"Oper

....

51

8501

0

SW-01"

Windows NT 6;0; id=AV-SB-02;0;

do?action= re_{\sim} 404 474

 $\int_{1.1} d = AV - SB$

9 82.24 "Mozilla/4.036 200 1901 ".0 (0 ?category http id

18 2" "Me 1" 200 1901 "Title" 1" 200 1901 "Title" reen?category "Title" ing" "Me ing" "Me

een en-US) ADD Webk tercup-shoppinebk ADFF2 HTTP 1 NE EDDY&JSE:1:

F2 HTTP TEDDY&JSESION 71 "POSTESS"

en-US) POST

SN-01&JSE

 roc_{233} , za_{33}

217 189 82.245.228. 189 "Mozilla/4.0³6

y.screen?com;at nopping.com/d: een?category_ic

The Agile Security Program

Maximizing efficacy in a world of fast-changing threats

Craig Vincent | Regional Security SME, Higher Education

August 2017



Outcomes Breakdown





The Checkbox.



(%:10:57:133] "GET /category.screen?category_id=GIFTS&ISESSIONID=SDISL4FF1eADFF1e HTTP 1.1" 404 720 "http://buttercup-shopping.com/catt.do?action=view@itemId=EST-6&product." (0//jn 18:10:57:123] "GET /category.screen?category_id=GIFTS&ISESSIONID=SDISL4FF1eADFF1e HTTP 1.1" 404 720 "http://buttercup-shopping.com/catt.do?action=view@itemId=EST-6&product." HTTP://buttercup-shopping.com/catt.do?action=view@itemId=EST-6&product." HTTP://buttercup-shopping.com/catt.do?action=view@itemId=EST-6&product." HTTP://buttercup-shopping.com/catt.do?action=view@itemId=EST-6&product." HTTP://buttercup-shopping.com/catt.do?action=view@itemId=EST-6&product." HTTP://buttercup-shopping.com/cattercup-shopping.com/cattercup-shopping.com/catt.do?action=view@itemId=EST-6&product." HTTP://buttercup-shopping.com/cattercup-shopping.



The Living, Breathing Security Program





sten to vour data

Forward-Looking Statements

During the course of this presentation, we may make forward-looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC.

The forward-looking statements made in this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements we may make. In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionality described or to include any such feature or functionality in a future release.

Splunk, Splunk>, Listen to Your Data, The Engine for Machine Data, Splunk Cloud, Splunk Light and SPL are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners. © 2017 Splunk Inc. All rights reserved.

uct.screen?product_id=FL-DSH-01&JSE

Objectives



Origins of Checkbox Culture Principles of Agile and Lean Philosophies

// froduct.screen?product_id=Eisessionid=S015(4Ff10ADFF10 GET /oldlink?item_id=Eisessionid=S05(9F1ADFF3 HTTP 1.1 200 1318 17 14 torsitem_id=Eise35(555100)10=S055(9FF1ADFF3 HTTP 1.1 27 14 torsitementset Common Challenges Framework



About Me Craig Vincent

Solution Engineer & Regional Security Subject Matter Expert



Screen?product 1d=FL-DSH-01&JSESSIONID=SD

Splunk MANDIANT







Universities & Colleges



State & Local Governments



Medical Centers

splunk >listen to your data*





Where did this culture come from?



//category.screen?category_id=GIFTS&JSESSIONID=SDISLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/catt.do?action=purchase&irenId=EST-6&product_inesister_ine











SOUNK listen to your data

Challenges Getting Started

- Invest once mentality
- Projects seem difficult to completely define

Screen?product id=FL-DSH-01&JSESSIONID=SD

Hard to manage operational risks



Getting started



Challenges

Keeping up with the security landscape



404 33

SURPRISE&JSESSIONID-

T / DECEMPTCATEGORY_1d=GIFTS&JSESSIONID=SD1SL4FF10ADFF10 HTTP I.1 GET /oldlink?item // oldlink?item // id=SI-2&JSESSIONID=SDSSIOFF1ADFF3 HTTP i.1 // id=SI-2&JSESSIOFF1ADFF3 // id=SI-2&JSESSIOFF1ADF73 // id=SI-2&JSESSIOF73 // id=SI-2&J



Advanced Threats are Hard to Find



Cyber Criminals



100% Valid credentials were used





40

Average # of systems accessed



143

Median # of days before detection



creen?product id=FL-DSH-01&JS



67% Of victims were notified by

external entity

Source: Mandiant M-Trends Report 2012/2013/2014/2015/2016

splunk listen to your data[®]

Advanced Threats are Hard to Find

Threat



People





Attack Approach

- Human directed
- Goal-oriented
- Dynamic (adjust to changes)
- Coordinated

Screen?product id=FL-DSH-01&JSE

- Multiple tools & activities
- New evasion techniques

Security Approach

- Fusion of <u>people</u>, <u>process</u>, <u>& technology</u>
- Contextual and behavioral
- Rapid learning and response
- Share info & collaborate
- Analyze all data for relevance
- Leverage IOC & Threat Intel

splunk listen to your data*

NIST Special Publication 800-137

NIST

National Institute of Standards and Technology

U.S. Department of Commerce

Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations

Kelley DémpseyNirali Shah ChawlaFederalArnold JohnsonFederalAngela OrebaughChangingMatthew SchollKevin Stine

INFORMATION SECURITY

Introduction to Agile & Lean



Project Management



-37:153] "GET / Gategory.screen?category_id=GIFTS&JSESSIONID=SDISLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=viow&itemId=EST=G&product_id=FI_SW_Gi_ 1.1:10:56:156] "GET /product.screen?category_id=GIFTS&JSESSIONID=SDISLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=viow&itemId=EST=G&product_id=FI_SW_Gi_ 3.1:10:56:156] "GET /product.screen?category_id=GIFTS&JSESSIONID=SDISLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=viow&itemId=EST=G&product_id=FI_SW_Gi_ 3.1:4222] "GET /product.screen?product_id=EIT=S&JSESSIONID=SDISLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup=sbopLaFFAADFF1.1" 202423 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST=G&product_id=FI_SW_Gi_ 3.1:4222] "GET /product.screen?product_id=EIT=S&JSESSIONID=SDISLAFF10ADFF10 HTTP 1.1" 200 1318 "http://buttercup=sbopLaFFAADFF1.1" 2025/action=changeduating_id=EST=G&JSESSIONID=SDISLAFF10ADFF10 HTTP 1.1" 200 2025/action=changeduating_id=EST=G&JSESSIONID=SDISLAFF10ADFF10 HTTP 1.1" 200 2025/action=changeduating_id=EST=G&JSESSIONID=SDISLAFF10ADFF10 HTTP 1.1" 200 2025/action=changeduating_id=EST=G&JSESSIONID=SDISLAFF10ADFF10 HTTP 1.1" 200 1318 "http://screen?category_iscreen?categor



Project Management



Traditional Project Management Challenges

Doesn't handle in-flight change

Extended time to value/ revenue

Little communication across groups

Limited focus on customer needs

In-flight Change

splunk > listen to your data

Time to Value/ Revenue



1



Cross-functional Communication





Customer Needs



splunk > listen to your data

Understanding the Terminology



5 Principles of Lean

- 1. Specify value from the standpoint of the end customer by product family.
- 2. Identify all the steps in the value stream for each product family, eliminating whenever possible those steps that do not create value.
- 3. Make the value-creating steps occur in tight sequence so the product will flow smoothly toward the customer.
- 4. As flow is introduced, let customers pull value from the next upstream activity.
- 5. As value is specified, value streams are identified, wasted steps are removed, and flow and pull are introduced, begin the process again and continue it until a state of perfection is reached in which perfect value is created with no waste.

www.lean.org

12 Principles of Agile

- 1. Our highest priority is to satisfy the customer through early and continuous delivery of valuable software.
- 2. Welcome changing requirements, even late in development. Agile processes harness change for the customer's competitive advantage.
- Deliver working software frequently, from a couple of weeks to a couple of months, with a preference to the shorter timescale.
- 4. Business people and developers must work together daily throughout the project.
- 5. Build projects around motivated individuals. Give them the environment and support they need, and trust them to get the job done.
- 6. The most efficient and effective method of conveying information to and within a

uct.screen?product id=FL-DSH-01&JS

development team is face-to-face conversation.

- 7. Working software is the primary measure of progress.
- Agile processes promote sustainable development. The sponsors, developers, and users should be able to maintain a constant pace indefinitely.
- Continuous attention to technical excellence and good design enhances agility.
- 10. Simplicity--the art of maximizing the amount of work not done--is essential.
- 11. The best architectures, requirements, and designs emerge from self-organizing teams.
- 12. At regular intervals, the team reflects on how to become more effective, then tunes and adjusts its behavior accordingly.

Splunk Slisten to your data

Relevant Principles



creen?product id=FL-DSH-01&JSE

splunk Slisten to your data



"http://buttercup-

/category

0//ja%;153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD1SLAFF10ADFF10 HTTP 1.1" 404 720 "http://butte://butter fCLR al.18:10:55:123] "GET /product.screen?product_id=GIFTS&JSESSIONID=SD1SLAFF10ADFF10 HTTP 1.1" 404 3322 "http://buttercup=shoppin ci_id=Rp_LI-056:156] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD5SL7FF0ADFF3 HTTP 1.1" 404 720 "http://buttercup=shoppin g.com/sciences/allocality and allocality and allocalit

CLR 1.1.4322)" 468 126 17 1010

oduct_id=RP-LI-02"

splunk >listen to your data* om/category.screen?categor ttercUP-sp95L4FFADDr/ty&itemId=ST-18&product_1d=AV ESSIONIDesDIDSL0FF .do2action=changequantitem_id=EST-6&JSESIONIDeSDIDSL0FF .do2action=changequantitem_creen?category_id=CoMm?categor 1871.~GEGET /categori08] GET /categori060reenwee&item

Poll

splunk.com/poll



How many of you have a SIEM?

Answer at splunk.com/poll



How many of you have a SIEM that you use?

Answer at splunk.com/poll



Are your security technologies static?

Answer at splunk.com/poll



Did it take a long time for you to start using your security technology?

Answer at splunk.com/poll



Think of the last major security threat, did you adapt your security technologies to address that threat?

Answer at splunk.com/poll



Do all your security teams communicate regularly?

Answer at splunk.com/poll



Do you regularly review your security processes to identify areas of improvement?

Answer at splunk.com/poll



Security Takeaways



Security Project Management Challenges

Doesn't handle in-flight change

Extended time to value/ revenue

Little communication across groups

Limited focus on customer needs



In-flight Change

splunk > listen to your data

Time to Value/ Use



A



Cross-functional Communication



Splunk > listen to your data



Operational Risks



splunk > listen to your data

Agile Security Operations Framework





Incident Response

'''I0:'57:133] "GET /category.screen?category_id=GIFTS&ISESSIONID=SDISL4FF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/category.screen?category_id=GIFTS&ISESSIONID=SDISL4FF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/category.screen?category_id=GIFTS&ISESSIONID=SDISL4FF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/category.screen?category_id=GIFTS&ISESSIONID=SDISL4FF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/category_id=GIFTS&ISESSIONID=SDISL4FF10ADFF10 HTTP 1.1" 404 720 "id=SUBF100ADFF10 HTTP 1.1" 404 720 "id=SUBF10ADFF10 HTTP 1.1" 404 720 "id=SUBF10ADFF10





Incident Response

> Incident responders/manager write 'User Stories' or short blurbs specifying a capability that they lack

Capability Backlog

ll3] "GET /Category.Screen?category_id=GIFTS&JSESSIONID=SD15LAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/category.screen?category_id=GIFTS&JSESSIONID=SD15LAFF10ADFF10 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/category.screen?category_id=GIFTS&JSESSIONID=SD15LAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/category.screen?category_id=GIFTS&JSESSIONID=SD15LAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/category.screen?category_id=GIFTS&JSESSIONID=SD15LAFF10ADFF10 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/category.screen?category_id=CIFTS&JSESSIONID=SD15LAFF10ADFF10 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/category.screen?category_id=CIFTS&JSESSIONID=SD15LAFF10ADFF10 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/category.screen?category_id=CIFTS&JSESSIONID=SD15LAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/category.screen?category_id=CIFTS&JSESSIONID=SD15LAFF10ADFF10 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/category.screen?category_id=CIFTS&JSESSIONID=SD15LAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/category.screen?category_id=CIFTS&JSESSIONID=SD15LAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/category.screen?category_id=CIFTS&JSESSIONID=SD15LAFF10ADFF10 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/category.screen?category_id=CIFTS&JSESSIONID=SD15LAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/category.screen?category_id=CIFTS&JSESIONID=SD15LAFF10ADFF10 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/category.screen?category_id=CIFTS&JSESIONID=SD15LAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/category.screen?category



Example User Story

Anomalous Process Start Detection

in list Capability Backlog

Description Edit

Story: As a Security Analyst, I want the ability to be notified of anomalous process initiated on covered machines so that I can detect threats and maintain compliance with NIST 800-171

Related to: snow.southharmon.edu/Fe293Kw

splun

listen to your data[®]



Sprint Backlog



Backlog

Security Engineering Security Engineering and other appropriate stakeholders annotate the 'user story' with the technical requirements and dependencies. If a task is too broad, it can be divided into smaller stories.



Security Engineering Designated Security Owner prioritizes a set number of capabilities to be developed in the next sprint by considering threat landscape and organizational priorities and initiatives

:reen?category_id=GIFTS&JSE5SIONID=SDISLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/category_iscreenrates%temid=Esries%product_ Juct.screen?product_id=GIFTS&JSE5SIONID=SDISLAFF10ADFF10 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/category_iscreenrates%temid=Esries%temid=Esr temid=Esries%te



Annotation by Security Engineering

Determining the 'how'

	Anomalous Process Start Detection				
	in list <u>Capability Backlog</u>				
	Due Date				
	Dec 31 at 12:00 PM				
	Description Edit				
	Story: As a Security Analyst, I want the ability to be notified of anomalous process initiated on covered machines so that I can detect threats and maintain compliance with NIST 800-171				
	Related to: snow.southharmon.edu/Fe293Kw				
_					
\checkmark	Dependencies Delete.				
0%					
	Process Logging to Splunk				
	Confirm installation of Splunk Addon for Nix @SplunkAdmin				
	Confirm that Enterprise Security is installed				
	Enable 'Anomalous Process Detected' Correlation Search				
	Add an item				

=GTFTSRISESSIONTD=SD3 Screen?product 1d=FL-DSH-01&JSESSIONID=SD55L te...

Splunk > listen to your data

Annotation by Security Engineering

Classify

d=GIFTS&JSESSIONID=SD1SL4FF10ADFF10 HTTP

IONID=SD5SL9FF1ADFF3 HTTP

/product.screen?product id=FL-DSH-01&JSESSIONID=SD5SL7FF6ADFF9

Anomalous Process Start Dete		Labels		
in list Capability Backlog			Search labels	
Labels	Due Date			
Detection Malware Persistance +	Dec 31 at 12:00 PM			~
Description Edit				~
Story: As a Security Analyst, I want the all process initiated on covered machines so compliance with NIST 800-171	ntain			
Related to: snow.southharmon.edu/Fe29	<u>3Kw</u>		Containment	ľ
Dependencies	De	lete	Detection 🗸	-
Process Logging to Splunk			Investigation	-
Confirm installation of Splunk Addon for I		Preparation	1	
Confirm that Enterprise Security is installed		Poviou	A.	
Enable 'Anomalous Process Detected' Co		neview	Í	
Add an item			Malware Persistance 🗸 🗸	<i>.</i>
			Phishing	<i>.</i>
Add Comment			User Account Compromise	<i>.</i>
Write a comment				

404 3322

200 1318

splunk >listen to your data*

Building a Sprint

Identify threat priorities and place story on incident response lifecycle

	Preparation	Detection	Investigation	Containment	Recovery	Review
Phishing						
User Account Compromise						
Persistent Malware		X				
20. (07/Jan 10			Anomalous Process Star in list <u>Capability Backlog</u> Description <u>Edit</u> Story: As a Security Analyst, I wa process initiated on covered mac compliance with NIST 800-171 Related to: <u>snow.southharmon.ec</u>	rt Detection	ous d maintain	
82 'Jan 18:10:57:153] "GET /category. :0-0.0 ' [07/Jan 18:10:57:123] "GET /category. :16&product[R1 1.18:10:56:15c; 'PET /pr :shopn; imp-shopn; imp-s	SCreen?category_id=GIFT5&JSESSIONID=:	5015L4FF10ADFF10 HTTP 1.1" 404 720 "h 1.1" 404 720 "h 1.1" 404	ttp://buttercup-shopping.com/cart.do7 3322 "http://buttercup-shopping.com/ //buttercup-shopping.com/cart.do7 1,1 //buttercup-shoppi_4FF4ADFF7 HTTP 1,1 //buttercup-shoppi_4FF4ADFF7 HTTP 1,1	action=view&itemId=EST-G&product_id= category.screen7category_id=GifFj:id= ion=purchase&itemIdEgory_G&product_i = 200 2423 "http://buil.cG&product_i ==ST-18&product_id=AV-Greups&_15ESSIOn &SJSSSIONID=SDI651&FF2ADFP&_15ESSION	Horitara Barko taraca	unk listen to your dat



Screen?product id=FL-DSH-01&JSESSIONID=



In Progress

Capability Backlog	Sprint Backlog	 In Progress ····
Add a card	Add a card	Anomalous Process Start Detection
		\bigcirc Jul 31 \equiv \boxdot 3/4
		Process Logging to Splunk
		=
		Add a card

Information is openly available

	Anomalous F in list In Progress	Process Star	t Detection	n			
	Labels						
	Detection Malv	vare Persistance	+				
	Due Date	00 PM (past due)					
	Description Edit						
	Story: As a Secur process initiated compliance with I	ity Analyst, I war on covered macl NIST 800-171	nt the ability to nines so that I	be notified of anomalous can detect threats and maintain			
	Related to: snow.	southharmon.ed	<u>u/Fe293Kw</u>				
750/	Dependencies			Hide completed items Delete			
75%	Process Logg	ing to Splunk					
\checkmark	Confirm installation of Splunk Addon for Nix @SplunkAdmin						
\checkmark	Confirm that Ente	rprise Security is	installed				
\checkmark	Enable 'Anomalou	us Process Detec	cted' Correlatio	on Search			
	 ↓ ↓	 Anomalous F in list In Progress Labels Detection Malv Due Date Jul 31 at 12:0 Description Edit Story: As a Secur process initiated of compliance with I Related to: snow. Dependenciess 75% Process Loggi Confirm installation Confirm that Enter Enable 'Anomaloo 	 Anomalous Process Star in list In Progress Labels Detection Malware Persistance Due Date Jul 31 at 12:00 PM (past due) Description Edit Story: As a Security Analyst, I war process initiated on covered mach compliance with NIST 800-171 Related to: snow.southharmon.ed Dependencies 75% Process Logging to Splunk Confirm installation of Splunk Ada Confirm that Enterprise Security is Enable 'Anomalous Process Detection 	 Anomalous Process Start Detection in list In Progress Labels Detection Malware Persistance + Due Date Jul 31 at 12:00 PM (past due) Description Edit Story: As a Security Analyst, I want the ability to process initiated on covered machines so that I compliance with NIST 800-171 Related to: snow.southharmon.edu/Fe293Kw Dependencies 75% Process Logging to Splunk Confirm installation of Splunk Addon for Nix @Signation Confirm that Enterprise Security is installed Enable 'Anomalous Process Detected' Correlation 			

SET /category.screen?category_id=GIFTS&JSESSIONID=SDISLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/category_iscreen?category_iscreen?category_id=GIFTS&JSESSIONID=SDISLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/category_iscreen?category_iscreen?category_id=GIFTS&JSESSIONID=SDISLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/category_iscreen?category_id=GIFTS&JSESSIONID=SDISLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/category_iscreen?category_id=GIFTS&JSESSIONID=SDISLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cate_id=2433 "http://butterCup-shopping.com/category_id=GIFTS&JSESSIONID=SDISLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cate_id=2433 "http://butterCup-shopping.com/category_id=GIFTS&JSESSIONID=SDISLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/category_id=GIEFT ADFF1 HTTP 1.1" 200 istory id=GIEFTADFF7 HTTP id=GIEFTADFF7 HTTP 1.1" 200 istory id=SURPRISESSIONID=SDISLAFF10ADF77 HTTP 1.1" 200 istory id=SURPRISESSIONID=SDISLAFF10ADF77 HTTP 1.1" 200 istory id=SURPRISESTORY id=GIEFTADF77 id=GIE /category_id=GIEFTADF77 id=GIEFTADF77 id=GIEFTADF77 id=GIE /category_id=GIEFTADF77 id=GIEFTADF77 id=GIEFTADF77 id=GIE /category_id=GIEFTADF77 id=GIEFTADF77





Security Engineering

.Screen?product id=FL-DSH-01&JSESS

The requestor validates that the requirements of the original 'user story' have been met. Deviations are permitted at the sub-story level. If there are any deviations or changes, a new user story can be authored and prioritized





Capture metrics to improve the process

splunk >listen to your data*

Early Results



- Certain customers have started incorporating this framework into their operations
- Challenges involved buy in with other groups and process purity
- Surprising benefit was increased motivation

(3) "GET / Category.screen?category_id=GIFTS&JSESSIONID=SDISLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=puritex&itemId=EST_6&product_1=0.5%, 000 and 000 a



Security Takeaways

The Benefits

- Faster time to value
- Save Money
- Higher Motivation
- Greater Collaboration
- Focus limited resources

ili3] "GET /category.screen?category_id=GIFTS&JSESSIONID=SDISL4FF19ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/category.screen?category_id=GIFTS&JSESSIONID=SDISL4FF19ADFF10 HTTP 1.1" 404 7322 "http://buttercup-shopping.com/category.screen?category_id=GIFTS&JSESSIONID=SDISL4FF19ADFF10 HTTP 1.1" 404 7322 "http://buttercup-shopping.com/category.screen?category_id=GIFTS&JSESSIONID=SDISL4FF19ADFF10 HTTP 1.1" 404 732 "http://buttercup-shopping.com/category.screen?category_id=GIFTS&JSESSIONID=SDISL4FF19ADFF10 HTTP 1.1" 404 7322 "http://buttercup-shopping.com/category.screen?category_id=GIFTS&JSESSIONID=SDISL4FF19ADFF10 HTTP 1.1" 404 7322 "http://buttercup-shopping.com/cate_id=ST-SBAPF0duct_id=AV-cB-sBapF10 HTTP 1.1" 200 1332 "http://buttercup-shopping.com/category_id=GIFTS&JSESSIONID=SDISL4FF19ADFF10 HTTP 1.1" 404 7320 "http://buttercup-shopping.com/category_id=GIFTS&JSESSIONID=SDISL4FF19ADFF10 HTTP 1.1" 404 7320 "http://buttercup-shopping.com/category_id=GIFTS&JSESSIONID=SDISL4FF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/category_id=GIFTS&JSESSIONID=SDIS



Related Works

- NIST 800-137 Information Security Continuous Monitoring
- Agile Cybersecurity Action Plan (ACAP)
- Agile Manifesto





Key Takeaways

1. Security is a Program, not a project

2. Outcomes-driven decision making

3. Focus on the 'quick wins'

4. Foster cross-functional communication



Thank You

