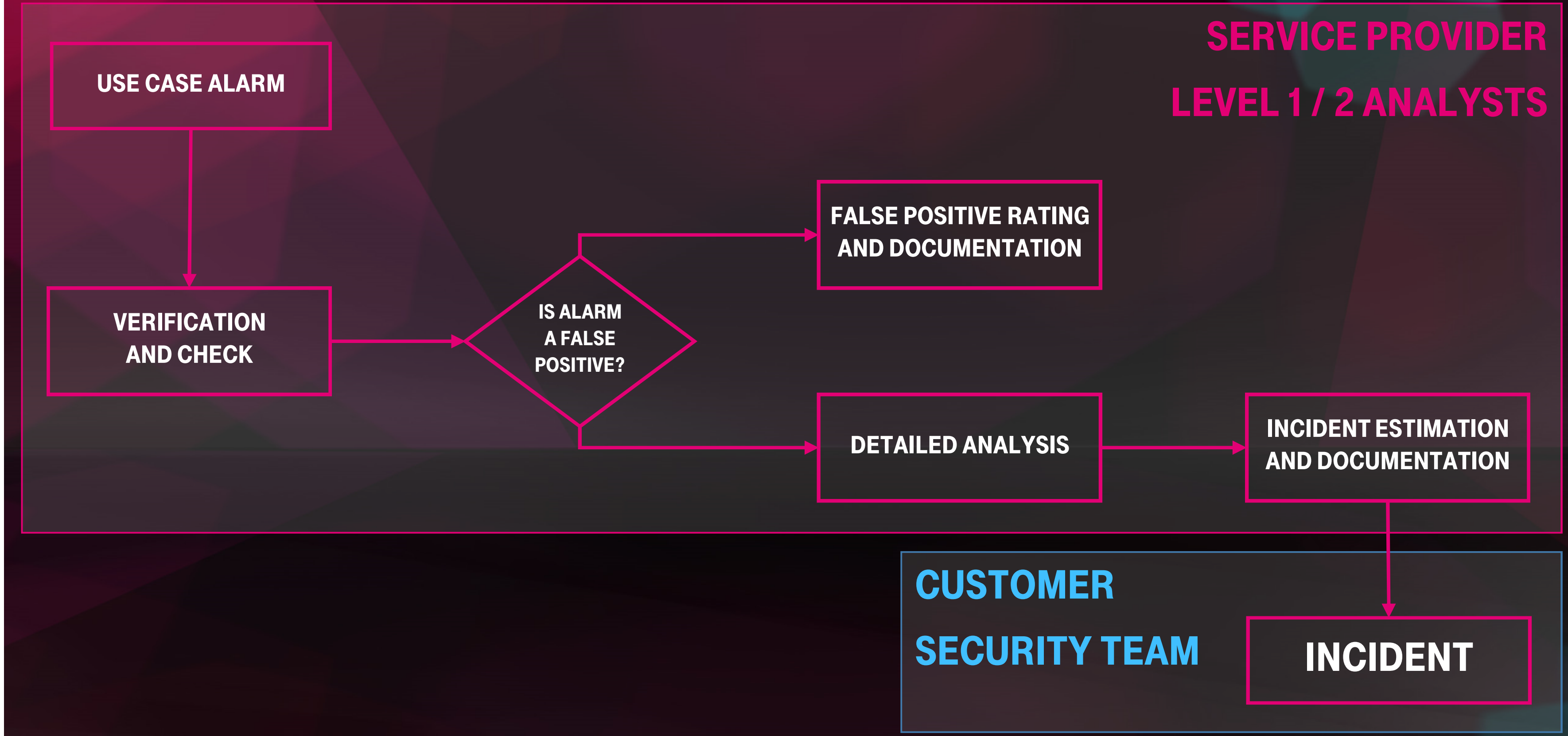
INCIDENT RESPONSE

IN-HOUSE CERT

EXPERT SUPPORT

LIFE IS FOR SHARING.

CYBER DEFENSE MONITORING WORKFLOW



SERVICE PROVIDER

LEVEL 1 / 2 ANALYSTS

USE CASE ALARM

VERIFICATION AND CHECK

IS ALARM A FALSE POSITIVE?

FALSE POSITIVE RATING AND DOCUMENTATION

DETAILED ANALYSIS

INCIDENT ESTIMATION AND DOCUMENTATION

CUSTOMER

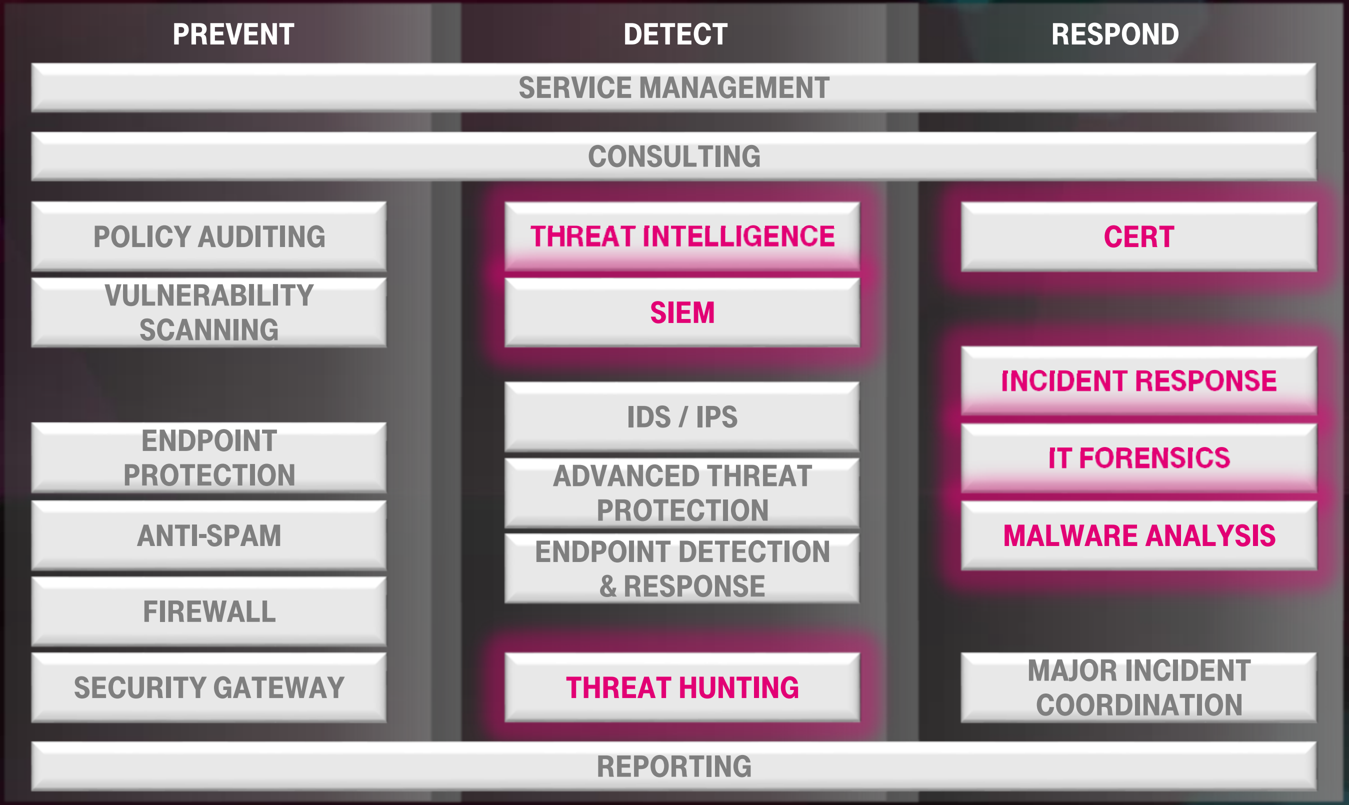
SECURITY TEAM

INCIDENT

CYBER DEFENSE IS PART OF OVERALL SECURITY OPERATIONS

FURTHER COOPERATION OPPORTUNITIES EXIST FOR OPERATIONAL SECURITY

SECURITY AS A SERVICE BY A TRUSTED PROVIDER



PREVENT

DETECT

RESPOND

SERVICE MANAGEMENT

CONSULTING

PREVENT:
- POLICY AUDITING
- VULNERABILITY SCANNING
- ENDPOINT PROTECTION
- ANTI-SPAM
- FIREWALL
- SECURITY GATEWAY

DETECT:
- THREAT INTELLIGENCE
- SIEM
- IDS / IPS
- ADVANCED THREAT PROTECTION
- ENDPOINT DETECTION & RESPONSE
- THREAT HUNTING

RESPOND:
- CERT
- INCIDENT RESPONSE
- IT FORENSICS
- MALWARE ANALYSIS
- MAJOR INCIDENT COORDINATION

REPORTING

LIFE IS FOR SHARING.

CYBER DEFENSE TAKE AWAY

DIGITIZATION INCREASES ATTACK SURFACE:

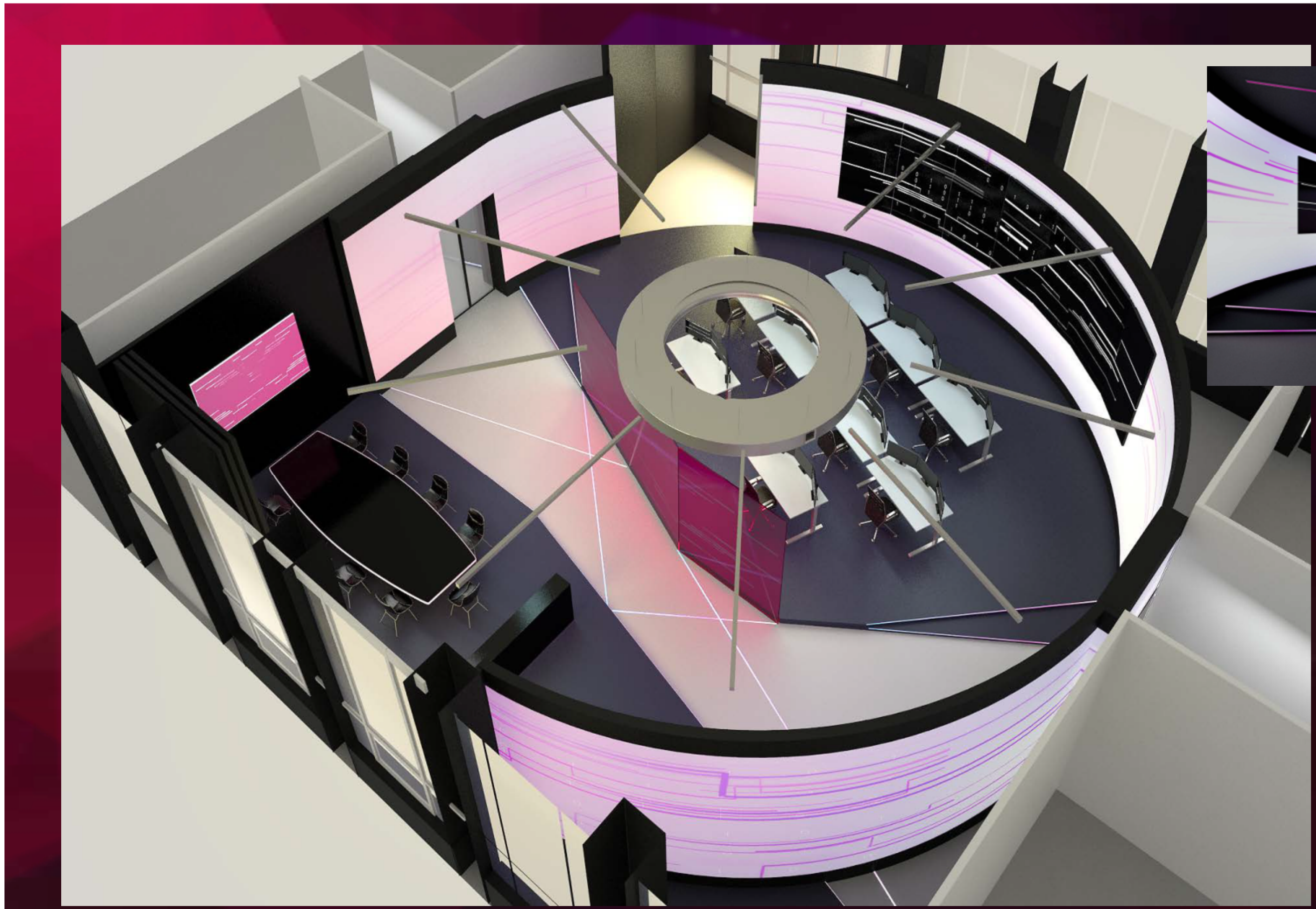
CRIME FOLLOWS BUSINESS

WE NEED RESILIENCE:

PREVENT + DETECT + RESPOND

MANAGED SERVICES HELP TACKLE

THE CYBER DEFENSE CHALLENGE



Q & A

LIFE IS FOR SHARING.