Protect 2015

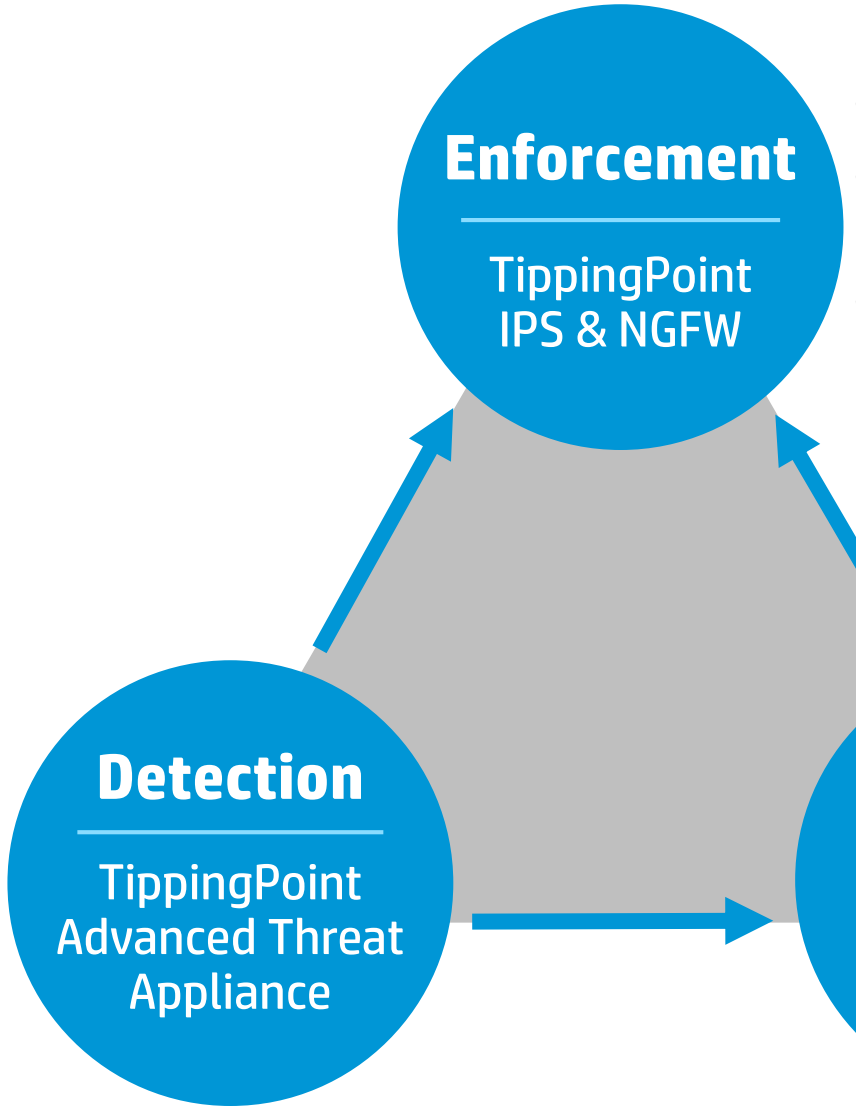
Hit the security trifecta: detection, enforcement and intelligence

TJ Alldridge, HP TippingPoint
Bob Corson, Trend Micro
Sri Karnam, HP ArcSight

#HPProtect

The trifecta pays well

Layered protection from HP Security



- Block communication to CnC
- Stop malware from moving laterally across the network
- Block future attacks

- Detect targeted attacks and slow detonating malware
- Analyze threats
- Deliver actionable info to SMS and ArcSight

- Assess threats further
- Correlate with other contextual data
- Further analyze the threat and display attack pattern

Anatomy of a targeted attack

Gather intelligence
Research potential targets

Point of entry
Access into the network

Command and control
Phone home for instructions

Lateral movement
Moving freely in the network

Data of interest
Finding the desired info

Data exfiltration
The drop site for the stolen info

Acme Corp. breach

Gather intelligence
Research potential targets

- Identify vendor list
- Do early recon
  - Badge scraping
  - Ping firewall
  - Map the perimeter
  - OS info

Point of entry
Access into the network

- Infiltrate by using hacked credentials

Command and control
Phone home for instructions

- Download additional payload
- Receive instructions to look for files named passwords
- Receive instructions to move laterally

Lateral movement
Moving freely in the network

- Map the network to identify security strength and weakness
- Find the crown jewels and how to get them out

Data of interest
Finding the desired info

- Widget designs for right hand watch
- Edit watch schematics so only works on left hand
- Make copy of all CEO's emails

Data exfiltration
The drop site for the stolen info

- Post all the files to Dropbox for undetectable retrieval

Acme Corp. breach

Gather intelligence
Research potential targets

- Identify vendor list
- Do early recon
  - Badge scraping
  - Ping firewall
  - Map the perimeter
  - OS info
- Employee education is critical

Point of entry
Access into the network

- Infiltrate by using hacked credentials
- HP TippingPoint Advanced Threat Appliance Family
  - Monitor 100+ protocols and all network traffic

- HP TippingPoint Advanced Threat Appliance Family and IPS/NGFW
  - Identify the CnC IP address and DNS info for blocking
  - Detonate and analyze payload in sandbox

Command and control
Phone home for instructions

- Download additional payload
- Receive instructions to look for files named passwords
- Receive instructions to move laterally

Lateral movement
Moving freely in the network

- Map the network to identify security strength and weakness
- Find the crown jewels and how to get them out

- HP TippingPoint Advanced Threat Appliance Family and IPS/NGFW
  - Detect and block lateral movement

Data of interest
Finding the desired info

- Widget designs for right hand watch
- Edit watch schematics so only works on left hand
- Make copy of all CEO's emails

- HP TippingPoint Advanced Threat Appliance Family
  - Visibility into over 100 protocols
  - Sees attacker activity like multiple login attempts at 3am
  - Sees data being moved at odd times

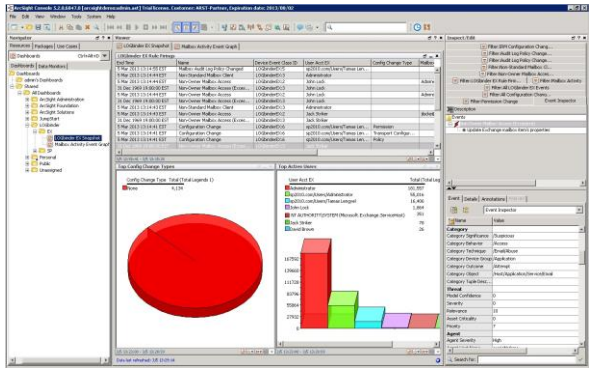
Data exfiltration
The drop site for the stolen info

- Post all the files to Dropbox for undetectable retrieval

- HP TippingPoint Advanced Threat Appliance Family
  - Visibility into over 100 protocols we can see small or large data movements
  - FTP, SQL, UDP

Why ATA with IPS and ArcSight?

Detecting and blocking a targeted attack



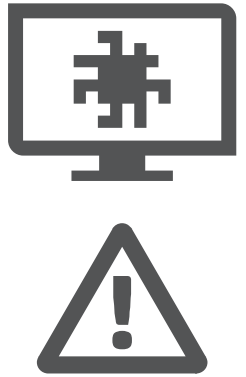
ArcSight SIEM

TippingPoint NGFW

TippingPoint Security Management System

TippingPoint Advanced Threat Appliance

TippingPoint IPS

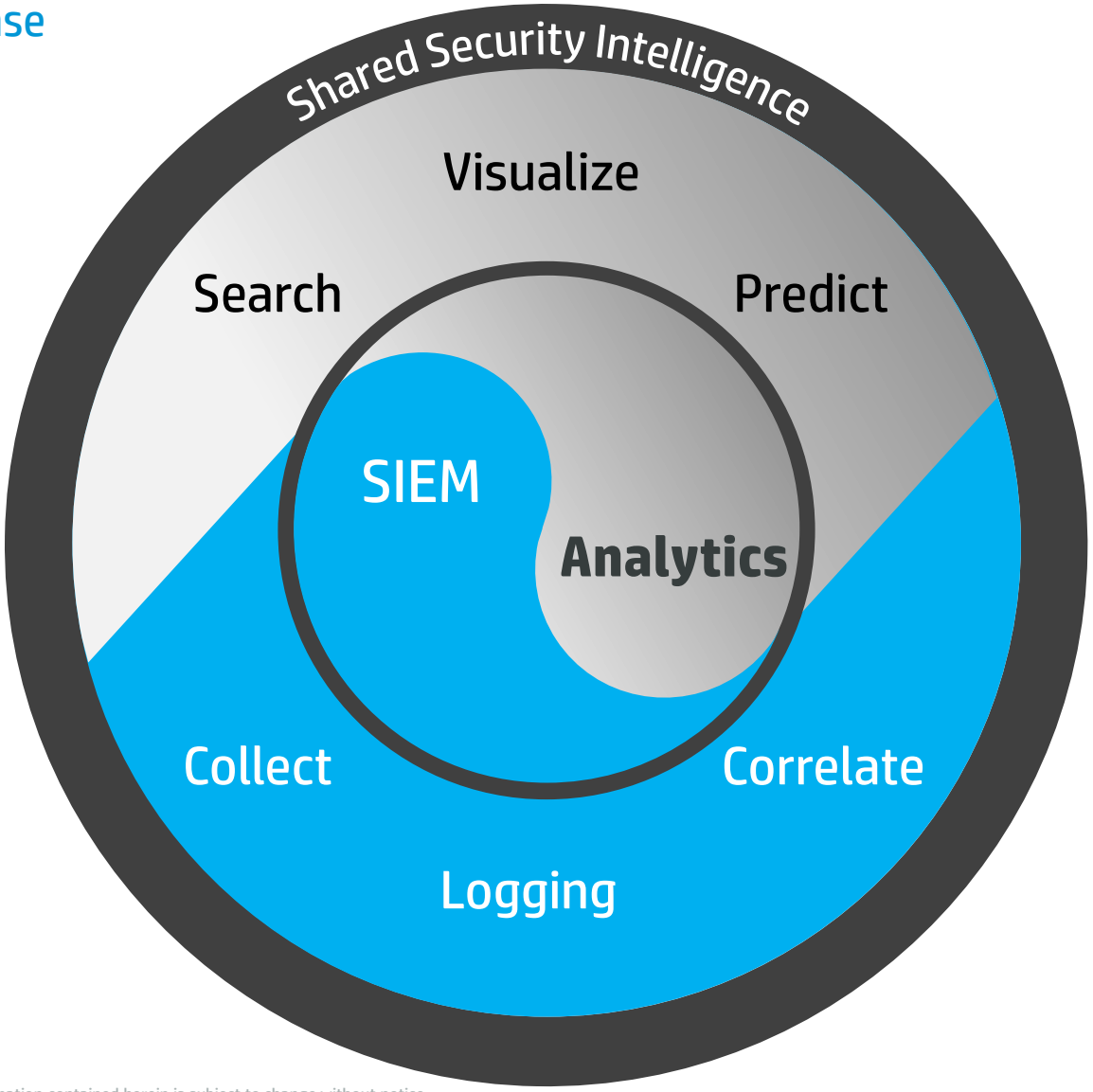


Why IPS with ATA and ArcSight?

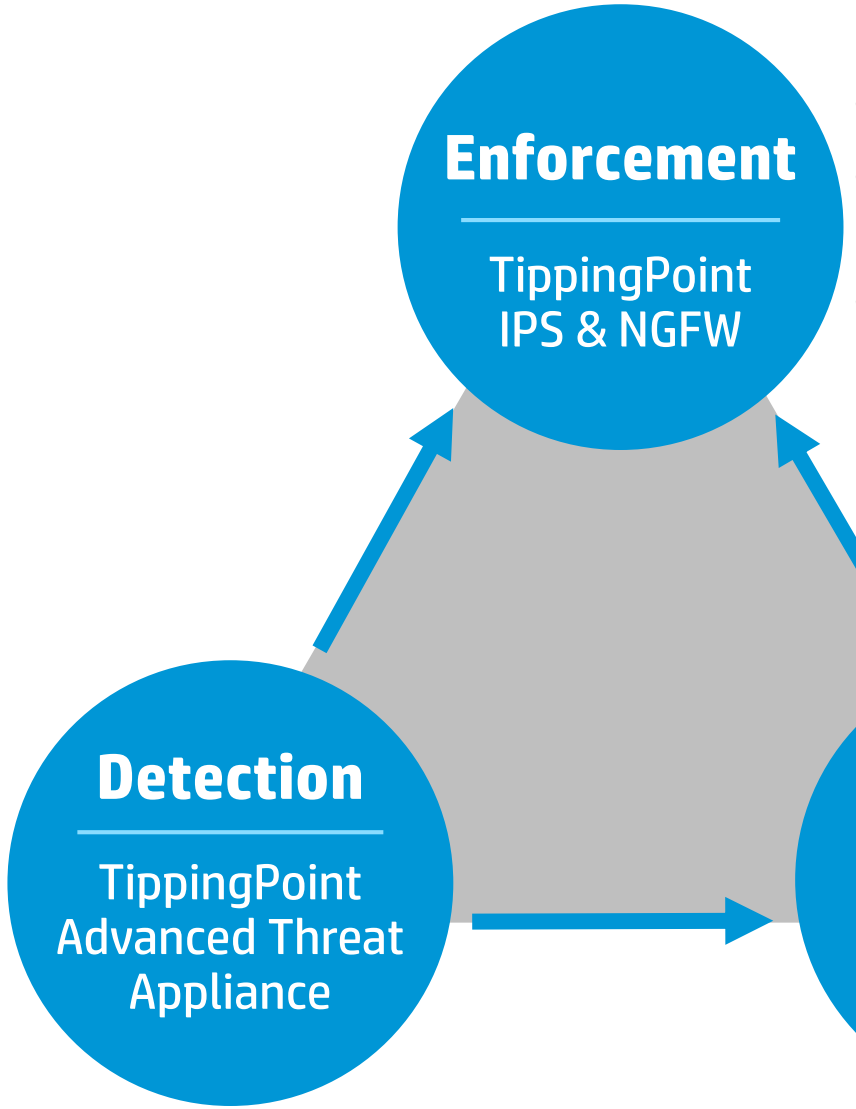
Block attacks inbound, outbound and laterally

Why ArcSight with ATA and IPS?

Next Generation Cyber Defense



Layered protection from HP Security



- Block communication to CnC
- Stop malware from moving laterally across the network
- Block future attacks

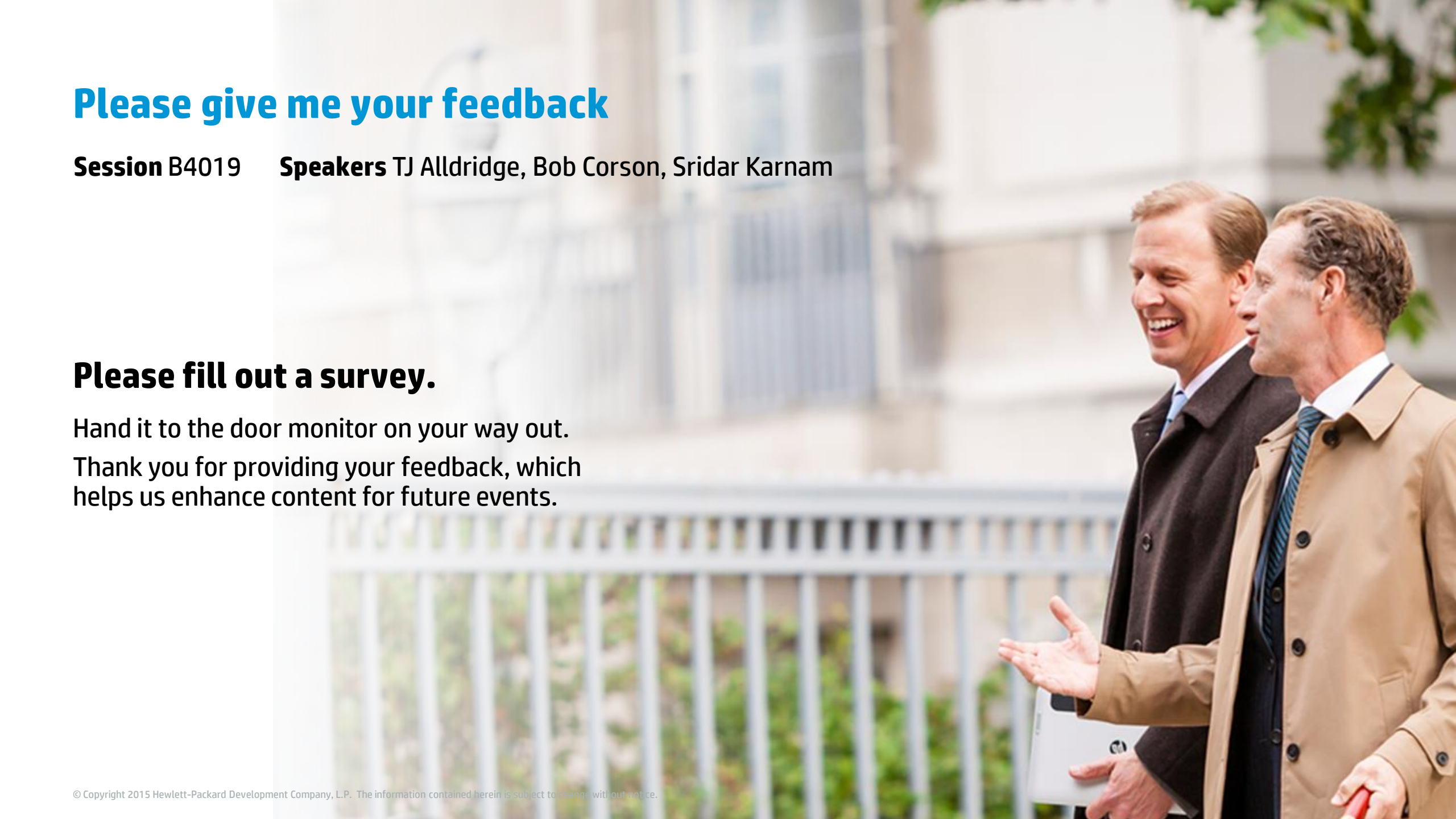
- Detect targeted attacks and slow detonating malware
- Analyze threats
- Deliver actionable info to SMS and ArcSight

- Assess threats further
- Correlate with other contextual data
- Further analyze the threat and display attack pattern

Q&A

Please give me your feedback

Session B4019 **Speakers** TJ Alldridge, Bob Corson, Sridar Karnam



Please fill out a survey.

Hand it to the door monitor on your way out.

Thank you for providing your feedback, which helps us enhance content for future events.

Thank you