ABOVE SECURITY®

RELEVANT IMPACT:

Building a Successful Threat Management Program

NTX ISSA 3rd Semi-Annual Cyber Security Conference
10-2-15

- Threat Management Definition
- Current State of Threat Management in Most Organizations
- Threat Management Goals
- Traits of a Successful Threat Monitoring Program
- Gathering Requirements

THREAT MANAGEMENT:

The ability to detect, analyze, remediate and report on threats to the business using human, or technological intelligence.

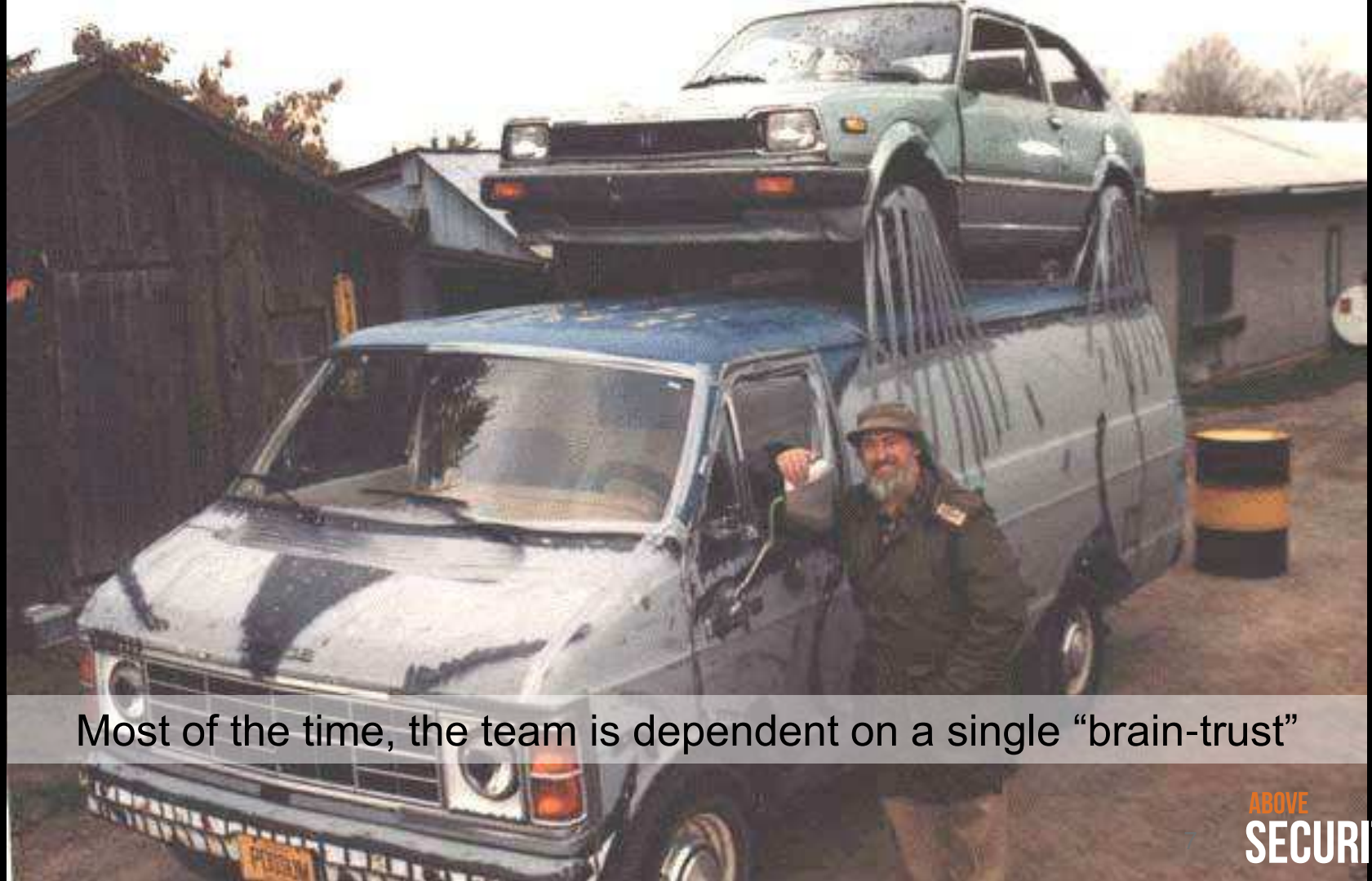
CURRENT STATE OF THREAT MANAGEMENT IN MOST ORGANIZATIONS

“We have nothing to protect.”

“We have controls - they should work…”

THE “FOOL’S PARADISE” MODEL

No threat management toolsets, or services	
Logging	Constantly overwriting
Alerting	Too many to handle - so ignored
Processes	Non existent, mostly focused on availability
Reporting	Only when needed, not targeted, too hard to understand
Accountability	Typically execs trust their management is getting things done… Management trust IT Sec (or Ops), who usually have no time…



Most of the time, the team is dependent on a single “brain-trust”

THE “DUCT TAPE” MODEL

Service is built off different ‘borrowed’ parts	
Logging	Done using the cheapest methods, and likely unreliable
Alerting	Alerts are handled hastily, and investigation is typically mishandled
Processes	Little/no processes
Reporting	Takes hours and hours to do - and still looks misassembled
Accountability	Management assume IT staff is handy and is on top of it…

Simply implementing technology doesn't give you a threat management service.

ABOVE SECURITY®

THE “SET IT AND FORGET” MODEL

Tool vendor driven threat management, lots of capital spending not much operational	
Logging	Done automatically on expensive hardware
Alerting	Was supposed to work out the box, but requires extensive configuration Internal team unaware of details
Processes	Yet to be created around tool
Reporting	A lot of reports, but none that fit the business’ requirements
Accountability	Spent a lot money on tools, so the vendor is on the hook (not really)

Services that lack context of the environment, don't integrate with processes do not offer value.

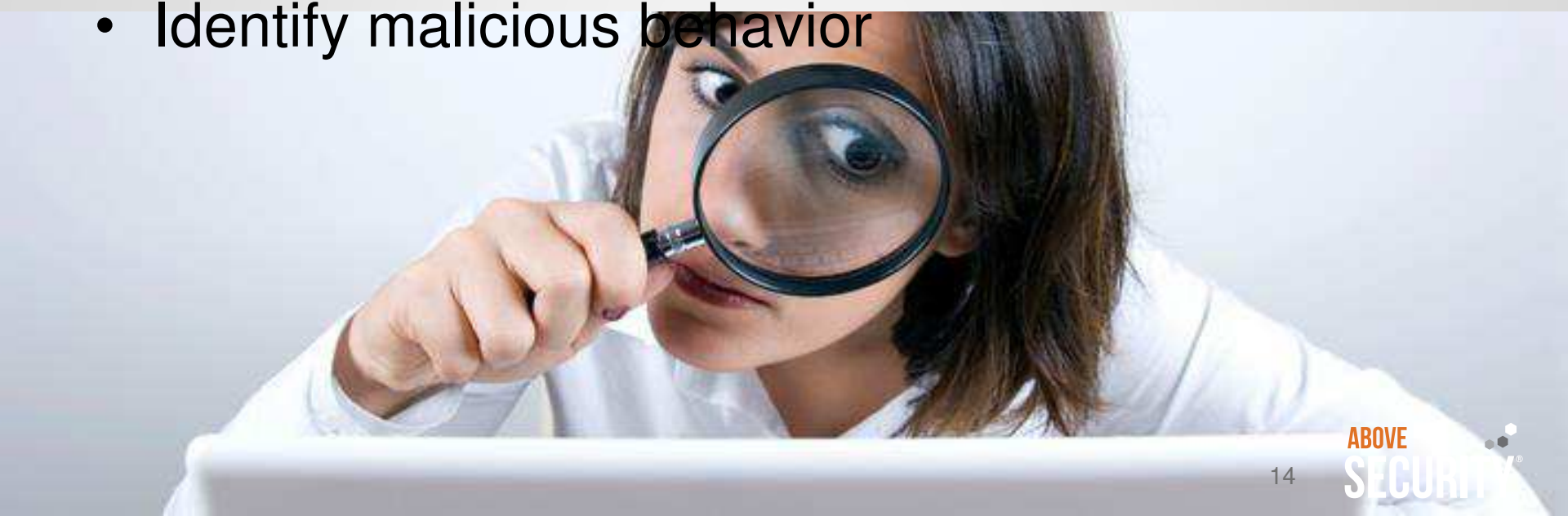
THE “PASSING THE BUCK” MODEL

Managed Security Service without proper integration	
Logging	Managed by Managed Security Service Provider (MSSP)
Alerting	Sent by MSSP to operations, and typically ignored by operations
Processes	Delegated, internal processes not developed
Reporting	Provided by MSSP, but typically no real context added
Accountability	Service Level Agreement (SLA), so MSSP vendor is on the hook (not really)…

THREAT MANAGEMENT GOALS

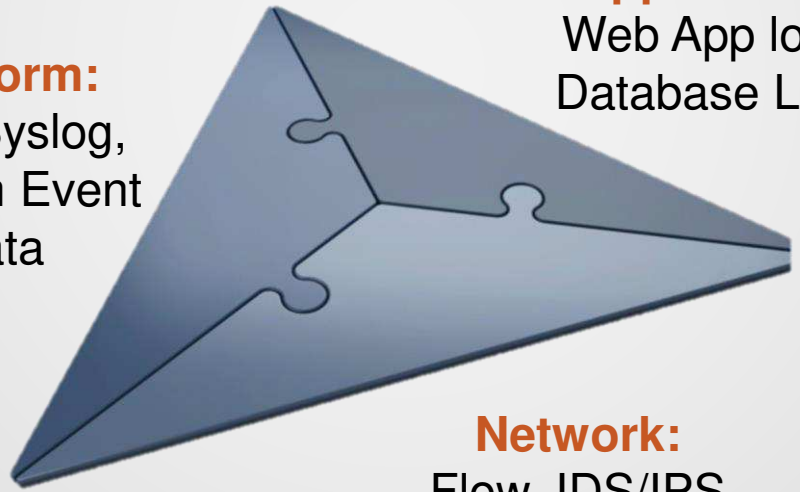
THREAT MANAGEMENT GOALS

- Identify malicious content (stationary and mobile)
- Identify malicious behavior



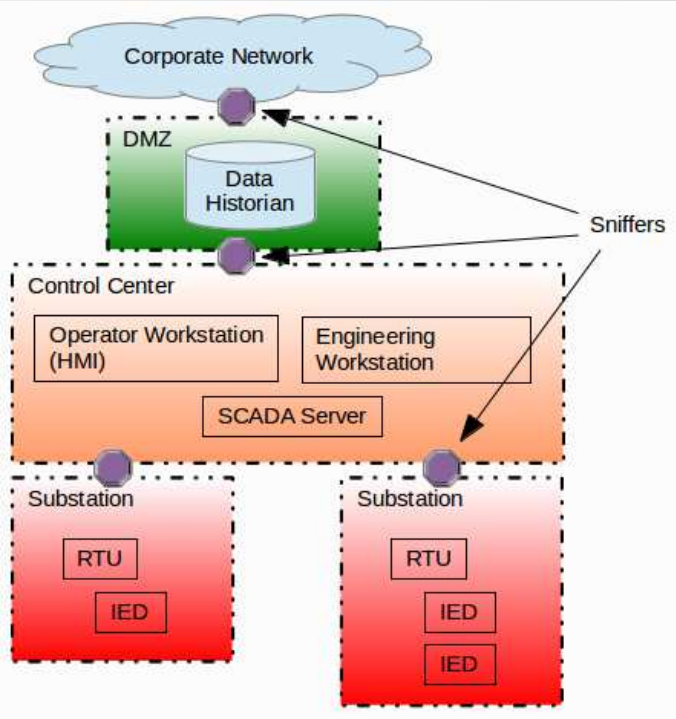
THREAT MANAGEMENT GOALS

- Ensure that the content detection occurs for all architectural layers



THREAT MANAGEMENT GOALS

- Ensure appropriate controls are in place between different security domains, or zones within the environment.



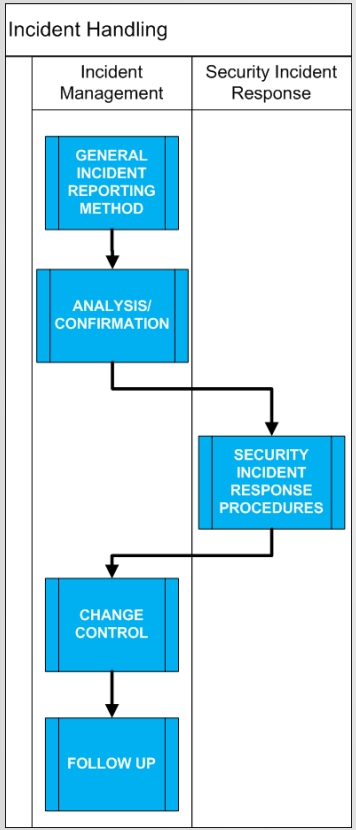
THREAT MANAGEMENT GOALS

- Triage the alert for priority and context

THREAT MANAGEMENT GOALS

- Ensure that activities indicative of an attack are escalated, assigned to the appropriate resource within the environment, and tracked

THREAT MANAGEMENT GOALS



- Provide a proper handoff to incident handling and response team(s)
- Tracking is very important, especially if the incident is beyond the knowledge of the operations team

ABOVE SECURITY

TRAITS OF A SUCCESSFUL THREAT MONITORING PROGRAM

SUCCESSFUL THREAT MANAGEMENT

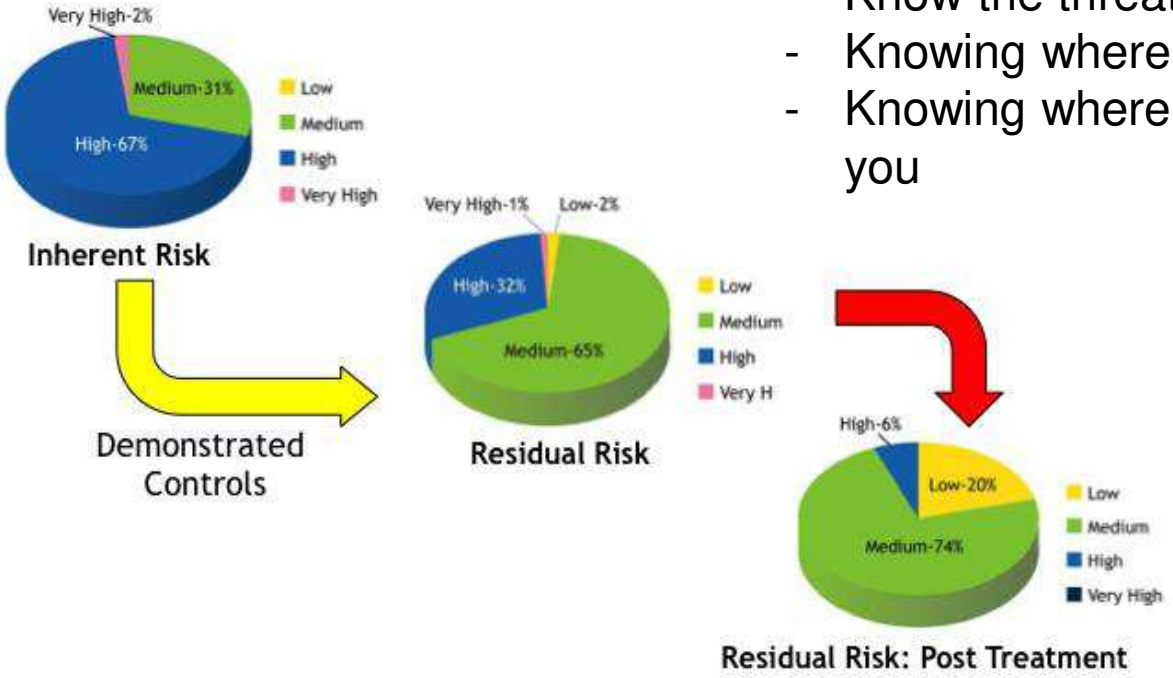
ID	Name	Address	Class	CIA
23176	External-Mail	10.10.10.10	Network: Server device	H H VH
20216	web1.acme.com	10.2.7.136	Network: Server device	M M VH
20215	fin01.acme.com	10.2.7.116	Network: Server device	VH VH VH
20214	lab2.acme.com	10.2.7.113	Network: Server device	M M VH
20217	web2.acme.com	10.2.7.137	Network: Server device	M M VH
20218	web3.acme.com	10.2.7.131	Network: Server device	M M VH
20219	act1.acme.com	10.2.7.125	Network: Server device	H H VH
20209	act2.acme.com	10.1.40.59	Network: Server device	H M VH
20198	prn1.acme.com	10.2.7.149	Network: Server device	M M VH
20193	fil1.acme.com	10.2.7.73	Network: Server device	H H VH
20197	fil3.acme.com	10.2.7.54	Network: Server device	H H VH

1. Asset/data classification
   - Asset classification not only gives the ability to create context during threat management, but also to have the ability to group these assets and providing reporting at a higher level.

SUCCESSFUL THREAT MANAGEMENT

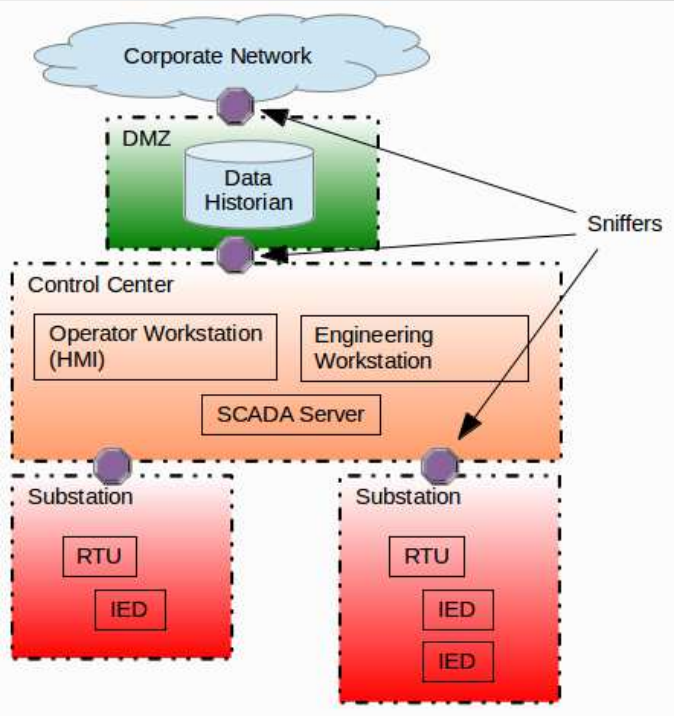
2. Threat and risk

- Know the threats that can affect you
- Knowing where your vulnerabilities are
- Knowing where your controls are failing you



SUCCESSFUL THREAT MANAGEMENT

3. Network zoning
   - Network zoning is the logical and sometimes physical segregation of parts of the network based on their security value.
   - Zones may be broken out in different trust levels.
   - Having proper zoning indicates that there's a good understanding of the network security requirements
   - Threat monitoring can scale starting with the secure zones first.

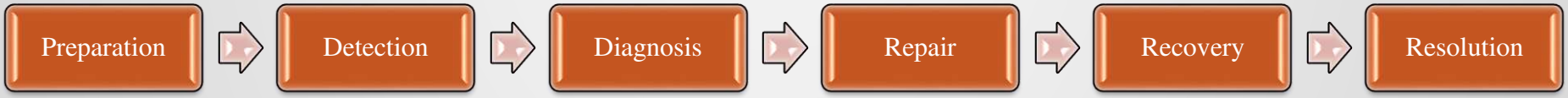


ABOVE SECURITY

SUCCESSFUL THREAT MANAGEMENT

4. Incident response capabilities
   - Organizations that know how to handle typical IT events, have a higher likelihood of being able to handle security events.

IT Incident Management Methodology



ABOVE SECURITY

SUCCESSFUL THREAT MANAGEMENT

4. Incident response capabilities

Security Incident Management Process

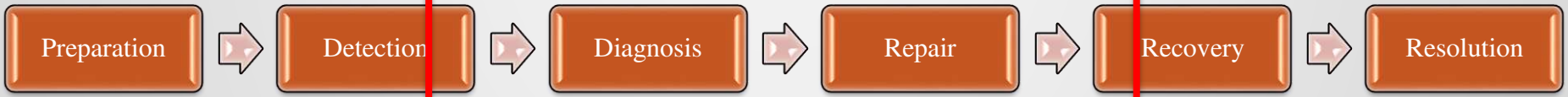
– Security incidents require more effort over a shorter amount of time to achieve containment.

SUCCESSFUL THREAT MANAGEMENT

4. Incident response capabilities

Security Incident Management Process

IT Incident Management Methodology



ABOVE SECURITY

GATHERING REQUIREMENTS

GATHERING REQUIREMENTS

- Identify the goals
- Define requirements:
    - Service
    - Reporting
    - Technical (toolset)

GATHERING REQUIREMENTS: SERVICE

WHO

- Architect
- Management
  - Security
  - Operational

WHAT

- Identify if the existing controls will provide the visibility to detect threats
- Define whether the organization be able to handle the service outputs
- Will operational teams be leveraged
- Define Service Levels/Service Flow

GATHERING REQUIREMENTS: SERVICE

WHO

- Information security staff
- Operational staff

WHAT

- Is Ad hoc reporting a requirement?
- What data is necessary for:
  - Internal Departmental Reports
  - Executive Reporting
  - Compliance/Audit Reporting
- Can the reports be generated with existing set of data sources

GATHERING REQUIREMENTS: SERVICE

WHO

- Information security staff
- Operational staff

WHAT

- Data Source Compatibility
  - (FW, IPS, AV, custom)
- Remote data collection
  - Encryption requirements
  - Threat identification
  - Correlation
  - Service Integration
  - Alerting
  - Integrated Alerting
  - Integrated Ticketing

SECURITY EVENT TICKET

Source:
Network Zone:
Ticket Identifier:
Short Description:
Initial Diagnosis:
Traffic Flow Details:
Traffic Correlations:
Time Stamps:
User:
Department:
Impacted device type specification:
What security attributes could be impacted:
Asset Classification Rating:
Containment Recommendations:

Typical data that should be in a security event ticket

ALIGN AND INTEGRATE AS PART OF DETECTION AND ANALYSIS

- Integrate detection in help desk processes
- Start to integrate information security tasks into day-to-day processes
- Engage security analysts to aid in security incidents
- Begin cross-training all analysts in handling security incidents

CONCLUSION

A well designed threat management service is not built only on technology. But rather built on understanding what your organizations' business and security requirements are, prior to deploying a threat management service.

THANK YOU

Questions?

ABOVE SECURITY®

Contact Information:
Patrick M. Hayes
Managing Director
817-876-5288
patrick.hayes@abovesecurity.com
www.abovesecurity.com