RSAConference2019
San Francisco | March 4–8 | Moscone Center

SESSION ID: STR-F03

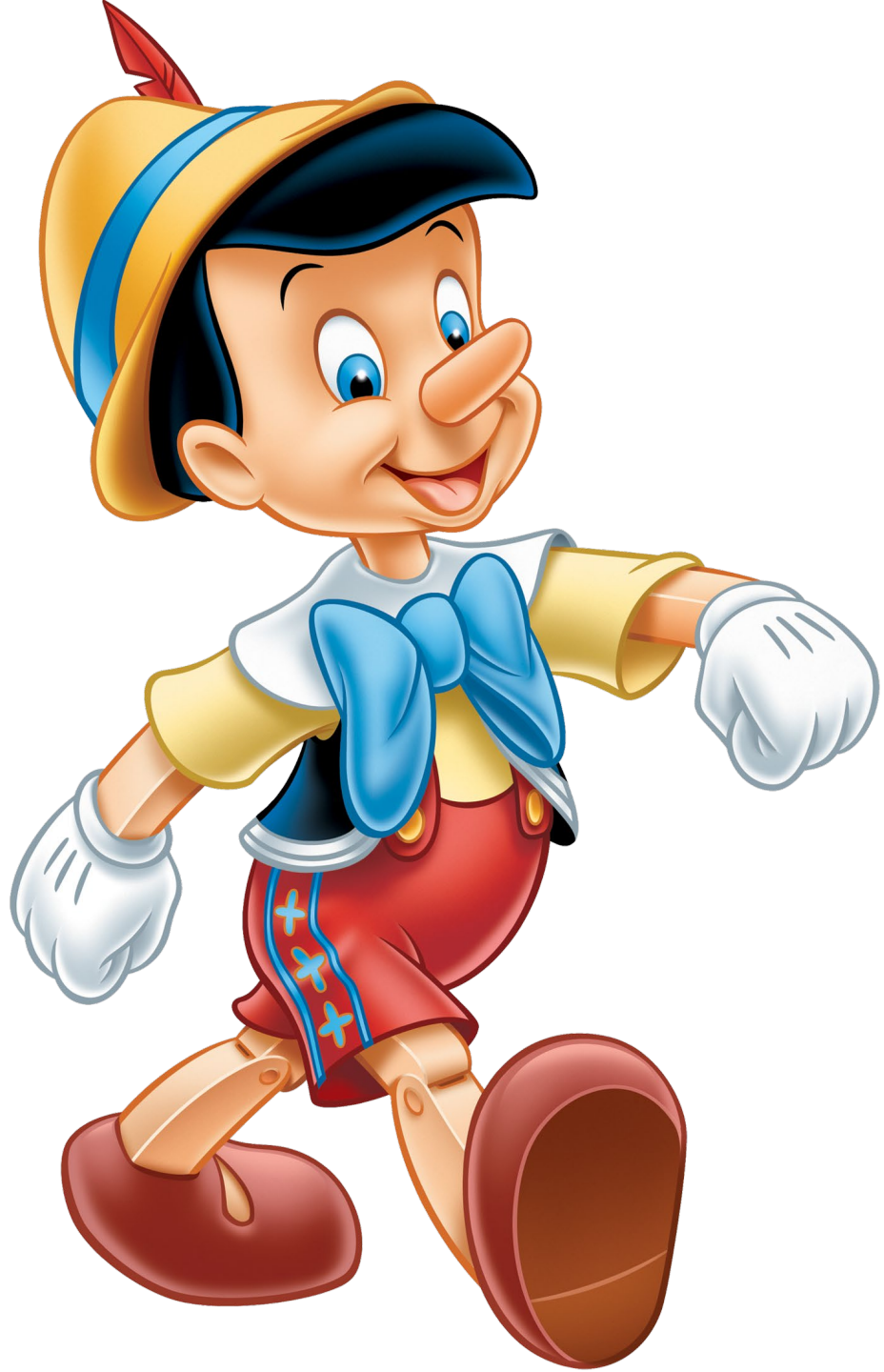
10 Lies you Tell your Security Vendors – And what to do instead

Michael Adler

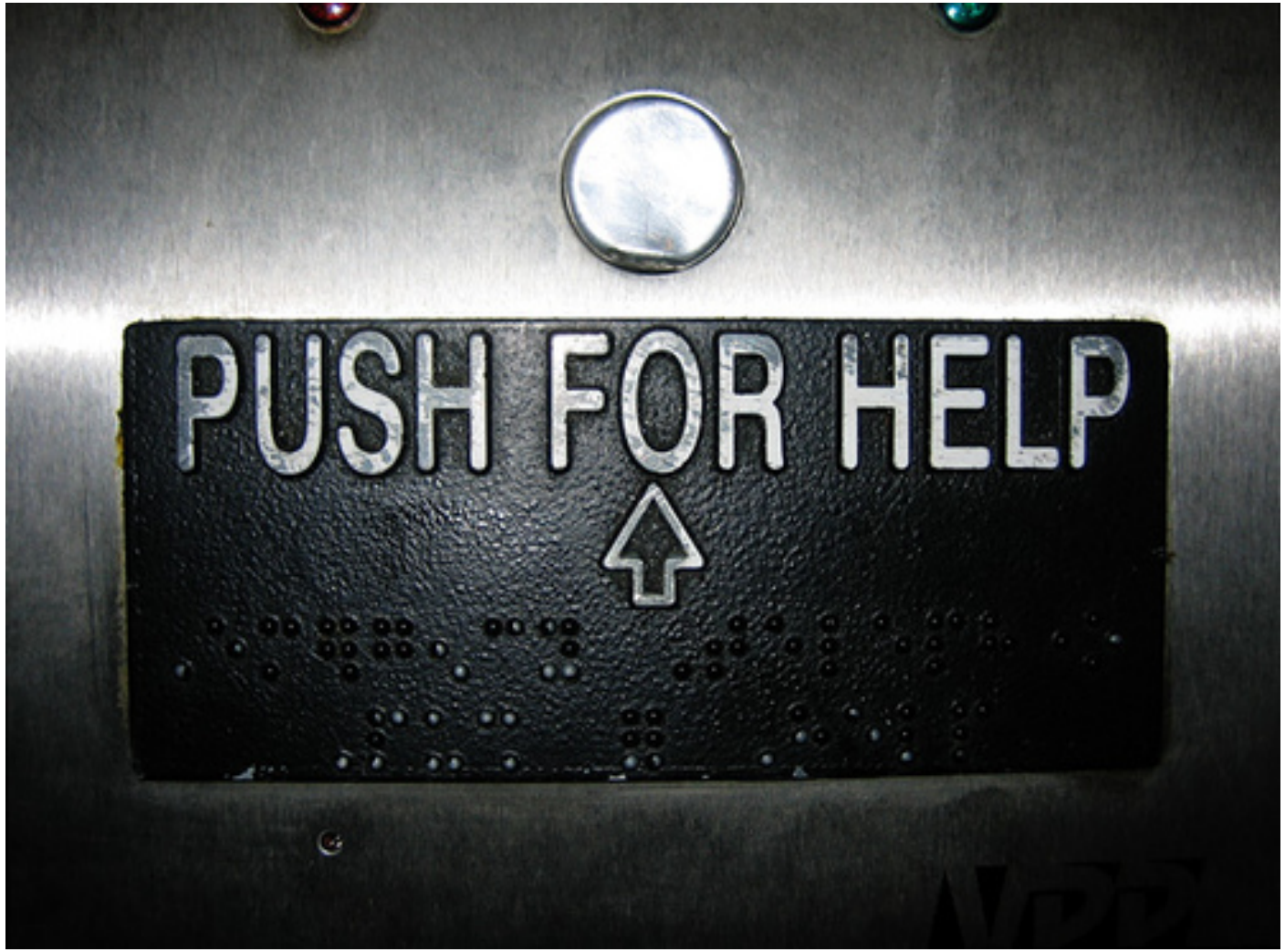
VP, Products
RSA

Who am I?

- 15 Years Building and Implementing Security Products
  - IMLogic – Secure Private and Public Instant Messaging
  - Symantec – Email Gateways, Endpoint, Mobile
  - RSA – Advanced Threat Detection and Response
- Implementations at Enterprises of all sizes
  - 500 employee companies
  - 400k employee companies
- Not only on the Vendor side, but as a customer as well



Maybe Vendors Can Help?



#1

" We understand our needs and our environment and just need you to tell us what your product does."

Setting Context – Take time to

- Explain the environment – Physical and Organizational
- Explain the challenges and needs – What are the problems you are looking to solve?
- Ask Vendors to describe their solution, not their product.

#1

~~*“ We understand our needs and our environment and just need you to tell us what your product does.”*~~

“Here is our environment, we have a problem with X. How do you help your customers solve this problem?”

#2

"We know our security requirements but can't share them."

Product Security Requirements

- There are organizational requirements –
  - Everyone has them
  - Be honest with them up front.

- We are transitioning workloads to _____
  - Does your solution allow to be run in the appropriate ways?
- We restrict internet access for security tools
  - What are the impacts?
- We require SLAs for included product security fixes
- We require the following certifications

#2

~~*"We know our security requirements but can't share them."*~~

"These are the certifications and security requirements required to operate in our environment, do you or can you meet these?"

#3

"All of these features are required to qualify for the RFP."

Current Situation	We are currently looking at upgrading our existing SIEM solution by the end of June 2019. The current SIEM solution handles 75,000 events per second (EPS) although it is likely that this will increase as we review the SIEM capability, log sources, and data enrichment in the future.

Area	Question		Answer	R
Data Collection - Cloud			Yes, RSA NetWitness Platform (NWP) you can deploy RSA NetWitness Logs within private, public or hybrid cloud architectures. In addition, you can easily monitor Office 365 environments or Salesforce applications. Modular components can be deployed virtually and within public clouds, including AWS and Amazon, to enable visibility across complex cloud environments. Platform capabilities in a cloud environment include:	
	Alerting	Does your solution automatically generate alerts when it perceives a threat?	Yes based on the enabled Network-rules / App-rules on the log/packet decoders & correlation rules on ESA	
		What type of alerting mechanism is used (such as emails, auto-generation of incidents, SMS and push notifications etc.)?	RSA NetWitness Platform supports real time notifications triggered by ESA correlation rules. These consist of syslog, SNMP, SMTP for email, or any Restful call or Script.	
	Prioritization		The RSA NetWitness Platform (NWP) includes native capabilities to support analysts and threat hunters involved in the IR process with a full set	
		Orchestration and Automation	RSA NetWitness® Orchestrator using the Demisto technology has a supported Interoperabilities provide such features in which the basic tasks of incident response are automated, making your analysts more efficient and effective. In addition, interactive investigations are supported, enabling collaboration, historical review, and real-time documentation of all actions.	
		Data Retention	RSA NetWitness platform has two main models for storing the collected data from logs, networks or endpoint or netflow either as a raw-log retention on logdecoders/decoders or a long-term data retention starting from 1-year+ on the Archivers. RSA NetWitness Archiver appliance – Provide tiered options for long-term retention including hot, warm and cold dependent on a customer's compliance requirements. It enables long-term archiving of logs by indexing and compressing log data and sending it to Archiving storage. The archiving storage is then optimized for long term data retention and compliance reporting. Archiver stores raw logs and log meta for long-term retention.. The hot tier can utilize high performance storage with options to age older data to a lower, warm tier, and, ultimately to cold archived storage. Data can be aged between tiers based on size or age. This data can be accessed/restored using our Workbench service and allows selective data to be restored and searched or reported on. An RSA NetWitness Platform user with the role of Administrator can configure NetWitness Platform to ensure that sensitive data has been removed after a specific retention period, regardless of system ingest rate. For instance, the policy might be to keep packets (both raw data and meta data) for no more than 24 hours, and to keep some logs (both raw data and meta data) for up to seven days. If sensitive data makes its way into another database on the Reporting Engine, Malware Analysis, Event Stream Analysis, and NetWitness Servers, data retention can be managed there as well. The administrator needs to set up each service individually across all NetWitness Platform components (except Event Stream Analysis) based on policy and data privacy laws.	
Data Collection - On premise				
Software Defined Networks				
Deployment model	Categorisation			
	Dashboard / Forensic Analysis			
Multiple SIEMS		Does your solution allow for the storage data for a pre-determined length of time?	An RSA NetWitness platform user can schedule a recurring job for Decoder, Log Decoder, and Concentrator services in NetWitness Platform to check if data is ready to be removed. The Data Retention Scheduler provides a means to configure basic scheduling (see below), and advanced	
		Integration	Please indicate if your solution has the capability of integrating with the following security tooling and DLG solutions:	Please answer Y or N to the following:
			AWS	Yes
			Azure	Yes
			Office 365	Yes
	Phishing		Email (Symantec cloud; Outlook 365)	Yes for Symantec Brightmail gateway & MS Office 365
			Email Data Loss Protection (IronPort)	Yes
			Data Loss Protection (Lumension & Bluecoat)	Yes
	Event Correla		Vulnerability management (Qualys)	Yes, through Archer module - also can be added as a feed.
			Endpoint protection (Sepm, Scep, Sophos)	Yes
			File Integrity Monitoring (Tripwire)	Yes
			Identity Access Management/PAM (CyberArk)	Yes
	Correlation R		Active Directory	Yes
				VMware AppDefense VMware vCenter Server VMware ESX/ESXi VMware NSX

#3

~~*"All of these features are required to qualify for the RFP."*~~

"Our Needs are labeled Must, Shall, Optional and also labeled with Priority 1-3."

A well formed RFP Example

Area	Need	Requirement	Priority
Log management	We have requirements around access to information for different organizations and need to be able to keep Event and Log Data Segregated for separate partied.	The Solution ***Shall*** enforce data segregation such that users in certain organizations do not have access to another organizations data. The solution ***may*** segregate at storage time	P2

#4

“I can POC this next week”

Can you really setup a product next week?

If you could, do you know what success would look like?

#4

~~*"I can POC this next week"*~~

"How long does it take to start a successful POC? What do you need from us?"

#5

“Budget isn’t a factor in our decision”


DEPTH
GAUGE
90 ft

#5

~~*"Budget isn't a factor in our decision"*~~

"We will purchase the tool that gives us the greatest value"

Or

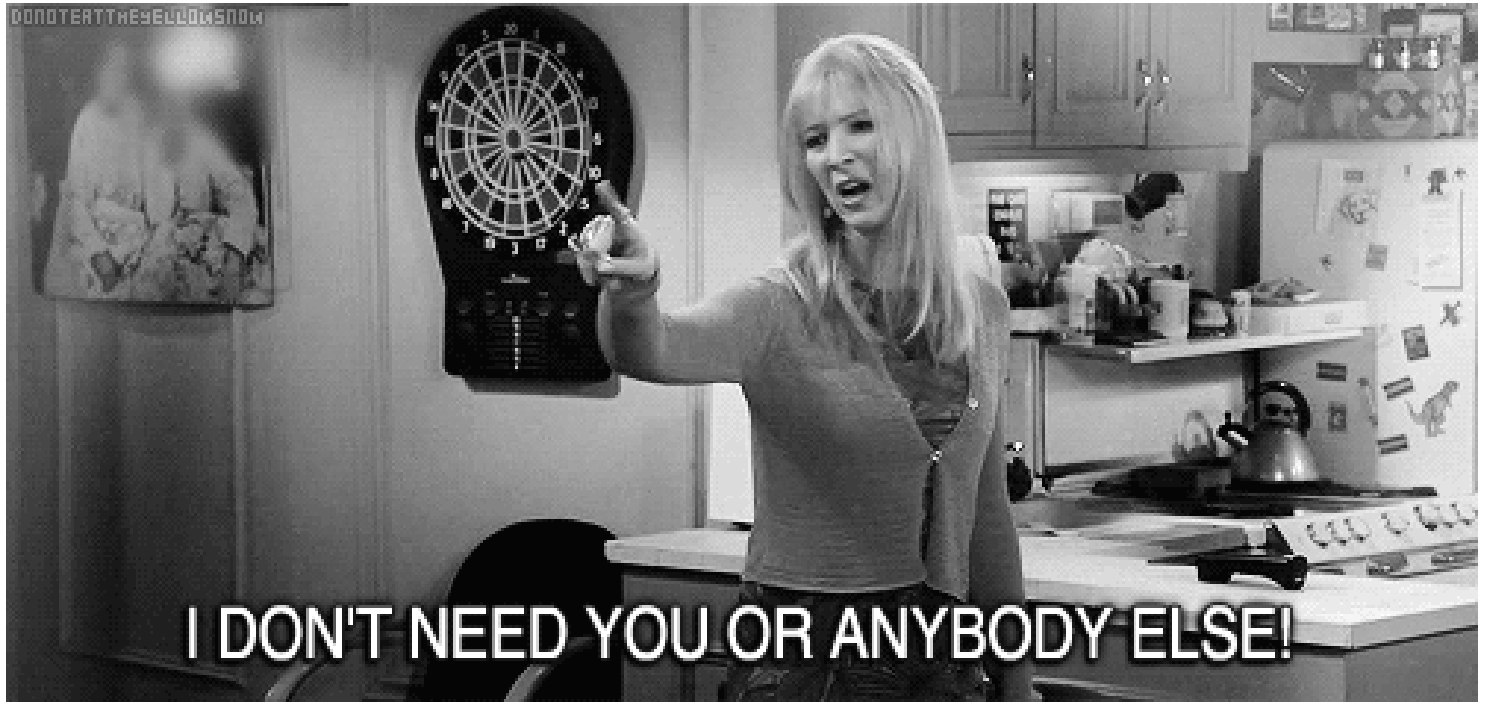
" We are looking for the greatest value at the best price"

#6

“We don’t need training or professional services”

Or

“We will do the installation ourselves”


DONOTEATTHEYELLOWSNOW
I DON'T NEED YOU OR ANYBODY ELSE!

#6

~~*"We don't need training or professional services"*~~

~~*Or*~~

~~*"We will do the installation ourselves"*~~

"What value do I receive if I use your professional services?"
Or
"What training is required to be successful with the product?"

Get the right kind of help.

- Implementations need quick strong wins
- Getting started correctly is critical
  - How many times has the start of a project determined its success?
- What training will users of the solution need to get the most out of it?
- Services starts training but won't complete it

#7

"We can plan/budget for increased usage/growth later"

Budget for the Future

- Does any company really plan to shrink?
- You do need to plan for a full deployment
- You should plan for future expansion
- Design and Understand the architecture now and in the future
  - Negotiate the future impacts of growth

#7

~~*"We can plan/budget for increased usage/growth later"*~~

"How do we design for increased usage/growth now and can we understand those costs?"

#8

“We can get this through purchasing/legal”

Getting the Purchase through…

- Are there any Procurement teams or Lawyers in the Room?
- Let your vendor help, vendors do this all the time….
  - Protect your internal brand, let the vendors track the individual pieces
- Read the legal agreements – There shouldn't be any surprises for either side.

#8

~~*“We can get this through purchasing/legal”*~~

“Can you help me get this through purchasing/legal?”

#9

“I need references to make a decision”

References

- What are reference checks for?
  - Confirm what you should have learned through your own process
  - Look for concerns that you won't be able to see in your evaluation process
    - How does the product scale?
    - How long did the rollout take?
    - How well was the training received?

#9

~~*"I need references to make a decision"*~~

"We have made a decision, but I would like to hear from references to validate our decision"

#10

"We don't plan on upgrading regularly"

Or

"You need to help us with that upgrade"

#10

~~*"We don't plan on upgrading regularly"*~~

~~*Or*~~

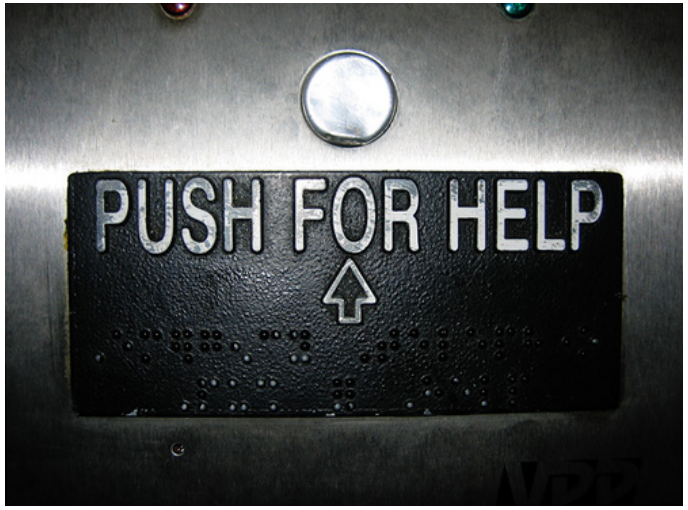
~~*"You need to help us with that upgrade"*~~

"What costs should I expect to perform an upgrade?"

10 Things

- Context and needs
- Non-Functional requirements and certifications
- Write a real/good RFP
- Prioritize success over fast RFP
- Know your budget and how it impacts your purchase
- Get the right kind of help
- Plan for growth
- Let vendors help with purchasing and legal
- Use references to validate decisions not make decisions
- Plan for upgrades

Maybe Vendors Can Help?



*Not all Vendors or representatives of Vendors will behave perfectly all of the time……

In Summary

- Security Vendors Want to Help
  - Look to identify those who you can partner with
  - Don’t look at purchases as transactions
- Be honest with your vendors
  - Vendors do a better job when they really understand needs and what success looks like
  - Don’t be embarrassed or hide information. Vendors have seen it all.
- Don’t try to solve every problem with a single solution
  - Find the right mix of products that provide solutions to the problems you actually have
  - Understand the organizational complexities of deploying a security solution

In the next 90 days

- Document your real needs in a format that you can share with vendors
- Document non-functional requirements for any security solution that you bring into the environment
- Review your RFP procedures and templates
- Understand your staffing, training, and skills strategies to prepare for your next purchase

RSAConference2019

Thank You