Hewlett Packard
Enterprise

Protect 2016

Please give me your feedback

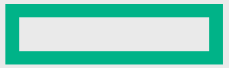
Session ID: B9407 **Speaker:** Tammy Torbert

—Use the mobile app to complete a session survey

1. Access “My schedule”
2. Click on the session detail page
3. Scroll down to “Rate & review”
   - If the session is not on your schedule, just find it via the app’s “Session Schedule” menu, click on this session, and scroll down to “Rate & Review”
   - If you don’t have it, download the event app today. Go to your phone’s app store and search for “HPE Protect 2016”

—To access the session survey online, go to the Agenda Builder in the event session catalog and click on your session

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



Hewlett Packard
Enterprise

Realizing value from your SIEM investments

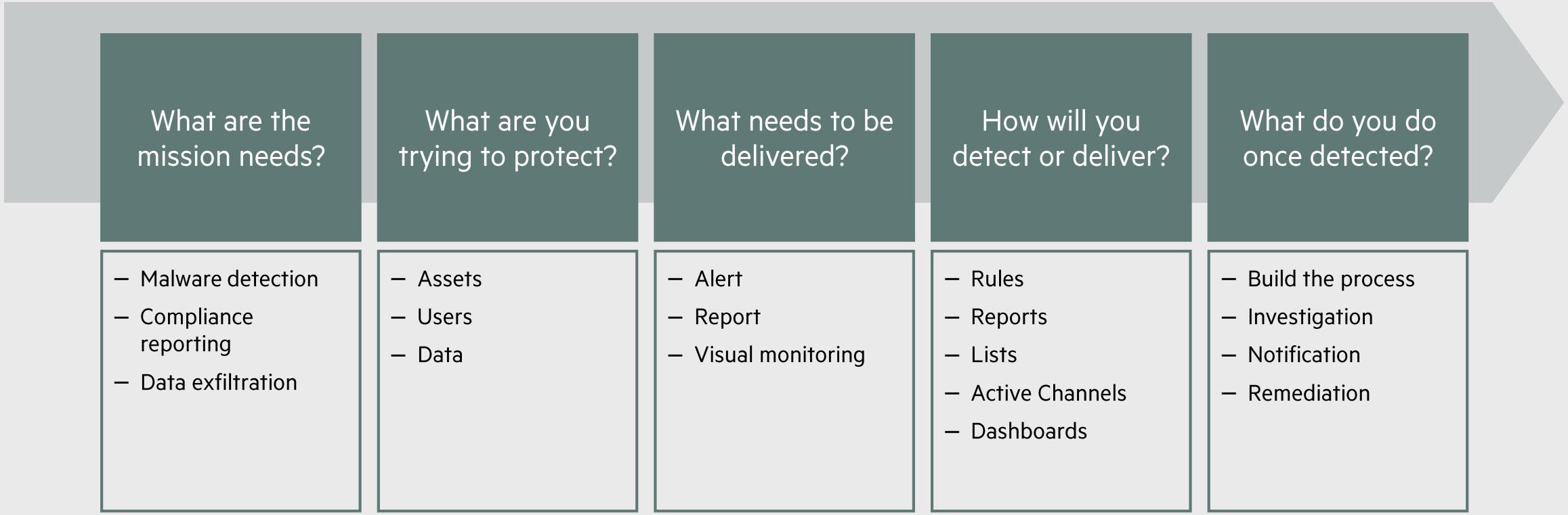
Tammy Torbert, Worldwide Solution Architect

Where does it go wrong?

It all starts with understanding the requirements

- What's the business or agency mission?
- Can everyone on the team articulate the SOC mission?
- Is the focus on compliance, perimeter, insider threat, application monitoring or some combination thereof?
- What type of use cases support the mission needs?
- Do you have the data feeds to support the mission requirements?
- Do I have the right resources and time allocated to make sure this project is a success?

What makes a use case?



What is the mission?

— Can everyone on the team articulate the SOC mission? Can they articulate the business or agency mission?

— Is the focus on compliance, perimeter, insider threat, application monitoring or some combination thereof?

— What type of use cases support the mission needs?

— Do you have the data feeds to support the mission requirements?

Mission focus

Perimeter

- Internet connection monitoring
- Malware detection
- Connection monitoring to partners

- Typical data feeds include
  - Firewall
  - VPN
  - IDS/IPS
  - Proxy
  - Sandboxing
  - Malware detection
  - Mail gateway

Mission focus

Insider threat

- Privileged user monitoring
- User activity monitoring
- Shared account usage
- Data exfiltration

- Typical data feeds include
  - Operating system logs
  - Authentication logs (RADIUS, LDAP, TACACS, etc.)
  - Application logs for user activities
  - Data loss prevention logs

Mission focus

Application monitoring

- Web application monitoring
- Database activity monitoring
- In-house application monitoring

- Typical data feeds include
  - Web server logs
  - Application middleware logs
  - Database server logs
  - Database activity monitoring logs
  - Custom application logs

What are you protecting?

- Assets
  - Do you know which assets are critical in your infrastructure?
  - Do you know what assets present the greatest risk to your infrastructure?
- Users
  - What users present the greatest risk if compromised?
  - Are you aware of the scope of access of user permissions?
  - Do you monitor user accounts that are not assigned to a person?
- Data
  - Do you know where your critical data resides?
  - How is this data accessed?
  - Do you have logs monitoring the access of this critical data?

What do I deliver?

- Do I need to alert on a specific event or series of events?
  - What alert needs to be generated?
  - When do they need to be generated?
  - Is there a threshold for the alert?
  - What actions need to be taken when the alert occurs?
- Do other items require reporting?
  - If yes, over what period of time? Daily, weekly, monthly?

Building the detection

- Build the mission relevant content
- This can include the rules, reports, active channels, lists, etc.
- Rules
  - Use these when you need an action taken
  - Use these when you need to update a list, generate an alarm
- Reports
  - Use these when you need to deliver something to another party, the customer, the business unit
- Lists
  - Use this for tracking; tracking bad guys, tracking recent infections
- Active Channels
  - Use this for watching the live stream

Build the process

The ‘now what’ moment?

– What do you do when something happens?

– What’s the process to classify an event as incident?

– What’s the incident handling procedures for every type of incident that occurs?

– How are events investigated?

– How do you handle events that span across a shift?

Recommended actions

The up front investment

- Take the time to build your network model (at least the zones portion)
  - The network model defines the IP ranges within your environment along with the assets
  - This can be used to drive permissions
  - This can help analysis and incident response activities
  - This can help with rule detection and reporting
- Take the time to establish mission relevant asset categories and attach to zones and/or assets
  - Asset categories can be used to help characterize the model
  - This information can be used in detection, reporting, analysis and incident response activities
- Consider your service offerings outside of the SOC
  - Do you have capabilities that you could extend to other IT support organizations?
  - Can you provide value to ISSO and ISSM staff in your organization?
  - Build some “standard” offering reports and/or dashboards that you can share with others

Recommended actions

The quick wins

- Build content that provides a quick return on value
  - If you are just getting started, don't focus on the edge cases or the tougher use cases
  - Start with the items that are known bad and provide quick value
    - Items like malware infections that are not remediated (failed clean)
    - Unallowed services being used in the environment
    - Unauthorized use of a service account, i.e. service accounts being used for interactive logins
    - Group membership updates to critical security groups
  - After building some quick return content, move on to tougher use cases
    - Items that require multiple data sources for correlation
    - Use cases that require refinement and testing to reduce the false positive rate
    - Use cases that require coordination with outside groups to define detection criteria or follow-on actions

Recommended actions

Measuring success

- Build a program to measure your success. **Metrics are key**
  - How many incidents do you create?
  - How many events do you investigate that never get declared an incident?
  - What is the breakdown of incidents/investigations per business unit?
  - How many total events are collected? Consider representing the number of investigations/incidents versus total events collected
  - What type of incidents are you detecting?
  - How many incidents per analyst hour are addressed? How many investigations per analyst hour are addressed?
  - What is the effectiveness of the rules you have deployed? Of the total rule fires, how many become declared incidents?
  - How many incidents/investigations are handled per shift? How many incidents/investigations are handled per hour? Are there differences in the typical outcome for the same type of event per analyst?

Please give me your feedback

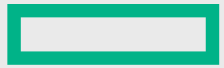
Session ID: B9407 **Speaker:** Tammy Torbert

–Use the mobile app to complete a session survey

1. Access “My schedule”
2. Click on the session detail page
3. Scroll down to “Rate & review”
   - If the session is not on your schedule, just find it via the app’s “Session Schedule” menu, click on this session, and scroll down to “Rate & Review”
   - If you don’t have it, download the event app today. Go to your phone’s app store and search for “HPE Protect 2016”

–To access the session survey online, go to the Agenda Builder in the event session catalog and click on your session

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



Hewlett Packard
Enterprise

Thank you

Tammy Torbert / tammy.torbert@hpe.com