IMPROVING SECURITY METRICS

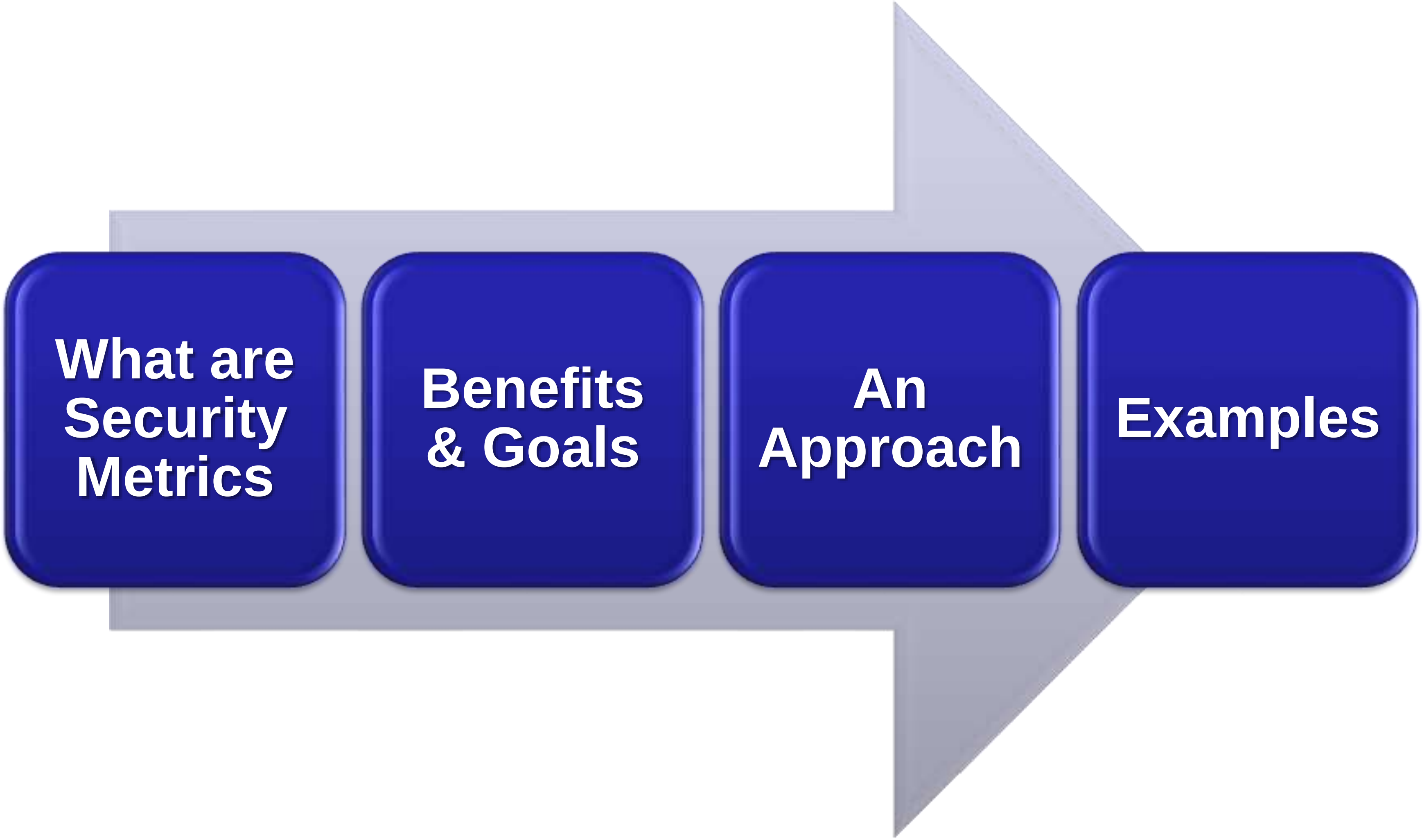
6 May 2016

SPEEDY GROUP
HOLDINGS CORP
INFORMATION SECURITY
Protect – Detect – Advise – Respond

Ron Shuck, CISSP, CISM, CISA, CPP, GCIA, GCED
Director Information Security

ISSA™
Information Systems Security Association
CENTRAL PLAINS CHAPTER

Agenda



What are Security Metrics

Benefits & Goals

An Approach

Examples

Security Metrics

An ongoing collection of measurements to assess security performance

Producing reliable and effective information security metrics is not easy

Security Metrics

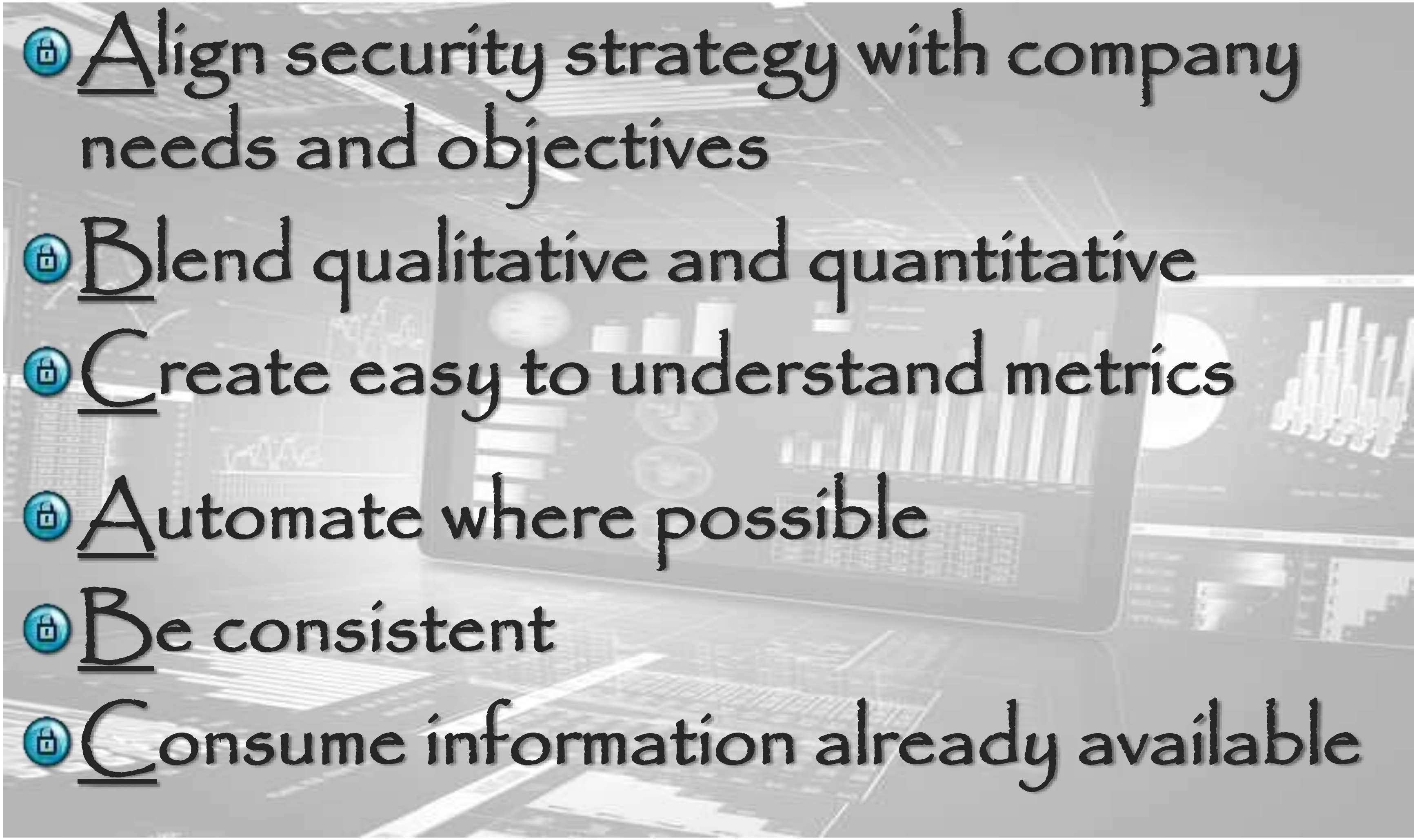
- **Security Metrics Should Measure**
  - – Implementation
  - – Effectiveness
  - – Impact

- **Measure Repeatable Processes**
  - – Contextually specific
  - – Consistently measured
  - – Cheap to produce

Benefits

- Improves Effectiveness of Security Strategies
- Increases Accountability
- Demonstrates Compliance
- Drives Performance Improvement

Goals – ABC's

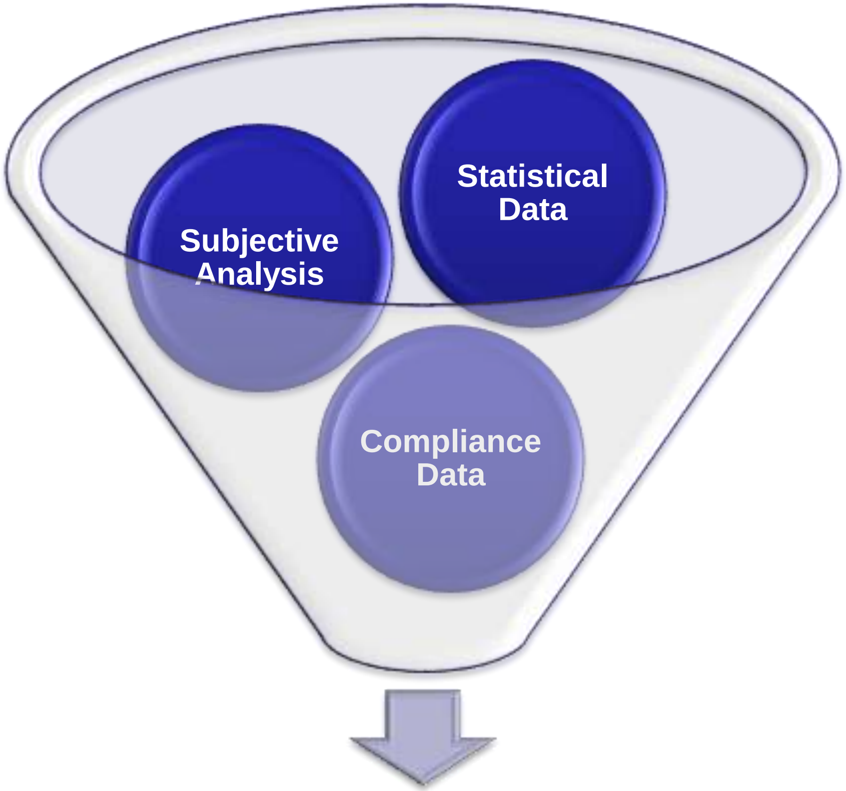


- Align security strategy with company needs and objectives
- Blend qualitative and quantitative
- Create easy to understand metrics
- Automate where possible
- Be consistent
- Consume information already available

Approach

One Metric to Rule Them All

Metric Composition


Subjective Analysis

Statistical Data

Compliance Data

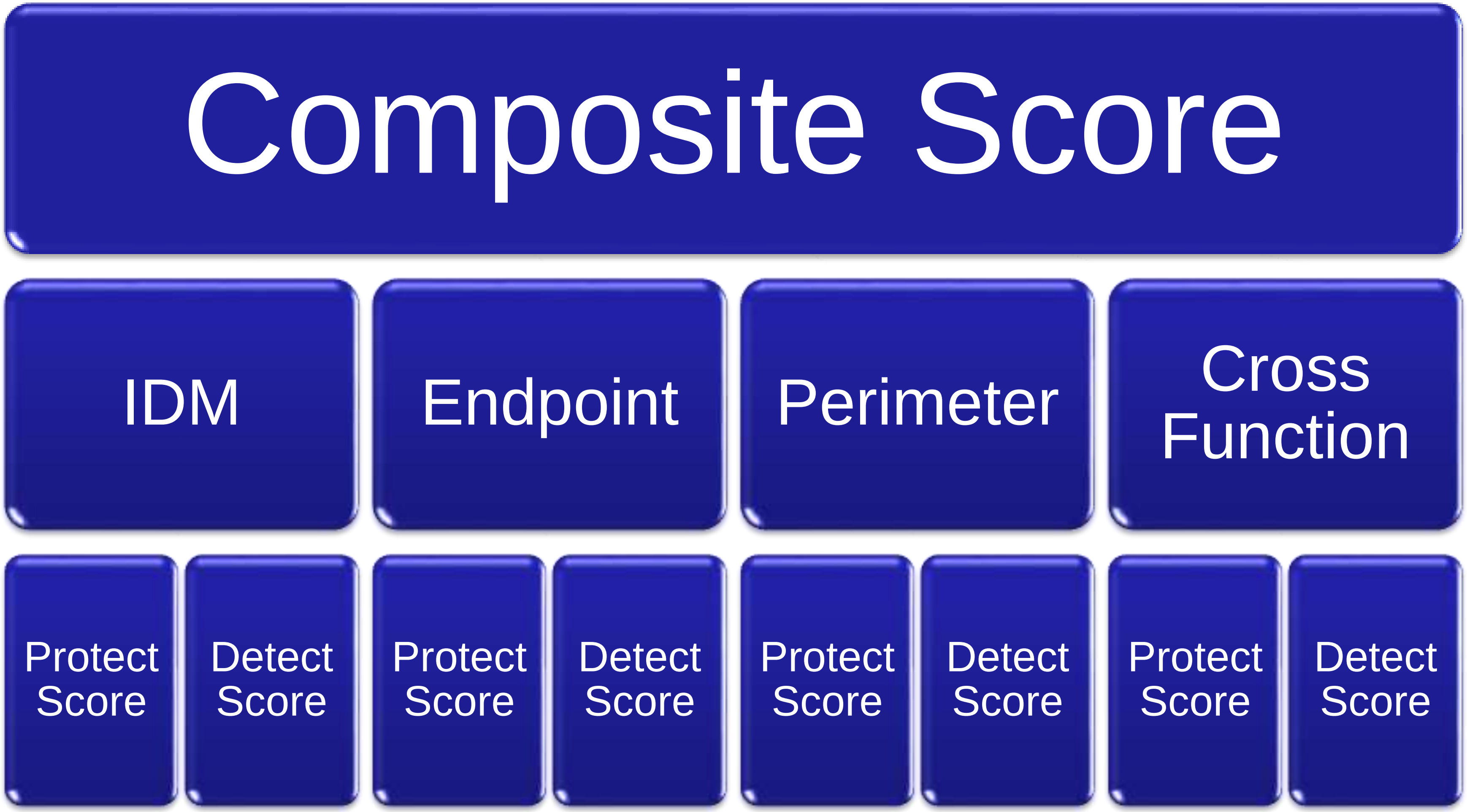
Composite Score

Protect & Detect

Outcome Based / Qualitative

Activity Based / Quantitative

Metric Composition



Composite Score

IDM

Endpoint

Perimeter

Cross Function

Protect Score

Detect Score

Protect Score

Detect Score

Protect Score

Detect Score

Protect Score

Detect Score

Metric Composition

Protect (Outcome Based / Qualitative)

- Completeness / effectiveness of solutions in place
- Alignment with business objectives & roadmap
- Compliance metrics if available (e.g. percent up to date or installed)

Detect (Activity Based / Quantitative)

- Event metrics from solutions
- Based on alerts that were not blocked
- Weighted by severity of alert

Identity & Access Management

Protect (Outcome Based / Qualitative)

- Two Factor Authentication
- Account Provisioning Process & Administration
- Administrative Access Controls
- Access Certifications

Detect (Activity Based / Quantitative)

- Failed Login / Account Lockout Events
- 3rd Party Access

Endpoint Protection

Protect (Outcome Based / Qualitative)

- Host-based Intrusion Prevention System (HIPS)
- Malware Protection (Antivirus, AntiSPAM)
- Advanced Malware Protection (AMP)
- Whole Disk Encryption

Detect (Activity Based / Quantitative)

- Endpoint Events

Perimeter Defense

Protect (Outcome Based / Qualitative)

- Firewalls
- Network Intrusion Prevention Systems (IPS)
- Security Information & Event Management (SIEM)
- Advanced Persistent Threat Protection (APT)
- Web Proxy & Web Application Firewall (WAF)
- Network Behavior Analysis (NBA) & Visibility

Detect (Activity Based / Quantitative)

- Perimeter Events (IPS, FireAMP, Proxy, WAF)

Cross Functional Security Services

Protect (Outcome Based / Qualitative)

- ➢ Risk Assessment
- ➢ Vulnerability Assessment
- ➢ Incident Response

Detect (Activity Based / Quantitative)

- ➢ Risk Levels (Vulnerability & Risk Assessment)
- ➢ Vulnerability Scan & Patch Statistics
- ➢ Median-time-to-remediation (MTTR)

Information Security Level Indicators

81% - 100%

61% - 80%

TARGET

41% - 60%

21% - 40%

< 20%

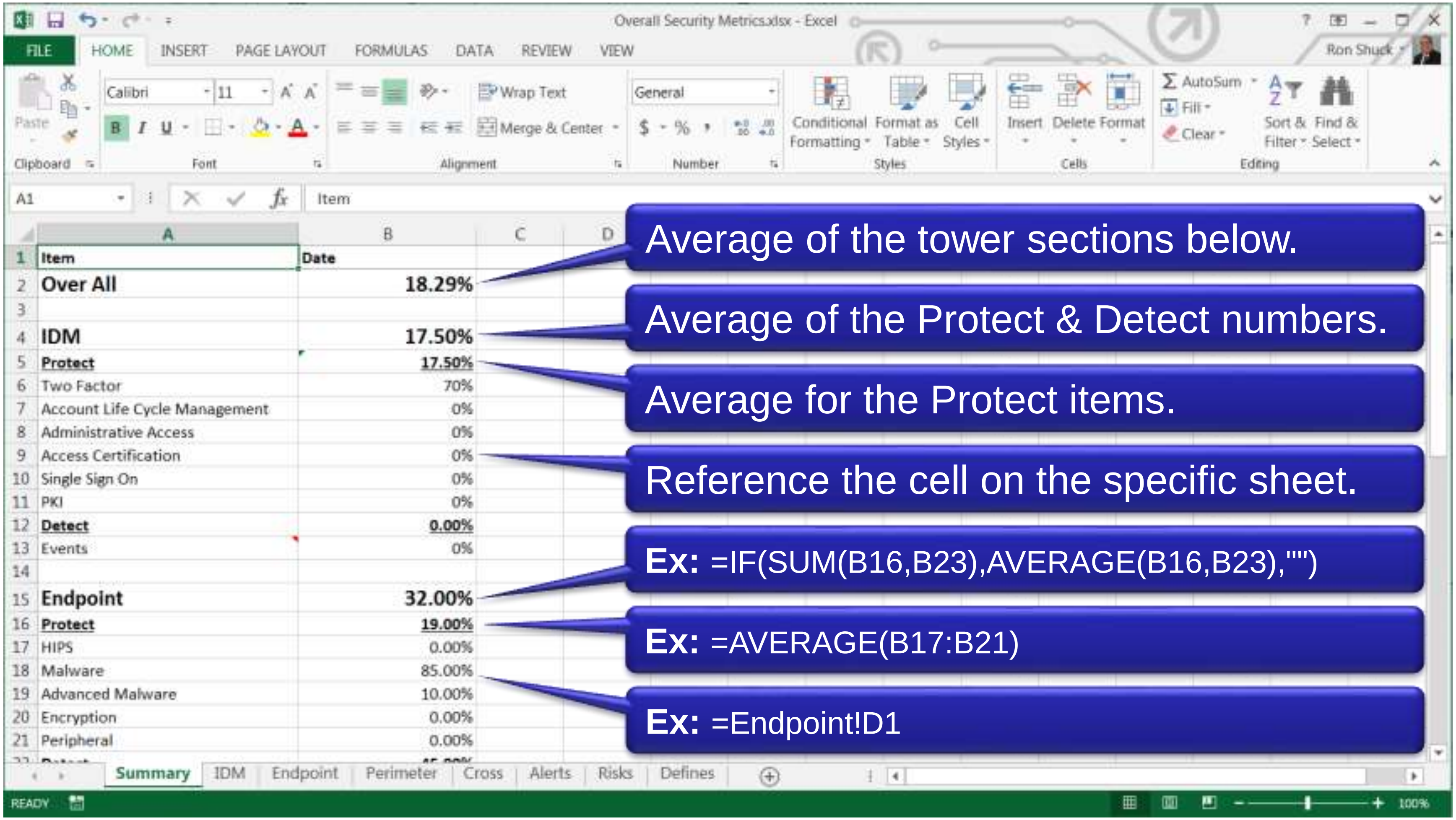
EXAMPLE

Example – Detect Tips

- **H/IPS, WAF, AV/AMP**
  - Blocked / Alerts (weighted by severity)
- **Firewall, Proxy**
  - Blocked / Total Packets
- **Anti-Malware**
  - Compliance (% covered)
- **Patch Management**
  - Compliance (% current)
- **Risk Assessments**
  - Mitigation Age (to target, weighted by severity)
  - Mitigation Status (weighted by severity)
- **Vulnerability Scans**
  - Mitigation Age
  - Mitigation Status
- **Incident Response**
  - MTTR / MTTD

Activity Based / Quantitative

Example – Summary



A1 | *fx* | Item

	A	B
1	**Item**	**Date**
2	**Over All**	**18.29%**
3		
4	**IDM**	**17.50%**
5	**Protect**	**17.50%**
6	Two Factor	70%
7	Account Life Cycle Management	0%
8	Administrative Access	0%
9	Access Certification	0%
10	Single Sign On	0%
11	PKI	0%
12	**Detect**	**0.00%**
13	Events	0%
14		
15	**Endpoint**	**32.00%**
16	**Protect**	**19.00%**
17	HIPS	0.00%
18	Malware	85.00%
19	Advanced Malware	10.00%
20	Encryption	0.00%
21	Peripheral	0.00%

Average of the tower sections below.

Average of the Protect & Detect numbers.

Average for the Protect items.

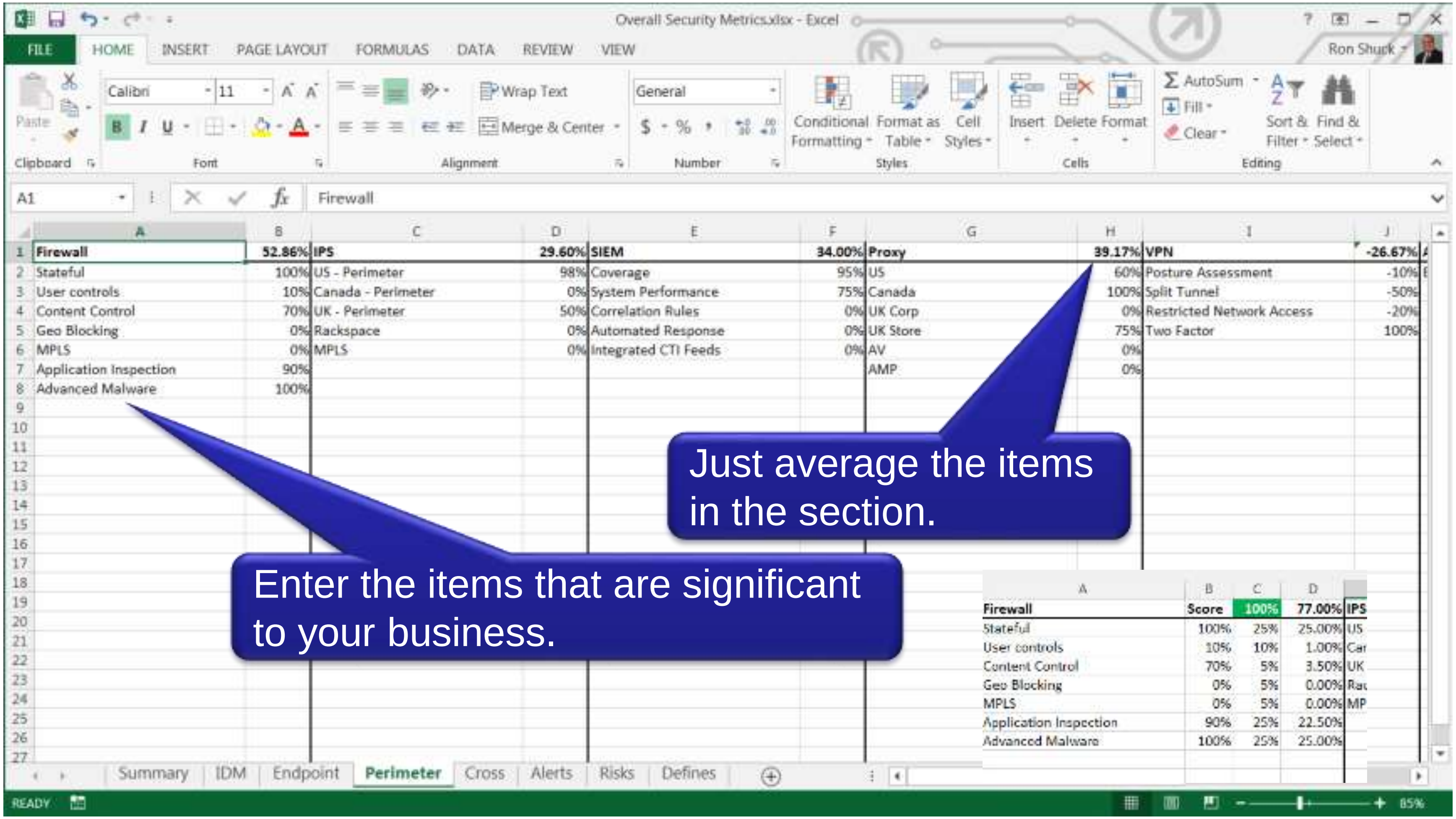
Reference the cell on the specific sheet.

Ex: =IF(SUM(B16,B23),AVERAGE(B16,B23),"")

Ex: =AVERAGE(B17:B21)

Ex: =Endpoint!D1

Example – Protect Detail



A1: Firewall

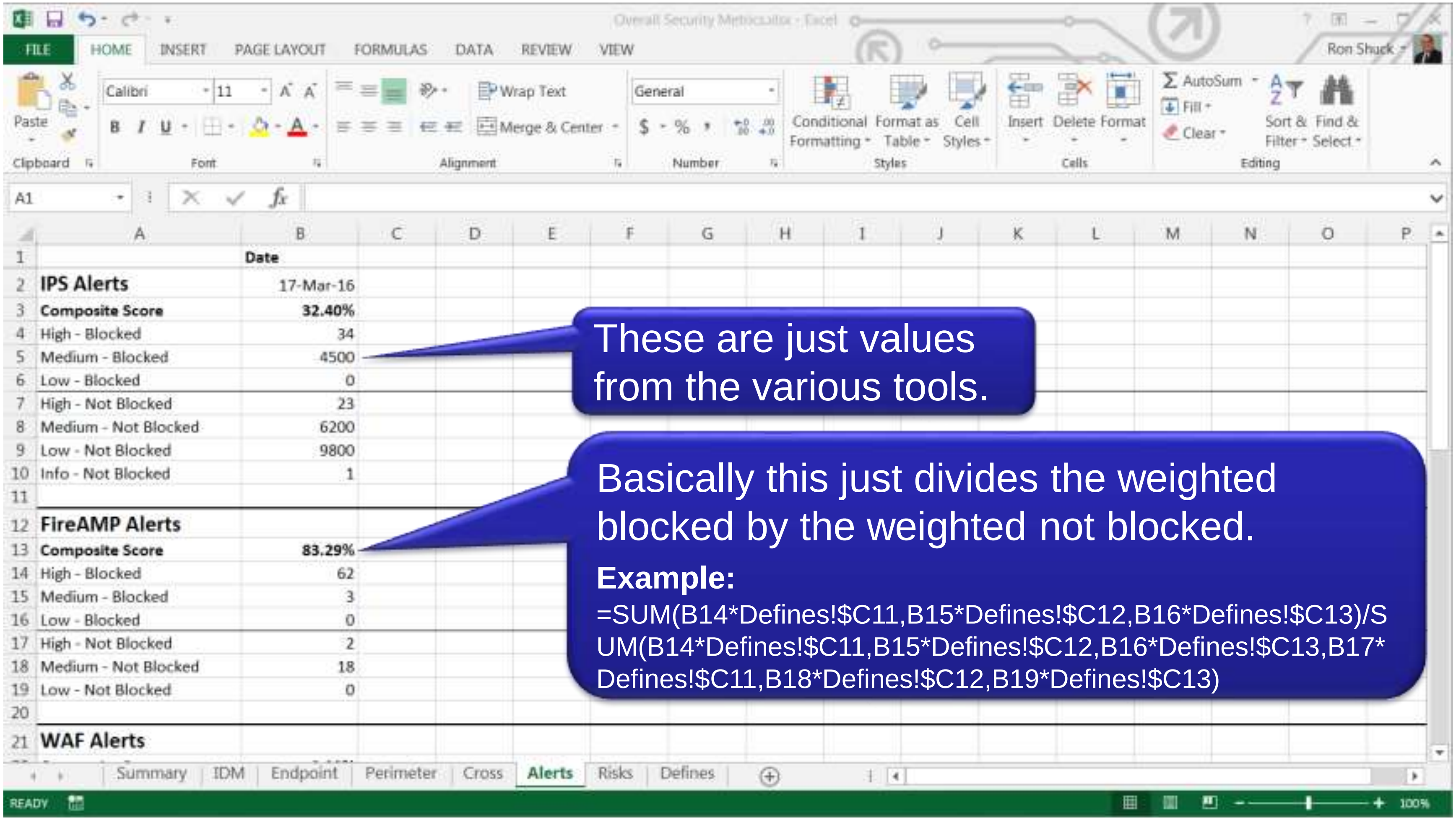
A	B	C	D	E	F	G	H	I	J
Firewall	**52.86%**	**IPS**	**29.60%**	**SIEM**	**34.00%**	**Proxy**	**39.17%**	**VPN**	**-26.67%**
Stateful	100%	US - Perimeter	98%	Coverage	95%	US	60%	Posture Assessment	-10%
User controls	10%	Canada - Perimeter	0%	System Performance	75%	Canada	100%	Split Tunnel	-50%
Content Control	70%	UK - Perimeter	50%	Correlation Rules	0%	UK Corp	0%	Restricted Network Access	-20%
Geo Blocking	0%	Rackspace	0%	Automated Response	0%	UK Store	75%	Two Factor	100%
MPLS	0%	MPLS	0%	Integrated CTI Feeds	0%	AV	0%		
Application Inspection	90%					AMP	0%		
Advanced Malware	100%								

A	B	C	D	
Firewall	**Score**	100%	**77.00%**	**IPS**
Stateful	100%	25%	25.00%	US
User controls	10%	10%	1.00%	Car
Content Control	70%	5%	3.50%	UK
Geo Blocking	0%	5%	0.00%	Rac
MPLS	0%	5%	0.00%	MP
Application Inspection	90%	25%	22.50%	
Advanced Malware	100%	25%	25.00%	

Just average the items in the section.

Enter the items that are significant to your business.

Example – Detect Detail



	A	B
1		Date
2	**IPS Alerts**	17-Mar-16
3	**Composite Score**	**32.40%**
4	High - Blocked	34
5	Medium - Blocked	4500
6	Low - Blocked	0
7	High - Not Blocked	23
8	Medium - Not Blocked	6200
9	Low - Not Blocked	9800
10	Info - Not Blocked	1
11		
12	**FireAMP Alerts**	
13	**Composite Score**	**83.29%**
14	High - Blocked	62
15	Medium - Blocked	3
16	Low - Blocked	0
17	High - Not Blocked	2
18	Medium - Not Blocked	18
19	Low - Not Blocked	0
20		
21	**WAF Alerts**	

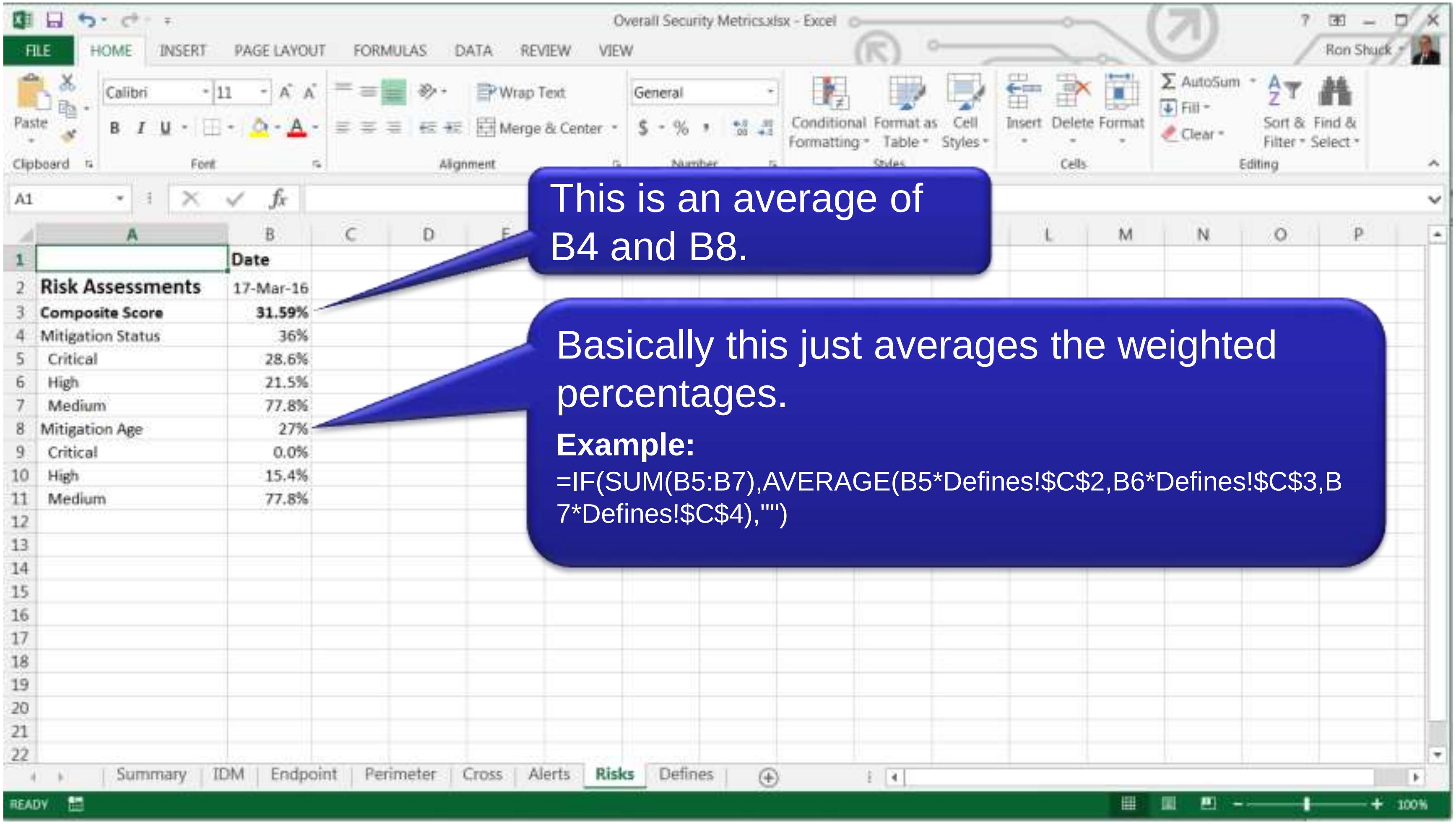
These are just values from the various tools.

Basically this just divides the weighted blocked by the weighted not blocked.

Example:

=SUM(B14*Defines!$C11,B15*Defines!$C12,B16*Defines!$C13)/SUM(B14*Defines!$C11,B15*Defines!$C12,B16*Defines!$C13,B17*Defines!$C11,B18*Defines!$C12,B19*Defines!$C13)

Example – Risk Detect Detail



	A	B
1		Date
2	Risk Assessments	17-Mar-16
3	Composite Score	31.59%
4	Mitigation Status	36%
5	Critical	28.6%
6	High	21.5%
7	Medium	77.8%
8	Mitigation Age	27%
9	Critical	0.0%
10	High	15.4%
11	Medium	77.8%

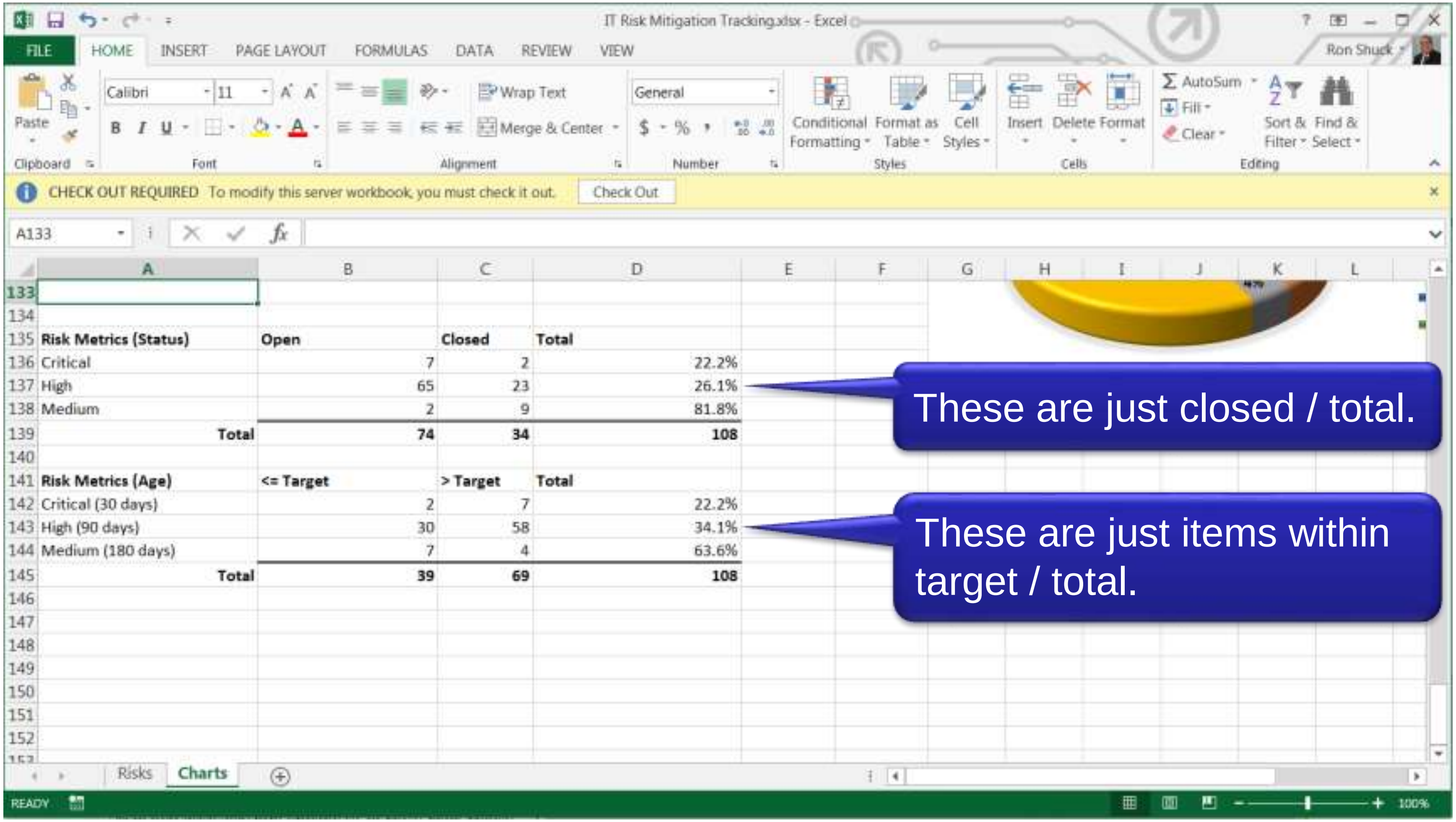
This is an average of B4 and B8.

Basically this just averages the weighted percentages.

Example:

=IF(SUM(B5:B7),AVERAGE(B5*Defines!$C$2,B6*Defines!$C$3,B7*Defines!$C$4),"")

Example – Risk Detail

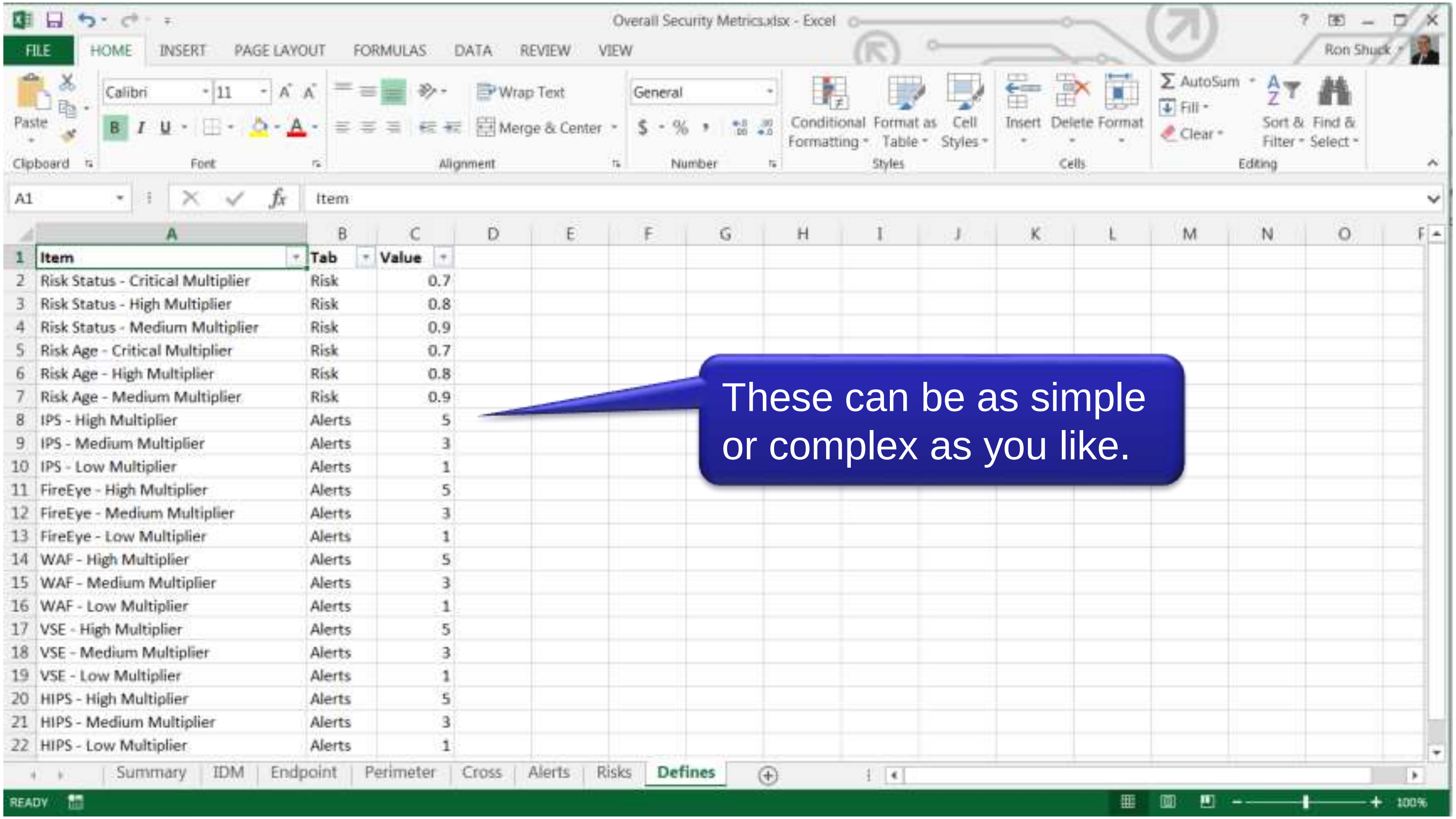


	A	B	C	D
133				
134				
135	**Risk Metrics (Status)**	**Open**	**Closed**	**Total**
136	Critical	7	2	22.2%
137	High	65	23	26.1%
138	Medium	2	9	81.8%
139	**Total**	**74**	**34**	**108**
140				
141	**Risk Metrics (Age)**	**<= Target**	**> Target**	**Total**
142	Critical (30 days)	2	7	22.2%
143	High (90 days)	30	58	34.1%
144	Medium (180 days)	7	4	63.6%
145	**Total**	**39**	**69**	**108**
146				
147				
148				
149				
150				
151				
152				

These are just closed / total.

These are just items within target / total.

Example – Defines



A1 | Item

Item	Tab	Value
Risk Status - Critical Multiplier	Risk	0.7
Risk Status - High Multiplier	Risk	0.8
Risk Status - Medium Multiplier	Risk	0.9
Risk Age - Critical Multiplier	Risk	0.7
Risk Age - High Multiplier	Risk	0.8
Risk Age - Medium Multiplier	Risk	0.9
IPS - High Multiplier	Alerts	5
IPS - Medium Multiplier	Alerts	3
IPS - Low Multiplier	Alerts	1
FireEye - High Multiplier	Alerts	5
FireEye - Medium Multiplier	Alerts	3
FireEye - Low Multiplier	Alerts	1
WAF - High Multiplier	Alerts	5
WAF - Medium Multiplier	Alerts	3
WAF - Low Multiplier	Alerts	1
VSE - High Multiplier	Alerts	5
VSE - Medium Multiplier	Alerts	3
VSE - Low Multiplier	Alerts	1
HIPS - High Multiplier	Alerts	5
HIPS - Medium Multiplier	Alerts	3
HIPS - Low Multiplier	Alerts	1

These can be as simple or complex as you like.

QUESTIONS?
CONCERNS?
COMMENTS?