# EFFECTIVELY TARGETING ADVANCED THREATS

Terry Sangha

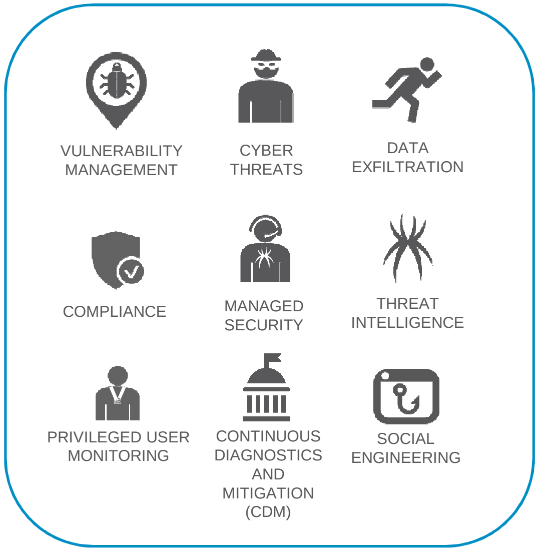
Sales Engineer at Trustwave

Trustwave®

Smart security on demand

# THE CHALLENGE

## PROTECTING YOUR ENVIRONMENT IS NOT GETTING EASIER



VULNERABILITY MANAGEMENT

CYBER THREATS

DATA EXFILTRATION

COMPLIANCE

MANAGED SECURITY

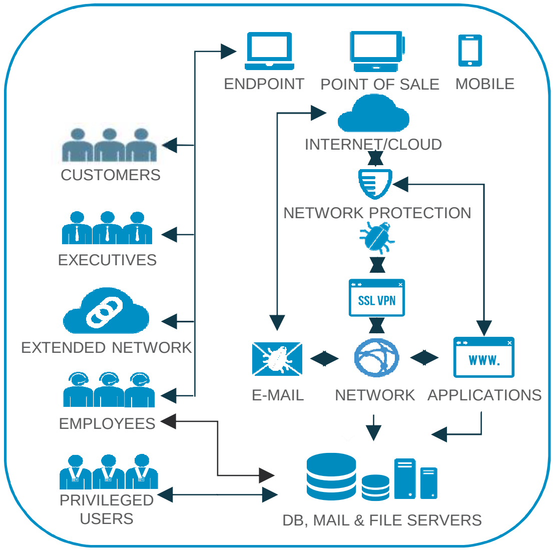
THREAT INTELLIGENCE

PRIVILEGED USER MONITORING

CONTINUOUS DIAGNOSTICS AND MITIGATION (CDM)

SOCIAL ENGINEERING

Considerations



ENDPOINT

POINT OF SALE

MOBILE

CUSTOMERS

INTERNET/CLOUD

NETWORK PROTECTION

EXECUTIVES

SSL VPN

EXTENDED NETWORK

E-MAIL

NETWORK

WWW.

APPLICATIONS

EMPLOYEES

PRIVILEGED USERS

DB, MAIL & FILE SERVERS

Complexity

In addition, there is an expected shortage of qualified security professionals totaling between 1 and 2 million by 2019.[1]

[1]Information Week, “Cyber-Security Skills Shortage Leaves Companies Vulnerable”, 8/1/16

# THE CYBER FOCUS

## UNDERSTANDING ADVANCED THREATS

### What is it?

A cyber-threat is any malicious act that could gain access to a computer network without authorization. A cyber-threat perpetrator is known as a Threat Actor or “Bad Actor”.

### What are some examples?

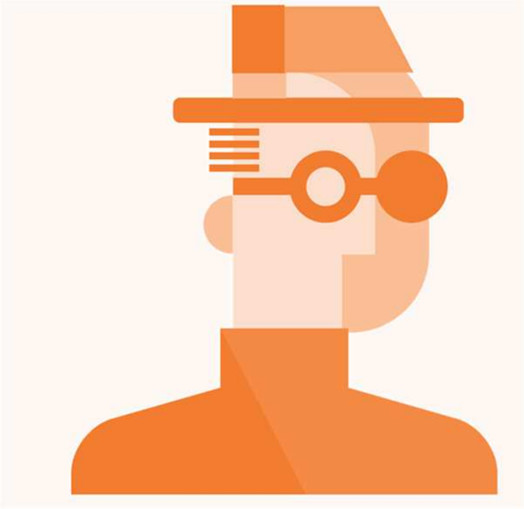
- Theft of identity, credit cards, intellectual property
- Spoofing wire transfers or access credentials
- Business disruption
- Criminal extortion
- Destruction
- Influence business decisions
- Weapons proliferation
- Criminal exploitation

### Who’s responsible?

- National Governments
- Terrorists
- Industrial Spies and Organized Crime Groups
- Hackivists
- Hackers

# CYBERCRIME MOTIVATIONS

## WHY THIS PROBLEM IS NOT GOING AWAY



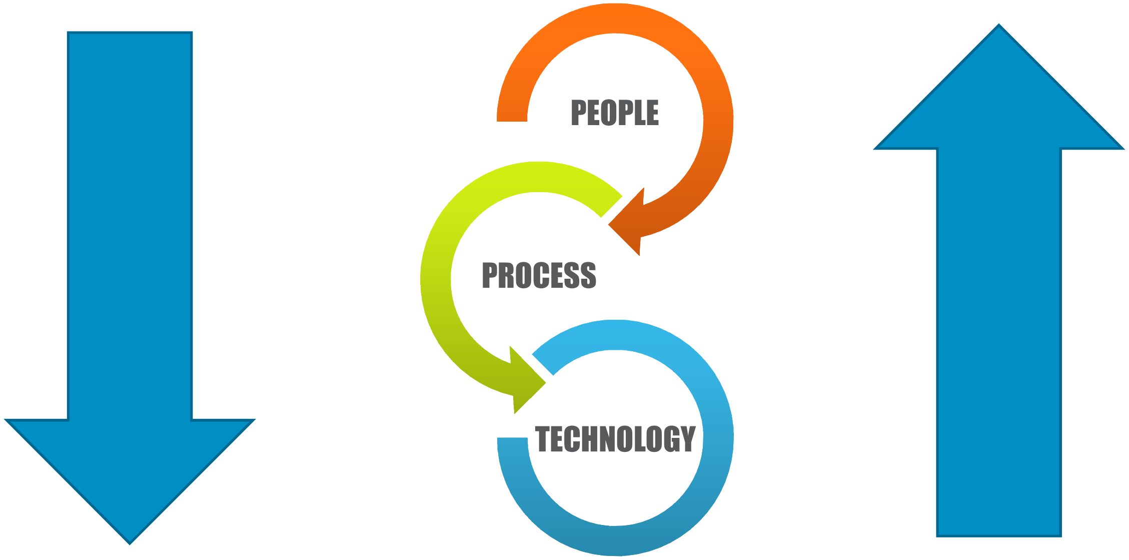
- Trustwave Global Security Report research shows 1,425% Return on Investment
- Estimated ROI for a one-month ransomware campaign
- Based on Trustwave SpiderLabs research into underground markets
- One example: $5,900 investment = $84,100 profit

# WHO’S ASKING

## PERCEIVED VALUE OF SECURITY

BUSINESS FOCUS

OPERATIONS FOCUS

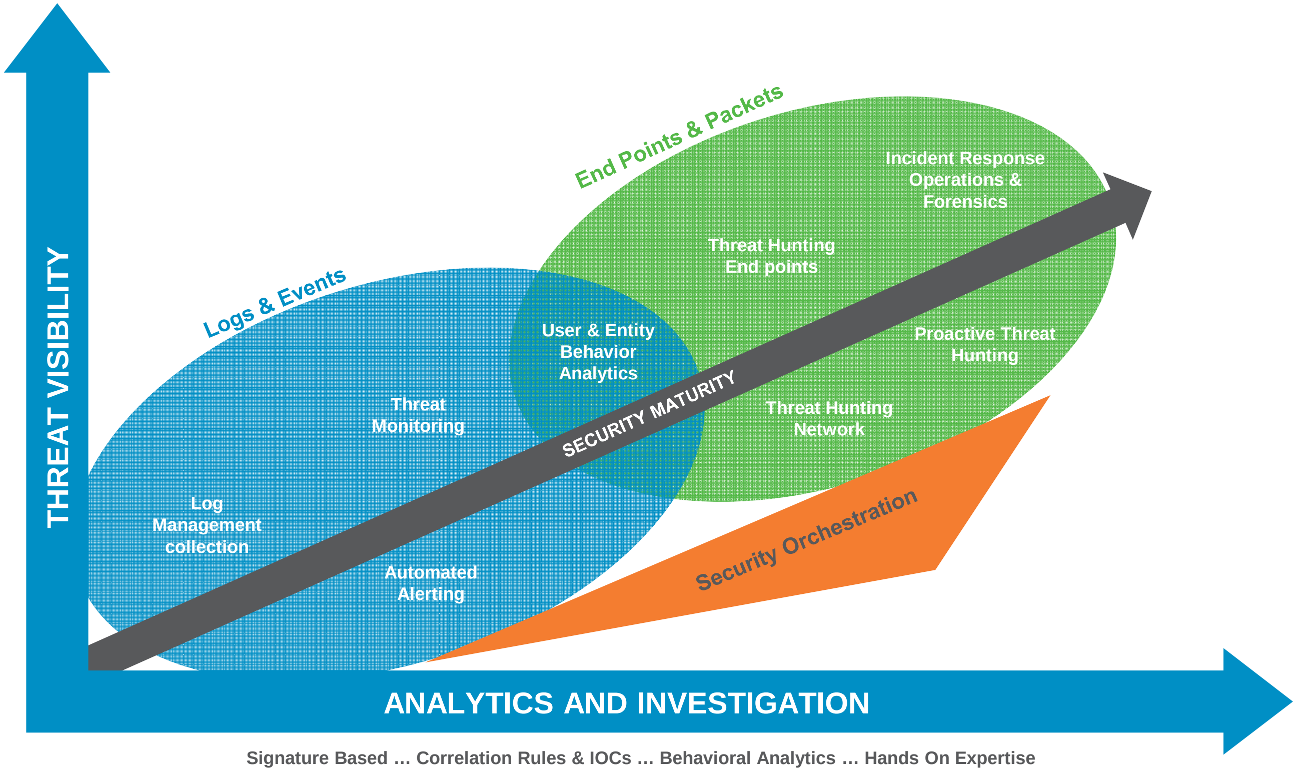


Business leaders tend to view value more holistically and from top down.

Operations leaders tend to view value starting from environment and work up toward people.

# THREAT DETECTION & RESPONSE

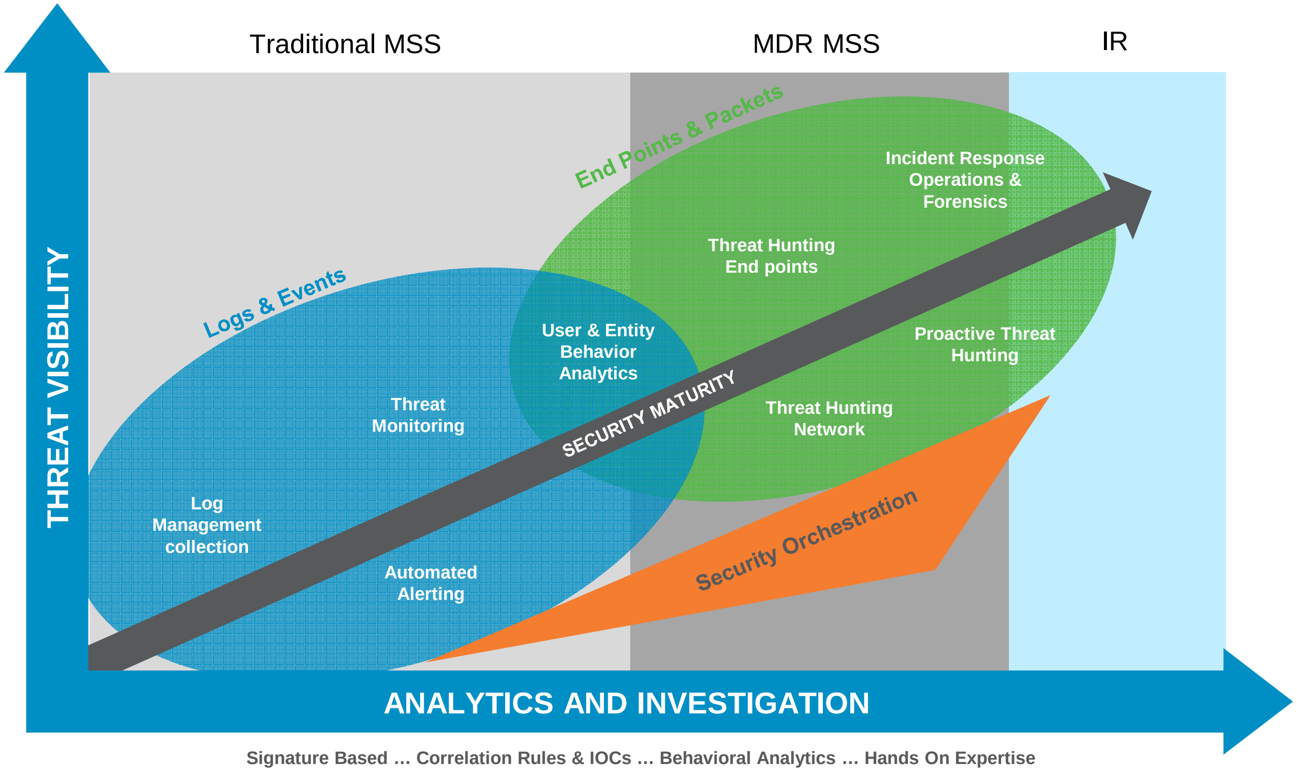
## A SECURITY MATURITY MODEL



Signature Based … Correlation Rules & IOCs … Behavioral Analytics … Hands On Expertise

# THREAT DETECTION & RESPONSE

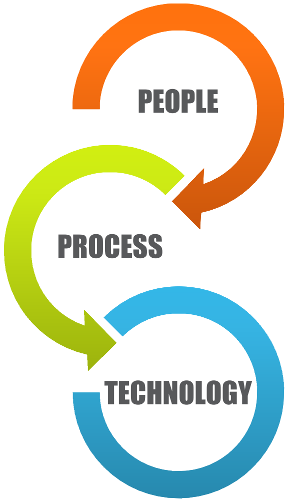
## A SECURITY MATURITY MODEL


Traditional MSS
MDR MSS
IR
THREAT VISIBILITY
ANALYTICS AND INVESTIGATION
Logs & Events
End Points & Packets
Incident Response Operations & Forensics
Threat Hunting End points
User & Entity Behavior Analytics
Proactive Threat Hunting
Threat Monitoring
SECURITY MATURITY
Threat Hunting Network
Log Management collection
Automated Alerting
Security Orchestration
Signature Based … Correlation Rules & IOCs … Behavioral Analytics … Hands On Expertise

- Traditional MSS provides foundational detect and notify capabilities.
- MDR MSS provides detect and remediate capabilities.

# WHAT IS MDR?

## DEFINITION OF MANAGED DETECTION AND RESPONSE



According to Gartner[1], Managed Detection and Response (MDR) services are:

- An emerging group of security monitoring providers with approaches that do not fit the traditional MSS model.
- These services aim to remove the burden from clients of having to figure out "what method or device to use" for a security monitoring and response capability.
- MDR services focus on specific outcomes — threat detection, with 24/7 monitoring and alerting, and remote incident investigation and response included in the end-to-end service.

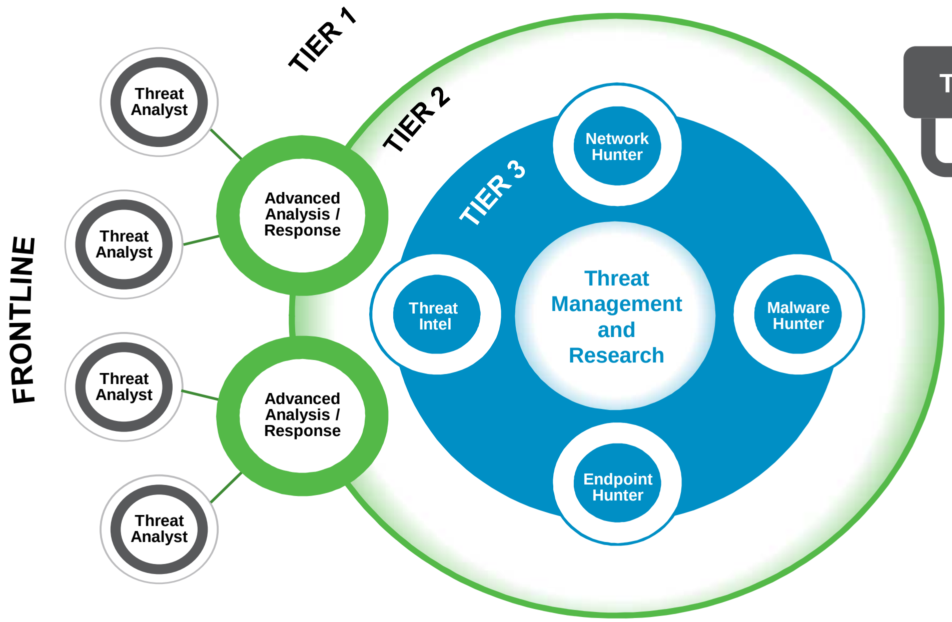
***How is this different than EDR?***

EDR is the technology piece of this service (does not include people and process).

[1]Market Guide for Managed Detection and Response Services, 10 May 2016, G00294325.

# WHAT IS MDR?

## “PEOPLE”



**Tier 1**

- Console Monitoring
- Take action
- 5-7 minutes on average per alert

**Tier 2**

- Deep investigation
- Tuning and mitigation
- 30 minutes on average per alert

**Tier 3**

- Malware reverser
- Data pivot and trend
- Industry alert
- Threat hunting

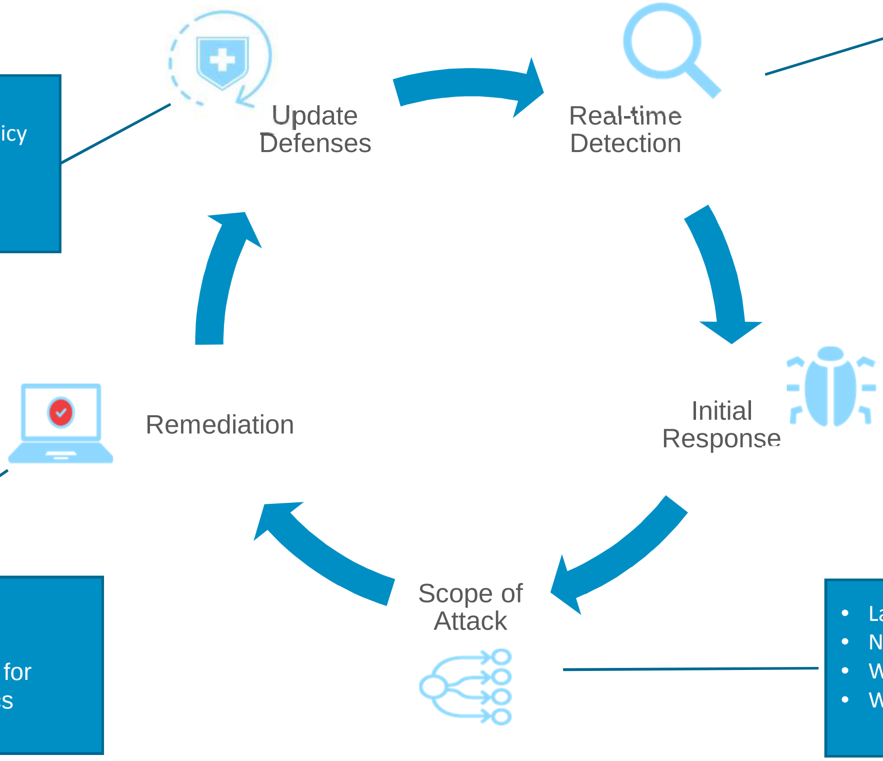
**KEY’S TO SUCCESS:**

1. The Right People
2. Standard Processes
3. Leveraged Technology

[1]Market Guide for Managed Detection and Response Services, 10 May 2016, G00294325.

# WHAT IS MDR?

## “PROCESS”



- Update EDR components
- Advise of further updates and/or policy changes to preventive solutions

- Endpoint behavior
- Executables
- File changes
- Registry mods
- Memory injection
- IOC’s
- Unique threat intelligence

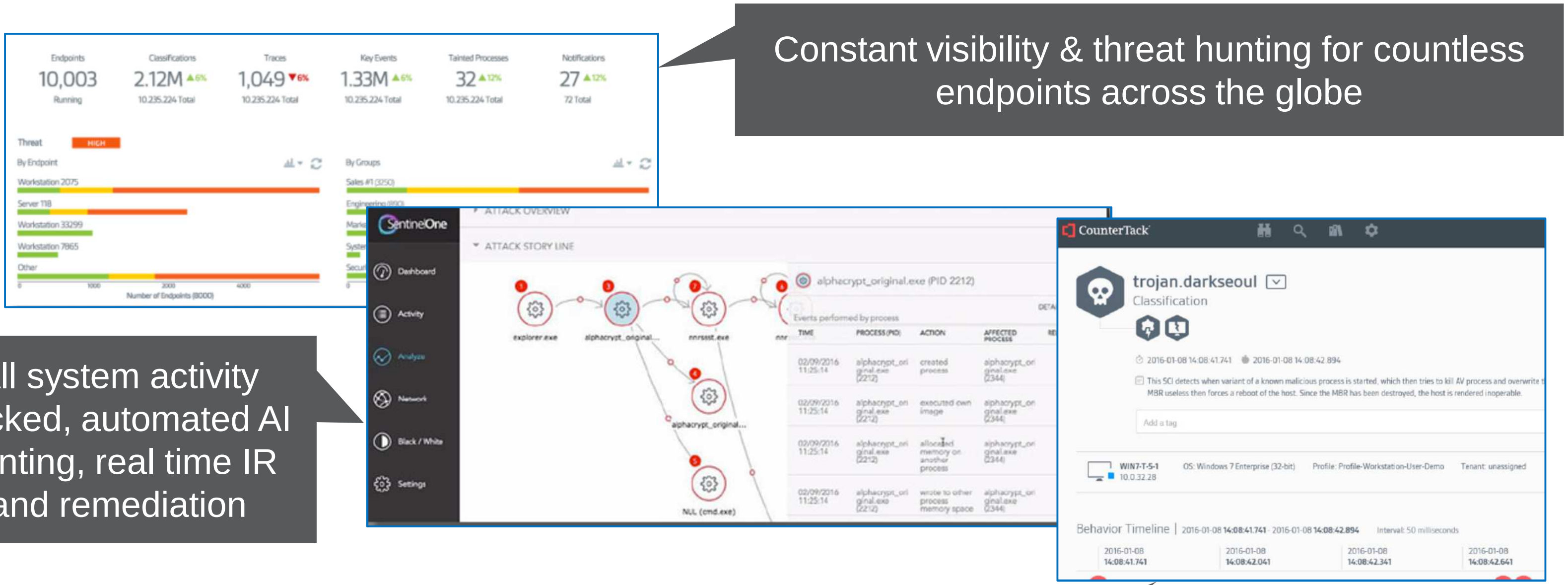
- Notification Actions
- Account lockouts
- Kill processes
- Files deletions
- Quarantine
- File blacklisting
- Remote shell

- Lateral movement
- Network comms
- What
- Where
- When
- How

- Remote actions
- Customer actions
- Potential onsite upon request for further remediation & forensics assistance

# WHAT IS MDR?

## “TECHNOLOGY”



alphacrypt_original.exe (PID 2212)

Events performed by process

| TIME | PROCESS (PID) | ACTION | AFFECTED PROCESS |
|---|---|---|---|
| 02/09/2016 11:25:14 | alphacrypt_original.exe (2212) | created process | alphacrypt_original.exe (2344) |
| 02/09/2016 11:25:14 | alphacrypt_original.exe (2212) | executed own image | alphacrypt_original.exe (2344) |
| 02/09/2016 11:25:14 | alphacrypt_original.exe (2212) | allocated memory on another process | alphacrypt_original.exe (2344) |
| 02/09/2016 11:25:14 | alphacrypt_original.exe (2212) | wrote to other process memory space | alphacrypt_original.exe (2344) |

2016-01-08 14:08:41.741 2016-01-08 14:08:42.894

This SCI detects when variant of a known malicious process is started, which then tries to kill AV process and overwrite t MBR useless then forces a reboot of the host. Since the MBR has been destroyed, the host is rendered inoperable.

WIN7-T-5-1 10.0.32.28 OS: Windows 7 Enterprise (32-bit) Profile: Profile-Workstation-User-Demo Tenant: unassigned

Behavior Timeline | 2016-01-08 **14:08:41.741** - 2016-01-08 **14:08:42.894** Interval: 50 milliseconds

2016-01-08 **14:08:41.741** | 2016-01-08 **14:08:42.041** | 2016-01-08 **14:08:42.341** | 2016-01-08 **14:08:42.641**

Constant visibility & threat hunting for countless endpoints across the globe

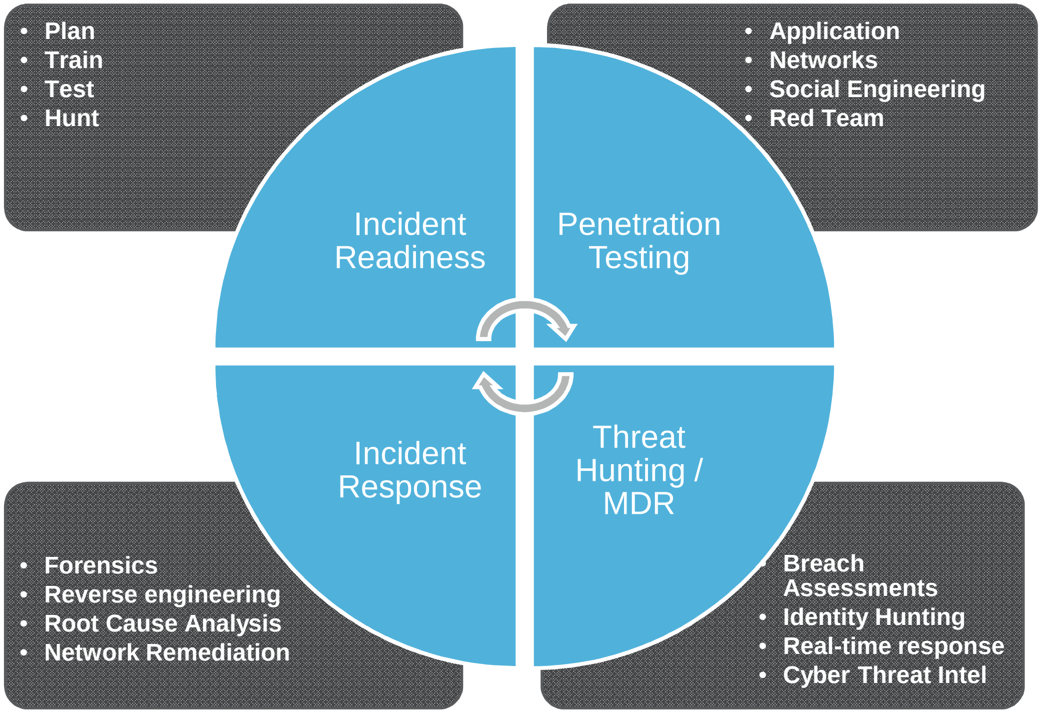
All system activity tracked, automated AI hunting, real time IR and remediation

Immediate threat intel generation and enterprise threat hunting capability

# MOVING TOWARD AN OFFENSIVE POSTURE

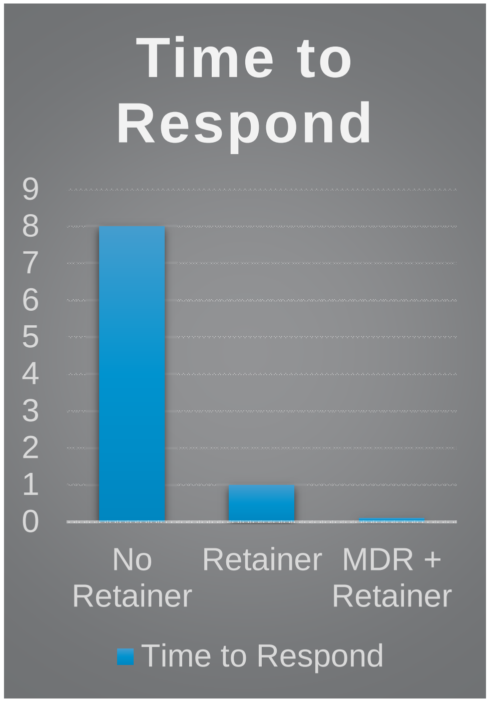
## INCIDENT READINESS AND THREAT HUNTING

- Threat hunting and incident response are inextricably linked
- All elements of a robust incident readiness program
- Incident readiness is an organized, holistic, and systematic approach designed to ***rapidly***:
  - ✓ Prevent
  - ✓ Identify
  - ✓ Respond
  - ✓ Remediate



# TIME MATTERS

## MINIMAL TIME TO DETECT AND REMEDIATE IS ESSENTIAL

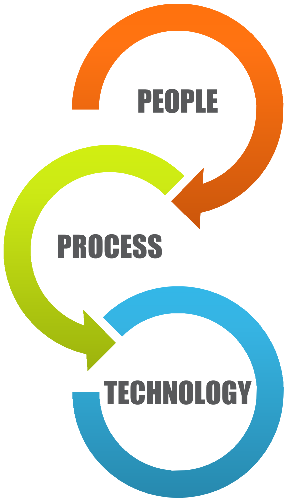


Every second an attacker is on your network, he/she is looking to move laterally and capture your golden secrets

- No retainer in place
  - ✓ Provider selection, contract negotiations, NDA, payment, travel time
  - ✓ Average time to respond 8 days
- IR retainer in place
  - ✓ IR responder on-call 24/7
  - ✓ 4-8 hour remote / 24-48 hour onsite global SLA
- MDR + retainer
  - ✓ Constant proactive threat hunting
  - ✓ Immediate remote IR – many steps automated
  - ✓ Analysis occurs concurrent to responder travel time
  - ✓ Response & remediation time is minutes, not days

# WHAT DOES GOOD LOOK AND FEEL LIKE?

DEFINE SUCCESS AND LEVEL SET EXPECTATIONS



- Define business objectives
- Understand your existing security posture
- Identify goals that tie to business outcomes
- Prioritize activities based on risk exposure
- “Rinse and repeat”

# THANK YOU

Trustwave®

Smart security on demand