

# GOHIO

*Lessons Never Learned*  
*A way through the valley*

October 2017 | Joel Fulton

splunk>



“I liken it to the very first aero-squadron, when they started with biplanes. We’re at the threshold of a new era... we are not exactly sure how combat in this new dimension of cyberspace will unfold. We only know we’re at the beginning.

“Few if any contemporary computer security controls have prevented a red team from easily accessing any information sought.

“The market does not work well enough to raise the security of computer systems at a rate fast enough to match the apparent growth in threats to systems.

“Computer intrusions, telecommunications targeting and intercept, and private-sector encryption weaknesses... account for the largest portion of economic and industrial information lost by US corporations.

“Espionage over networks can be cost-efficient, offer nearly immediate results, and target specific locations... and are insulated from risks of internationally embarrassing incidents.

“The almost obsessive persistence of serious penetrators is astonishing.”

“I almost feel like it’s the early days of flight with the Wright brothers. First of all, you need to kind of figure out that domain, and how are we going to operate and maintain within that domain. So I think it will take a period of time, and it’s going to be growing.

“Our red teams do get into most of the networks we target.

“We’ve had market failure when it comes to cybersecurity. Security doesn’t come out of voluntary actions and market forces.

“Cyber tools have enhanced the economic espionage threat, and the Intelligence Community judges the use of such tools is already a larger threat than more traditional espionage methods.

“I liken it to the very first aero-squadron, when they started with biplanes. We’re at the threshold of a new era... we are not exactly sure how combat in this new dimension of cyberspace will unfold. We only know we’re at the beginning.” - **1996**

“Few if any contemporary computer security controls have prevented a red team from easily accessing any information sought.” - **1979**

“The market does not work well enough to raise the security of computer systems at a rate fast enough to match the apparent growth in threats to systems.” - **1981**

“Computer intrusions, telecommunications targeting and intercept, and private-sector encryption weaknesses... account for the largest portion of economic and industrial information lost by US corporations.” - **1995**

“Espionage over networks can be cost-efficient, offer nearly immediate results, and target specific locations... and are insulated from risks of internationally embarrassing incidents.” - **1988**

“The almost obsessive persistence of serious penetrators is astonishing.” - **1988**

“I almost feel like it’s the early days of flight with the Wright brothers. First of all, you need to kind of figure out that domain, and how are we going to operate and maintain within that domain. So I think it will take a period of time, and it’s going to be growing.” - **2009**

“Our red teams do get into most of the networks we target .” - **2008**


“We’ve had market failure when it comes to cybersecurity. Security doesn’t come out of voluntary actions and market forces .” - **2012**

“Cyber tools have enhanced the economic espionage threat, and the Intelligence Community judges the use of such tools is already a larger threat than more traditional espionage methods .” - **2010**

“Foreign collectors of sensitive economic information are able to operate in cyberspace with relatively little risk of detection in the private sector data targets.” - **2010**



"I liken it to the very first aero squadron when they started with biplanes. We're at the threshold of a new era where we're sure how combat

in  The image cannot be displayed. Your computer may not have enough memory to open the image, or the image may have been corrupted. Restart your computer, and then open the file again. If the red x still appears, you may have to delete the image and then insert it again.

"F

"T

sys

"C

eco

"Espionage over networks can be cost-effective and internationally embarrassing incidents."

"T

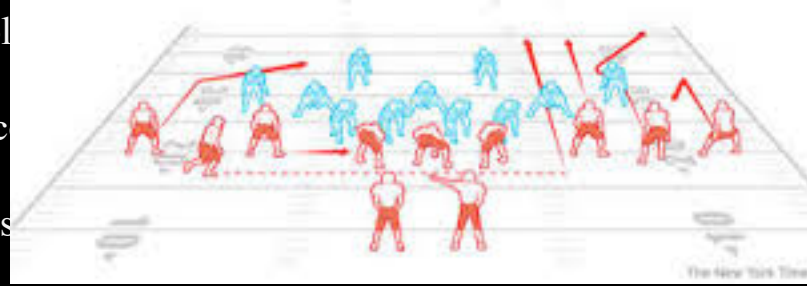
"I  
to operate and maintain within that domain"

"Our red teams do get into most of the ne

"We've had market failure when it comes to cybersecurity. Security doesn't come out of voluntary actions and market forces."

- 2012

splunk listen to your data



ssin

79

ough to match the apparent growth in threats to



ryption wea

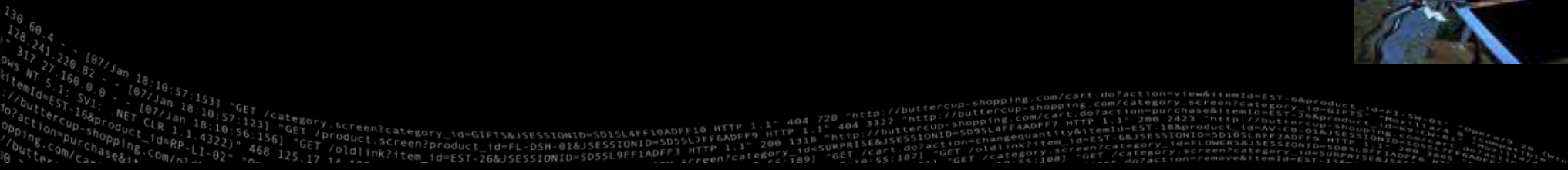
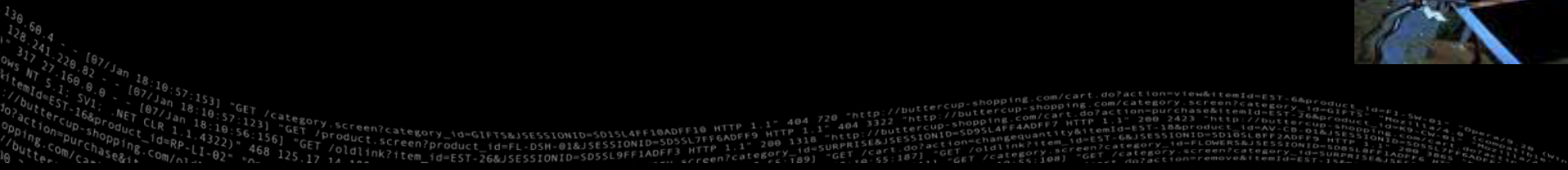
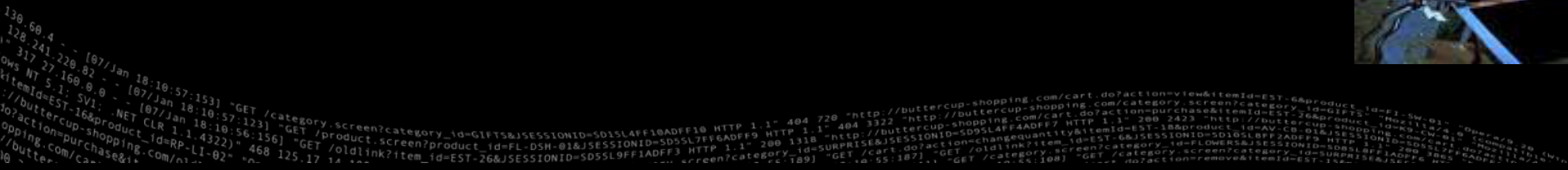
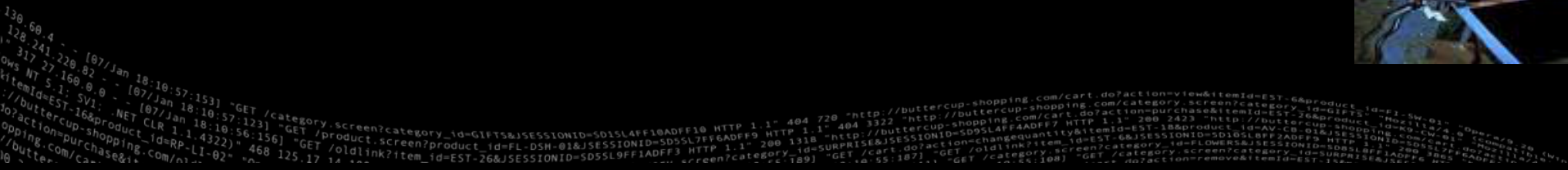
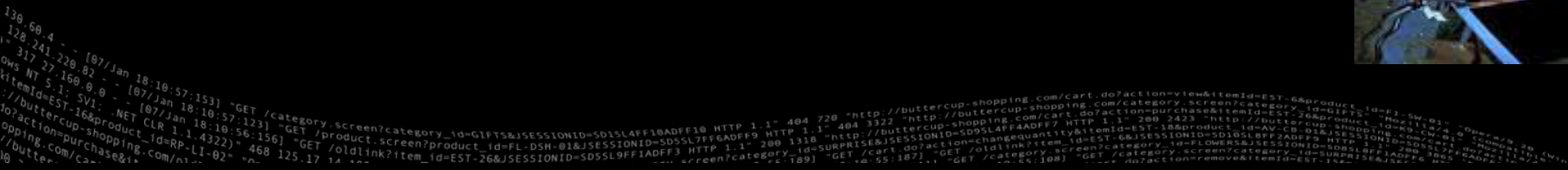
largest portion of

specific lo

form risks of



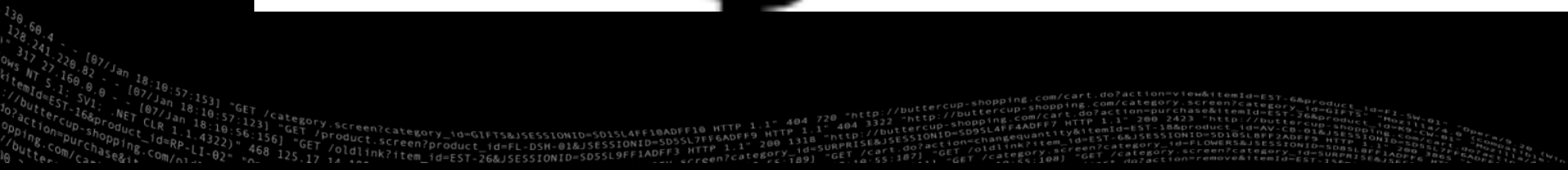
oing





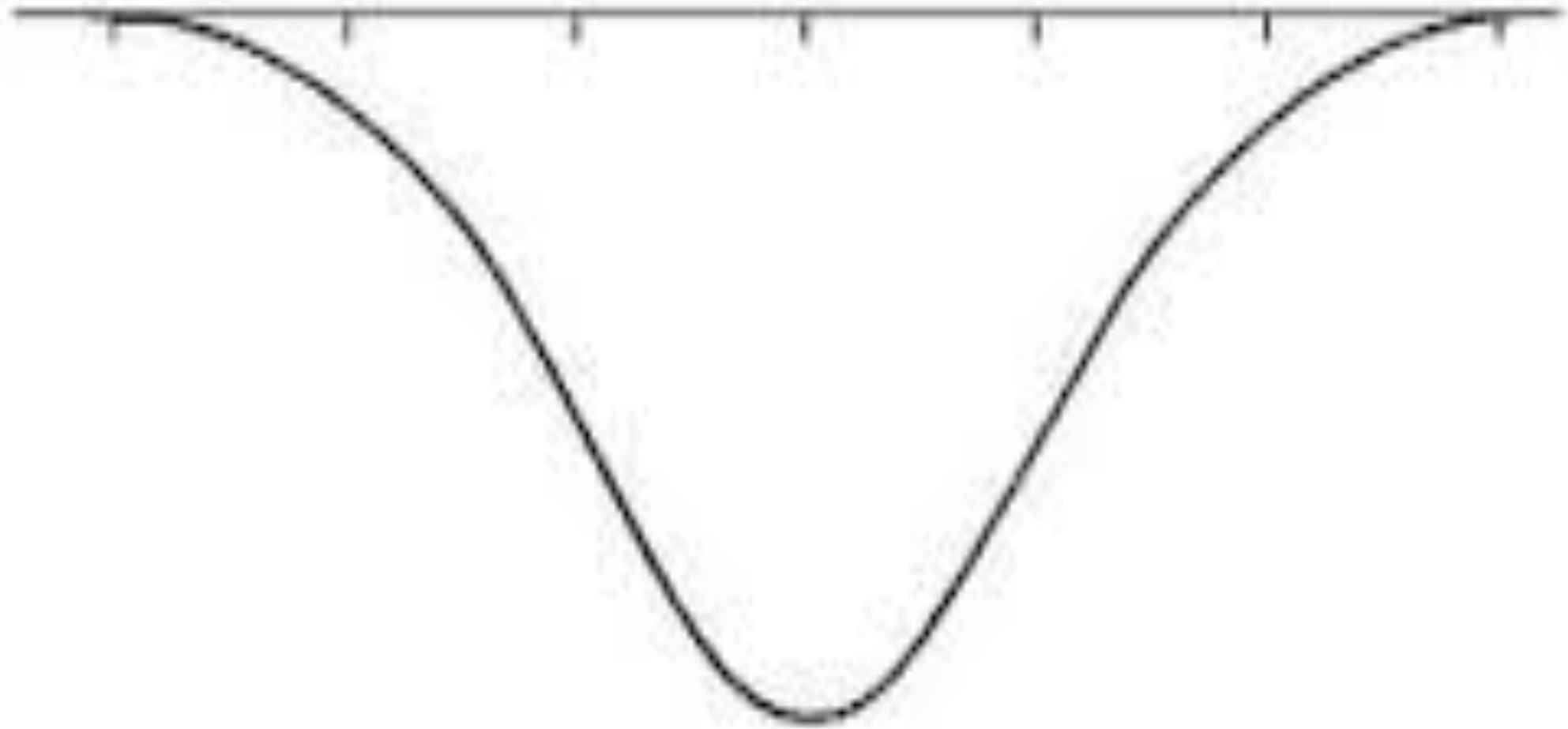


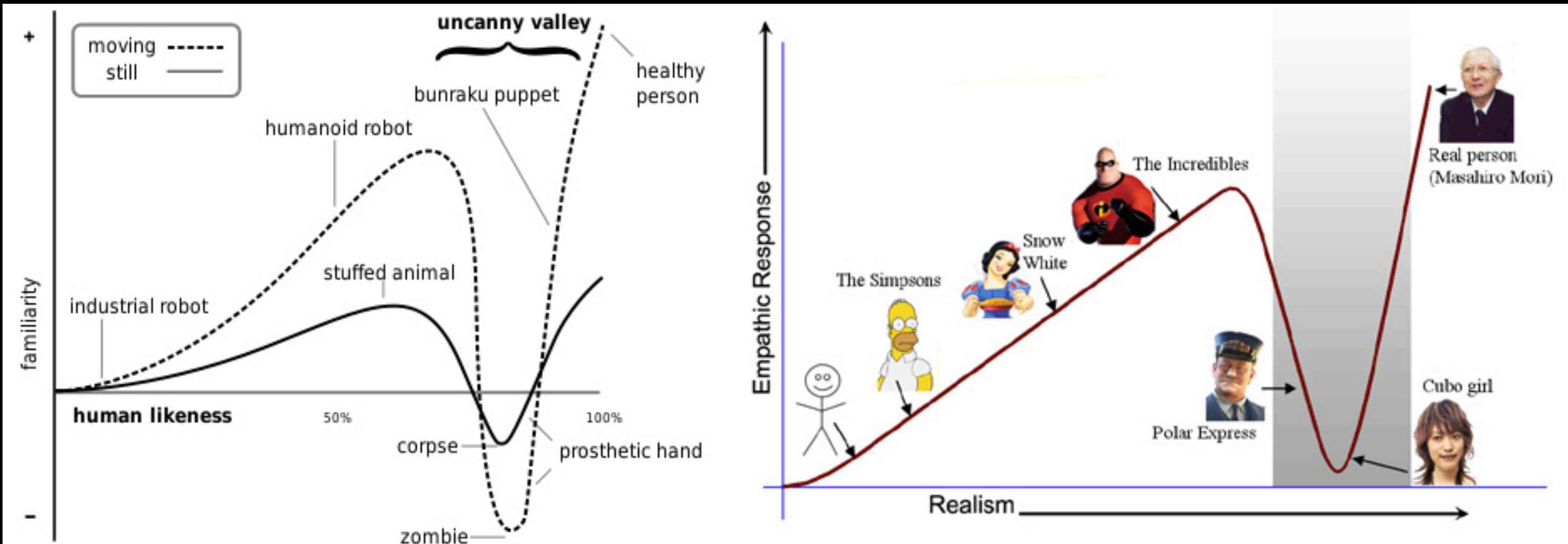
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category\_id=GIFTS&JSESSIONID=50  
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product\_id=FL-DSH-01&JSESSIONID=5055L9FF1ADFF3 HTTP/1.1" 200 125.17 14  
317 27.160.0.0 - - [07/Jan 18:10:57:123] "GET /product.screen?product\_id=FL-DSH-01&JSESSIONID=5055L9FF1ADFF3 HTTP/1.1" 200 125.17 14  
ows NY 5.1; SV1; - - [07/Jan 18:10:57:123] "GET /product.screen?product\_id=FL-DSH-01&JSESSIONID=5055L9FF1ADFF3 HTTP/1.1" 200 125.17 14  
//buttercup-shopping.com/oldlink?item\_id=EST-26&JSESSIONID=5055L9FF1ADFF3 HTTP/1.1" 200 125.17 14  
do?action=purchase&product\_id=RP-LI-02" 468 125.17 14  
shopping.com/purchase&product\_id=RP-LI-02" 468 125.17 14  
//buttercup-shopping.com/purchase&product\_id=RP-LI-02" 468 125.17 14  
//buttercup-shopping.com/purchase&product\_id=RP-LI-02" 468 125.17 14



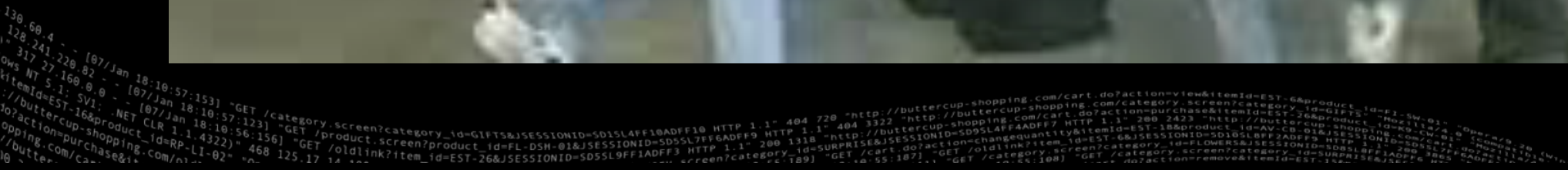




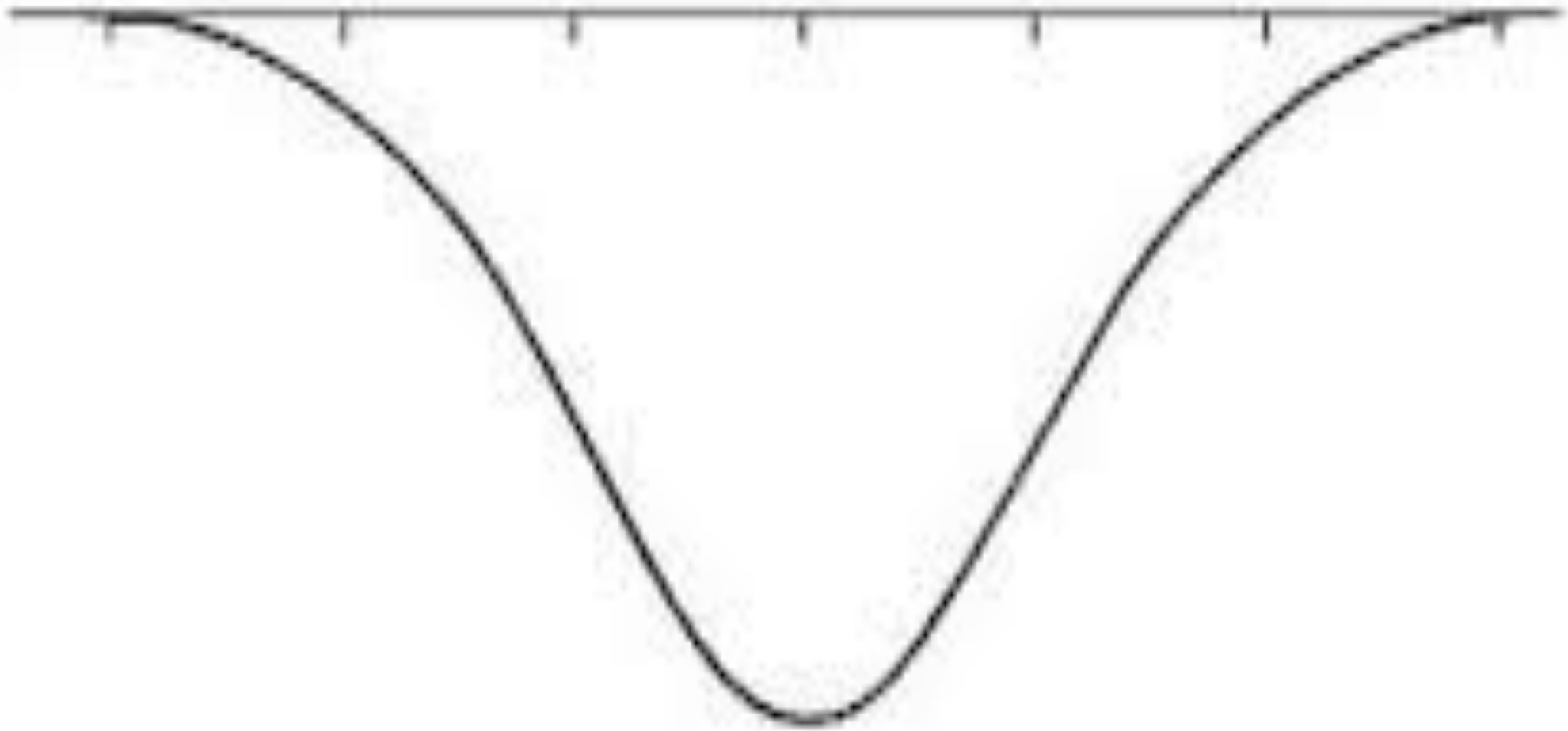






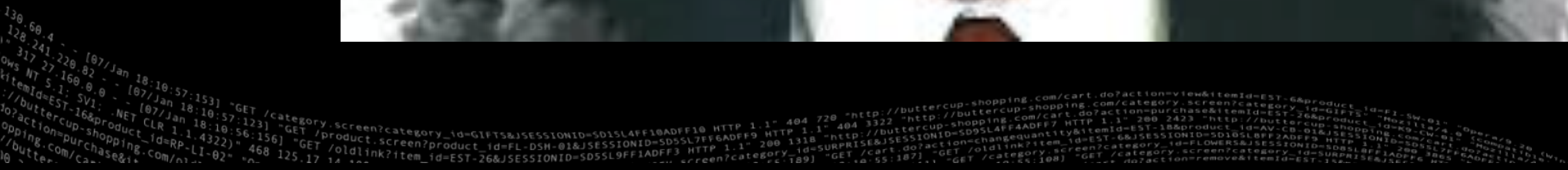


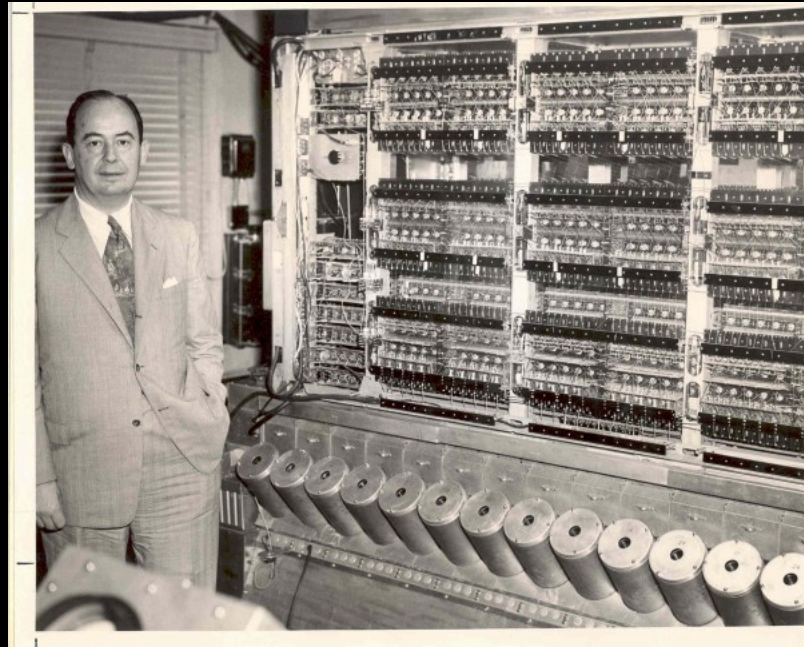














S-Gt

*mf*

TAB

10-15 14 12 13

4

TAB

12 14 10 14 12 10 12 10 13

7

TAB

8 12 10 9 10 8 12 15 12

10

TAB

14 10 14 12 10 12 12 10 13 15 12 8 8 9 8 8 12 15 13 12 13 12 15 20 15 17 17 17 19 15 19 17 17 15 20

let ring



The image features a central photograph of a baby crawling on a black surface, wearing a diaper. The baby is positioned in the center, facing left, with its head turned slightly towards the camera. The background is a white sheet of music paper with black musical notation. The notation includes a treble clef, a key signature of one sharp (F#), and a 4/4 time signature. The music is written in a style that suggests a guitar or string instrument, with various notes, rests, and fingerings indicated. The notation is arranged in a way that it appears to be a continuous piece of music, with measures separated by bar lines. The overall composition is a blend of a real-world photograph and a musical score.

# Strategy on a napkin

	Identify	Protect	Detect	Respond	Recover
Confidentiality					
Integrity					
Availability					

# Strategy on a napkin

	Identify	Protect	Detect	Respond	Recover
Confidentiality					
Integrity	X	X	!	!	!
Availability					

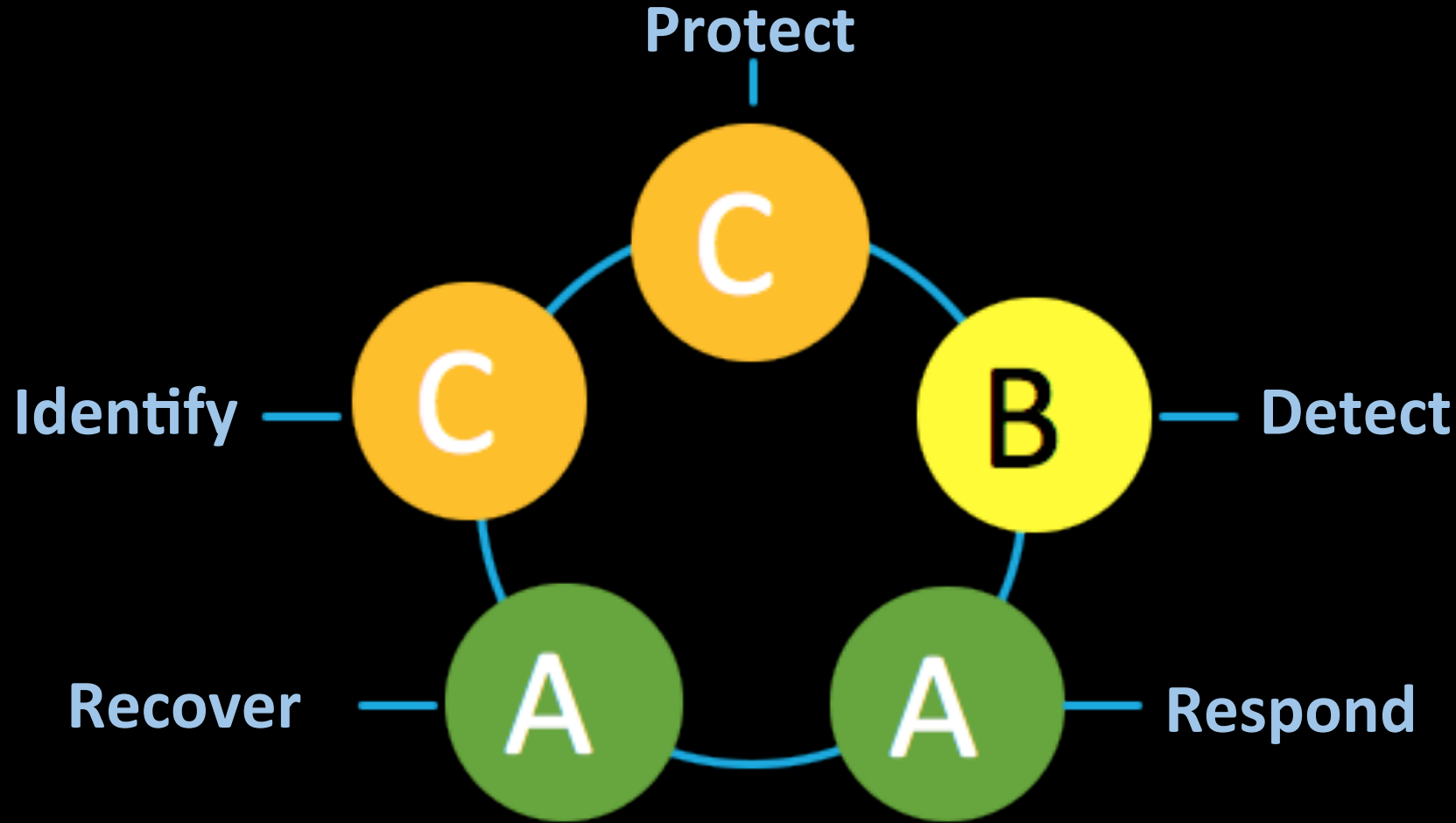


# Strategy on a napkin

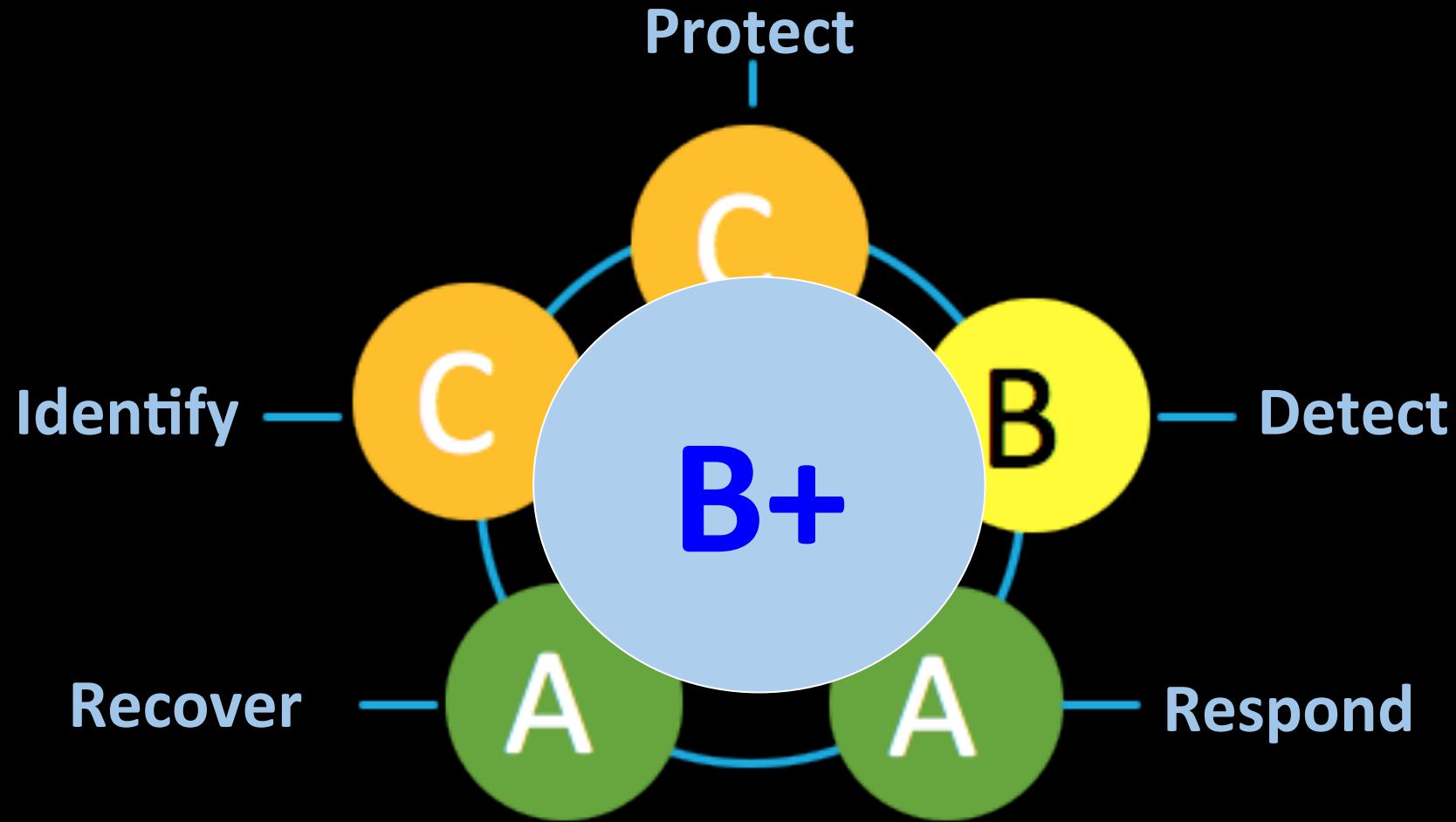
	Identify	Protect	Detect	Respond	Recover
Confidentiality					
Integrity			X →	X →	X
Availability					

# GOHIO

A diagram of a cycle graph  $C_4$  with four nodes arranged in a square. The nodes are labeled A, B, C, and D. Node C is highlighted in orange and has the word "Protect" written above it. The other nodes are colored: A is green, B is yellow, and D is light blue. The nodes are connected by blue edges forming a cycle.

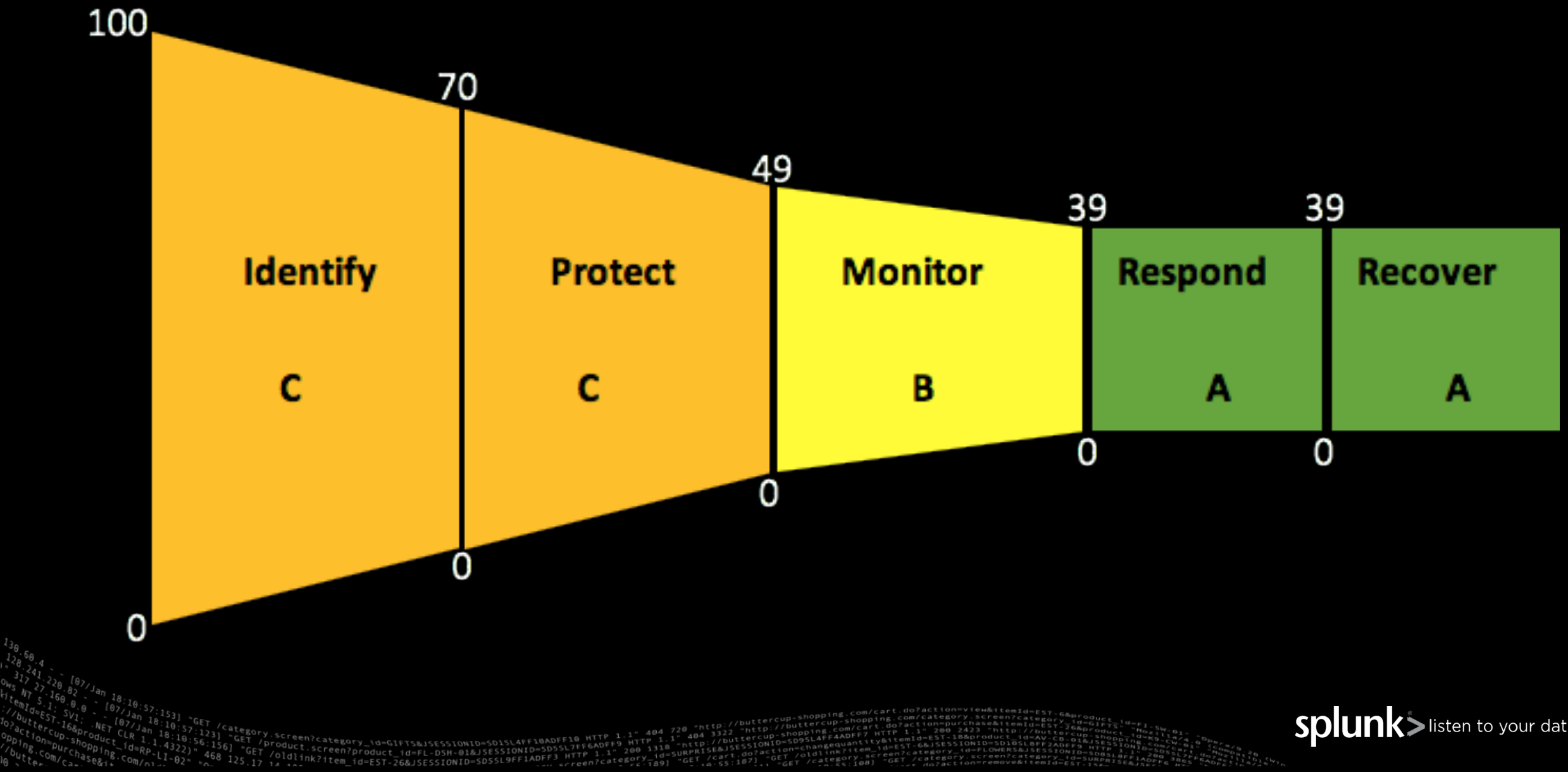


# Order of operations

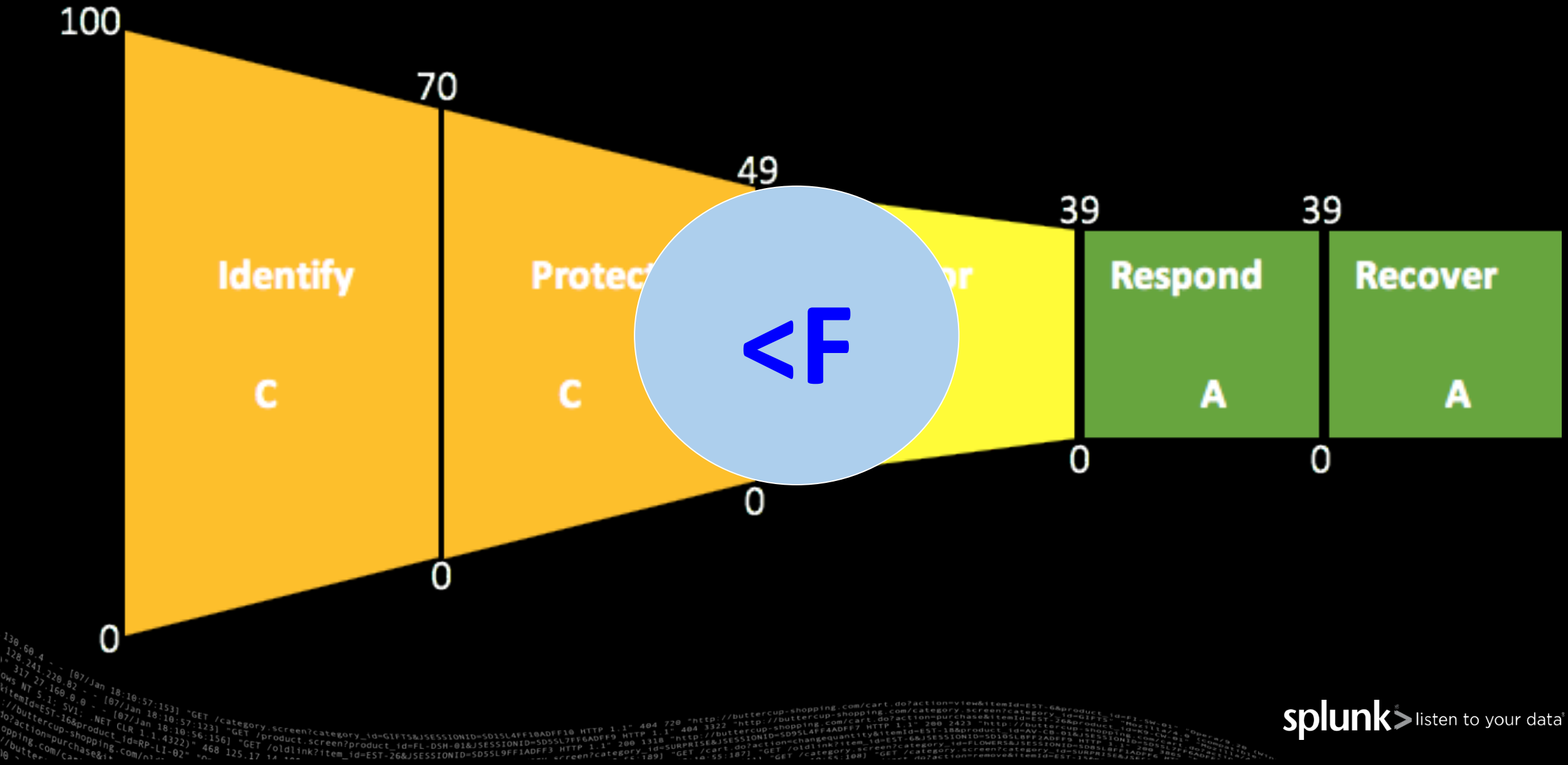




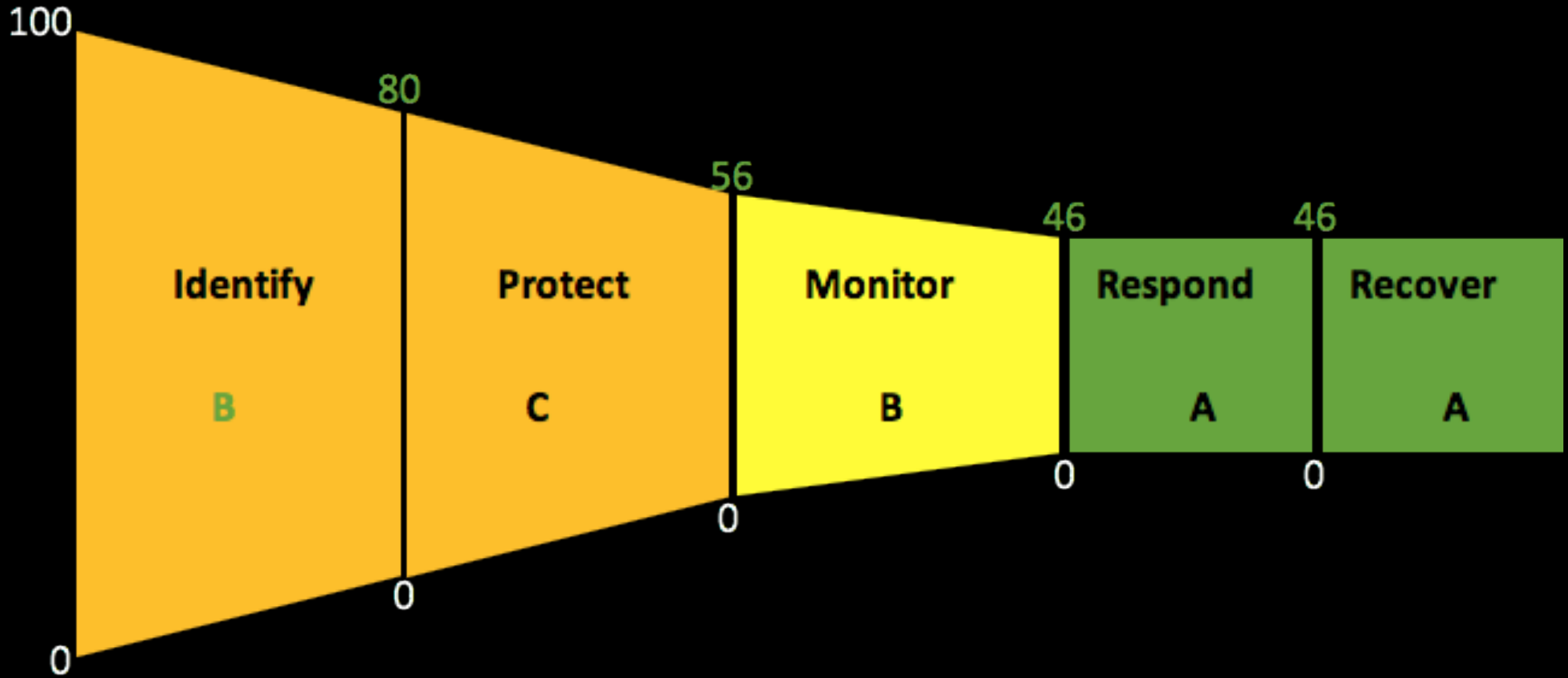
# Order of operations



# Security Efficacy Consequences



# Security Efficacy Consequences



# Thank you

*Joel Fulton, PhD*

*CISO*

*jfulton@splunk.com*

**splunk** >