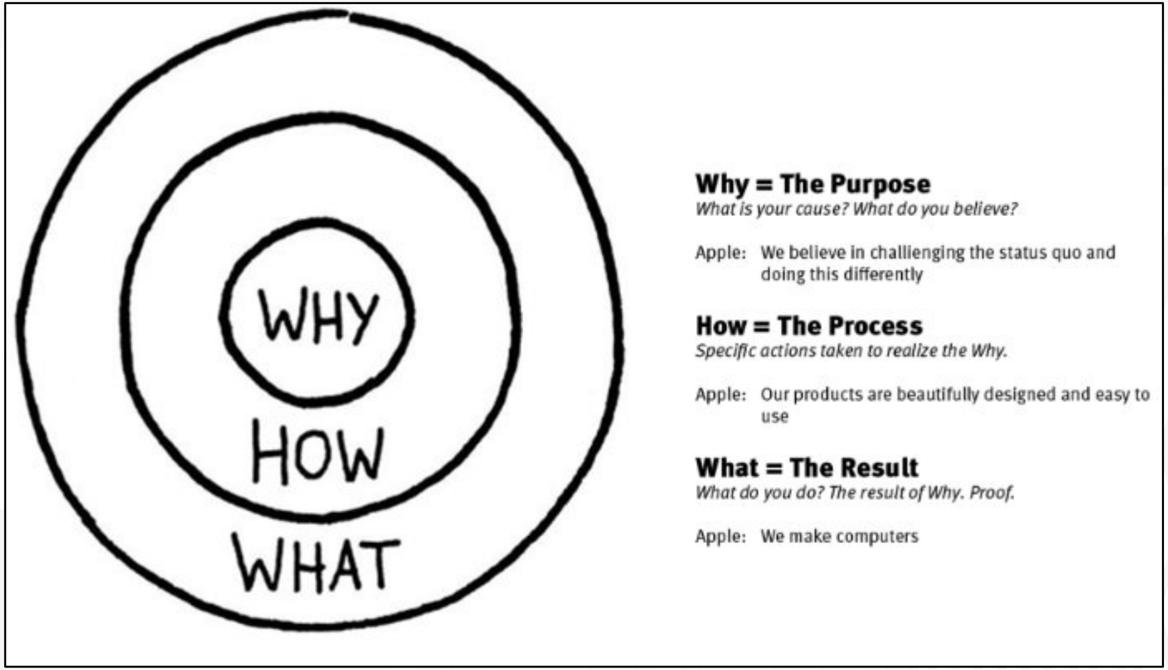
CONTROL YOUR FUTURE

TANIUM CONVERGE17

Risk Scoring, Security Orchestration and Automated Response

Gregory Pothier

Start with Why by Simon Sinek



Why = The Purpose
What is your cause? What do you believe?

Apple: We believe in challlenging the status quo and doing this differently

How = The Process
Specific actions taken to realize the Why.

Apple: Our products are beautifully designed and easy to use

What = The Result
What do you do? The result of Why. Proof.

Apple: We make computers

The Why: Objective of Risk Scoring

- Measure risk across multiple planes.
- Motivate users and system owners to reduce risk.
- Track improvement over time.
- Provide a single score for every user and every device.
- Enable senior management a conduit to support risk program.
- Inspire competition through gamification.

The How: Scoring Methodology

- Typical scoring has 100% as perfect score. Risk scoring is the opposite.
- Risk scoring is the aggregated (weighted) score.
- The higher the score, the greater the risk with zero as a perfect score.
- Score of a single object (i.e. user).
- Score of a set of objects (i.e. a team).

The What: Scoring Components

- Software Vulnerabilities.
- Patches (OS & application-level).
- Security Compliance.
- Anti-Virus.
- Standard Operating Environment Compliance.
- Cyber Security Awareness Training.
- Malicious and Behavior Analytics.

Risk Score

- 0 to 100 (0=, 100=)
- Base Score
  - 20% - Tanium Comply Score
  - 20% - Critical OS Patches1
  - 0% - 3rd Party App Versions
  - 10% - Anti-Virus
  - 10% - Tanium SOE/Health Check
  - 10% - User Behavior Analytics
  - 10% - Operating System Score
  - 5% - Encryption
  - 5% - Malicious Analytics

Score Multipliers
(super secret deep machine learning AI math formula)

where
ts = total score
m = incremental increase in %
n = number of occurrences of risk above redline threshold

Data Sets and Tools

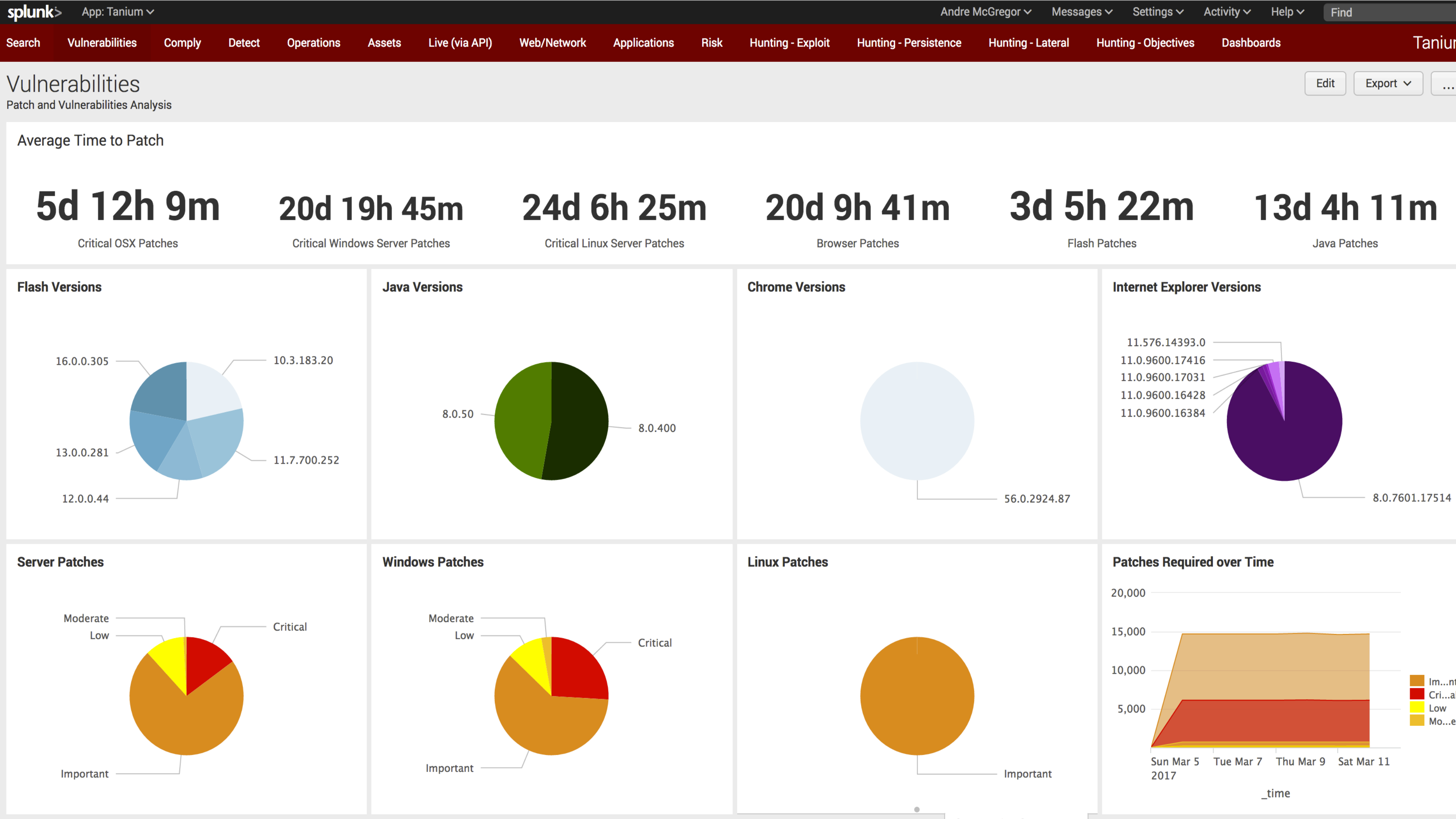
- Tanium Platform – Core, Comply, Threat Response, Discover, Patch, Integrity Monitor
- Splunk
- Sophos
- PhishMe
- Bitlocker, FileVault
- HR Management Software

Splunk? Why Splunk?

- Easy to dump raw data, normalize, and resolve anomalies.
- Can handle large data sets and large quantities of data.
- Front end dashboards easy to design and edit.
- Can handle high frequency of API calls without added costs.
- Tanium data + Splunk visualization.

Collect the Data

- Tanium asks the Questions
- Uses Connect to send to splunk
- Splunk collects the logs
- We create visualizations and actionable intelligence



Vulnerabilities

Patch and Vulnerabilities Analysis

Average Time to Patch

5d 12h 9m	20d 19h 45m	24d 6h 25m	20d 9h 41m	3d 5h 22m	13d 4h 11m
Critical OSX Patches	Critical Windows Server Patches	Critical Linux Server Patches	Browser Patches	Flash Patches	Java Patches

Flash Versions

Java Versions

Chrome Versions

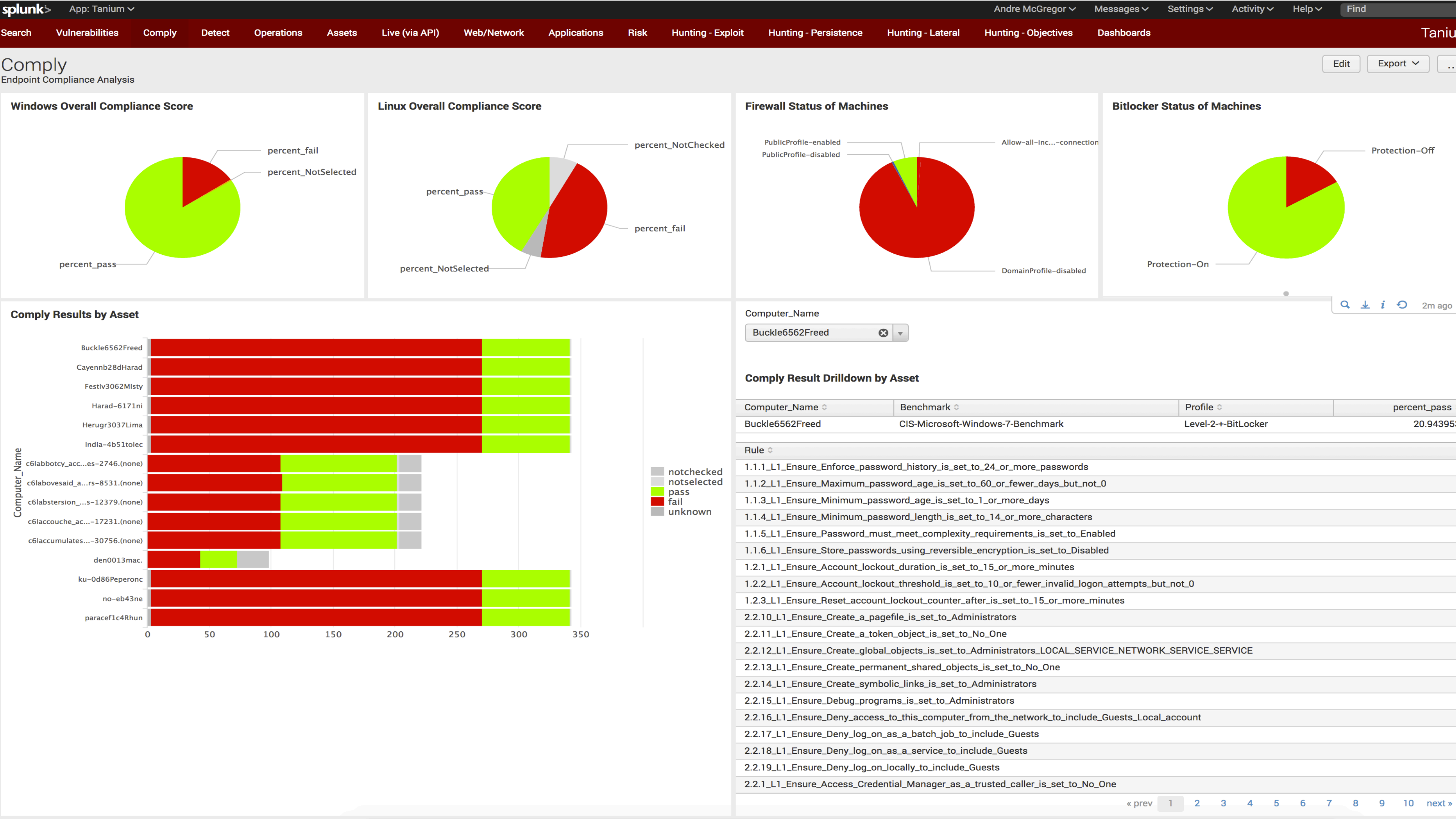
Internet Explorer Versions

Server Patches

Windows Patches

Linux Patches

Patches Required over Time



Comply

Endpoint Compliance Analysis

Windows Overall Compliance Score

Linux Overall Compliance Score

Firewall Status of Machines

Bitlocker Status of Machines

Comply Results by Asset

Computer_Name

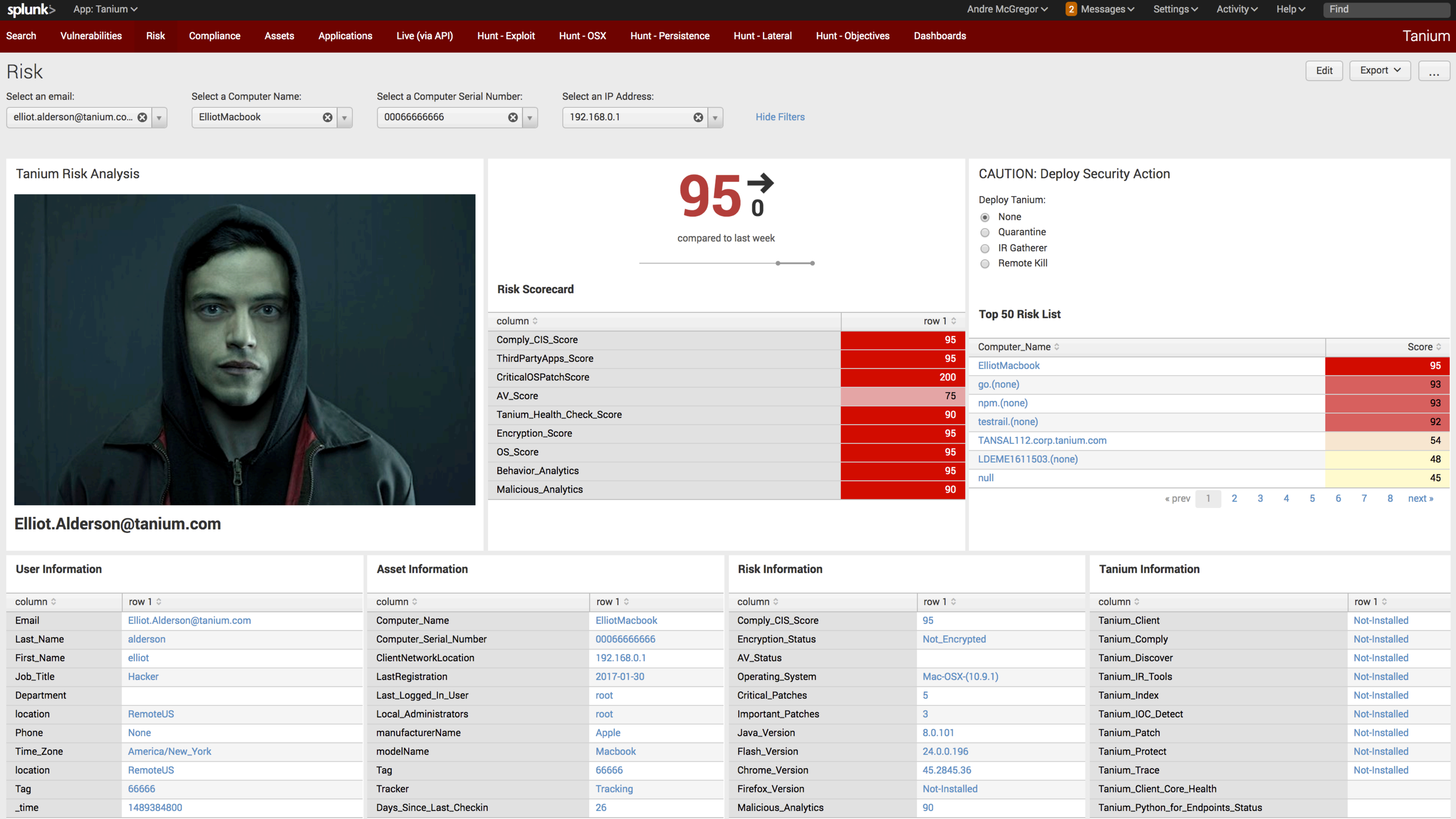
Buckle6562Freed

Comply Result Drilldown by Asset

Computer_Name	Benchmark	Profile	percent_pass
Buckle6562Freed	CIS-Microsoft-Windows-7-Benchmark	Level-2-+-BitLocker	20.94395

Rule
1.1.1_L1_Ensure_Enforce_password_history_is_set_to_24_or_more_passwords
1.1.2_L1_Ensure_Maximum_password_age_is_set_to_60_or_fewer_days_but_not_0
1.1.3_L1_Ensure_Minimum_password_age_is_set_to_1_or_more_days
1.1.4_L1_Ensure_Minimum_password_length_is_set_to_14_or_more_characters
1.1.5_L1_Ensure_Password_must_meet_complexity_requirements_is_set_to_Enabled
1.1.6_L1_Ensure_Store_passwords_using_reversible_encryption_is_set_to_Disabled
1.2.1_L1_Ensure_Account_lockout_duration_is_set_to_15_or_more_minutes
1.2.2_L1_Ensure_Account_lockout_threshold_is_set_to_10_or_fewer_invalid_logon_attempts_but_not_0
1.2.3_L1_Ensure_Reset_account_lockout_counter_after_is_set_to_15_or_more_minutes
2.2.10_L1_Ensure_Create_a_pagefile_is_set_to_Administrators
2.2.11_L1_Ensure_Create_a_token_object_is_set_to_No_One
2.2.12_L1_Ensure_Create_global_objects_is_set_to_Administrators_LOCAL_SERVICE_NETWORK_SERVICE_SERVICE
2.2.13_L1_Ensure_Create_permanent_shared_objects_is_set_to_No_One
2.2.14_L1_Ensure_Create_symbolic_links_is_set_to_Administrators
2.2.15_L1_Ensure_Debug_programs_is_set_to_Administrators
2.2.16_L1_Ensure_Deny_access_to_this_computer_from_the_network_to_include_Guests_Local_account
2.2.17_L1_Ensure_Deny_log_on_as_a_batch_job_to_include_Guests
2.2.18_L1_Ensure_Deny_log_on_as_a_service_to_include_Guests
2.2.19_L1_Ensure_Deny_log_on_locally_to_include_Guests
2.2.1_L1_Ensure_Access_Credential_Manager_as_a_trusted_caller_is_set_to_No_One

« prev 1 2 3 4 5 6 7 8 9 10 next »



Risk

Select an email: elliot.alderson@tanium.co...

Select a Computer Name: ElliotMacbook

Select a Computer Serial Number: 00066666666

Select an IP Address: 192.168.0.1

Tanium Risk Analysis

Elliot.Alderson@tanium.com

95 → 0

compared to last week

Risk Scorecard

column	row 1
Comply_CIS_Score	95
ThirdPartyApps_Score	95
CriticalOSPatchScore	200
AV_Score	75
Tanium_Health_Check_Score	90
Encryption_Score	95
OS_Score	95
Behavior_Analytics	95
Malicious_Analytics	90

CAUTION: Deploy Security Action

Deploy Tanium:

● None
○ Quarantine
○ IR Gatherer
○ Remote Kill

Top 50 Risk List

Computer_Name	Score
ElliotMacbook	95
go.(none)	93
npm.(none)	93
testrail.(none)	92
TANSAL112.corp.tanium.com	54
LDEME1611503.(none)	48
null	45

« prev 1 2 3 4 5 6 7 8 next »

User Information

column	row 1
Email	Elliot.Alderson@tanium.com
Last_Name	alderson
First_Name	elliot
Job_Title	Hacker
Department	
location	RemoteUS
Phone	None
Time_Zone	America/New_York
location	RemoteUS
Tag	66666
_time	1489384800

Asset Information

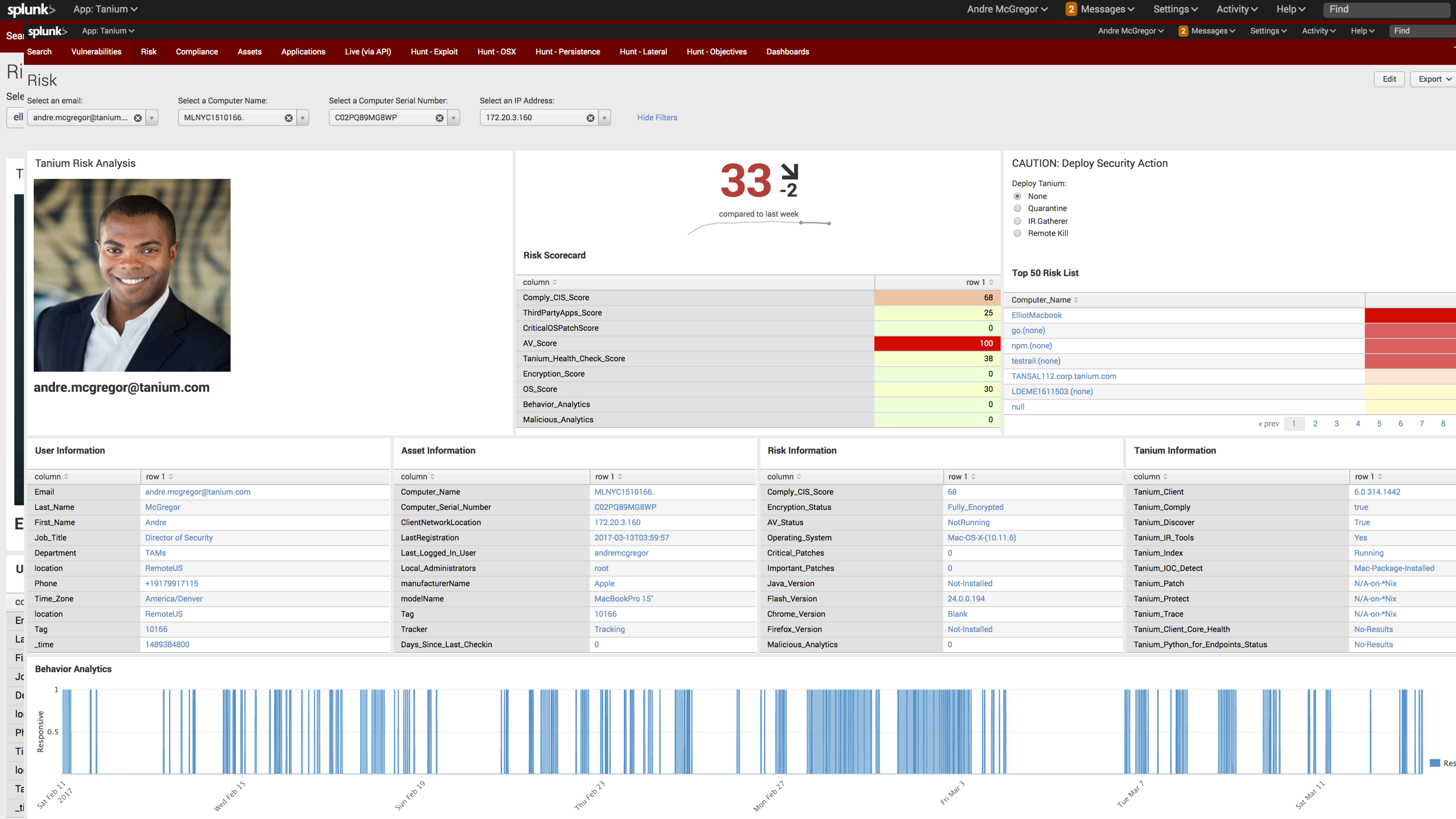
column	row 1
Computer_Name	ElliotMacbook
Computer_Serial_Number	00066666666
ClientNetworkLocation	192.168.0.1
LastRegistration	2017-01-30
Last_Logged_In_User	root
Local_Administrators	root
manufacturerName	Apple
modelName	Macbook
Tag	66666
Tracker	Tracking
Days_Since_Last_Checkin	26

Risk Information

column	row 1
Comply_CIS_Score	95
Encryption_Status	Not_Encrypted
AV_Status	
Operating_System	Mac-OSX-(10.9.1)
Critical_Patches	5
Important_Patches	3
Java_Version	8.0.101
Flash_Version	24.0.0.196
Chrome_Version	45.2845.36
Firefox_Version	Not-Installed
Malicious_Analytics	90

Tanium Information

column	row 1
Tanium_Client	Not-Installed
Tanium_Comply	Not-Installed
Tanium_Discover	Not-Installed
Tanium_IR_Tools	Not-Installed
Tanium_Index	Not-Installed
Tanium_IOC_Detect	Not-Installed
Tanium_Patch	Not-Installed
Tanium_Protect	Not-Installed
Tanium_Trace	Not-Installed
Tanium_Client_Core_Health	
Tanium_Python_for_Endpoints_Status	



Risk

Select an email: andre.mcgregor@tanium....

Select a Computer Name: MLNYC1510166.

Select a Computer Serial Number: C02PQ89MG8WP

Select an IP Address: 172.20.3.160

Tanium Risk Analysis

andre.mcgregor@tanium.com

33 -2

compared to last week

Risk Scorecard

column	row 1
Comply_CIS_Score	68
ThirdPartyApps_Score	25
CriticalOSPatchScore	0
AV_Score	100
Tanium_Health_Check_Score	38
Encryption_Score	0
OS_Score	30
Behavior_Analytics	0
Malicious_Analytics	0

CAUTION: Deploy Security Action

Deploy Tanium:

- ● None
- ○ Quarantine
- ○ IR Gatherer
- ○ Remote Kill

Top 50 Risk List

Computer_Name
ElliotMacbook
go.(none)
npm.(none)
testrail.(none)
TANSAL112.corp.tanium.com
LDEME1611503.(none)
null

« prev 1 2 3 4 5 6 7 8

User Information

column	row 1
Email	andre.mcgregor@tanium.com
Last_Name	McGregor
First_Name	Andre
Job_Title	Director of Security
Department	TAMs
location	RemoteUS
Phone	+19179917115
Time_Zone	America/Denver
location	RemoteUS
Tag	10166
_time	1489384800

Asset Information

column	row 1
Computer_Name	MLNYC1510166.
Computer_Serial_Number	C02PQ89MG8WP
ClientNetworkLocation	172.20.3.160
LastRegistration	2017-03-13T03:59:57
Last_Logged_In_User	andremcgregor
Local_Administrators	root
manufacturerName	Apple
modelName	MacBookPro 15"
Tag	10166
Tracker	Tracking
Days_Since_Last_Checkin	0

Risk Information

column	row 1
Comply_CIS_Score	68
Encryption_Status	Fully_Encrypted
AV_Status	NotRunning
Operating_System	Mac-OS-X-(10.11.6)
Critical_Patches	0
Important_Patches	0
Java_Version	Not-Installed
Flash_Version	24.0.0.194
Chrome_Version	Blank
Firefox_Version	Not-Installed
Malicious_Analytics	0

Tanium Information

column	row 1
Tanium_Client	6.0.314.1442
Tanium_Comply	true
Tanium_Discover	True
Tanium_IR_Tools	Yes
Tanium_Index	Running
Tanium_IOC_Detect	Mac-Package-Installed
Tanium_Patch	N/A-on-*Nix
Tanium_Protect	N/A-on-*Nix
Tanium_Trace	N/A-on-*Nix
Tanium_Client_Core_Health	No-Results
Tanium_Python_for_Endpoints_Status	No-Results

Behavior Analytics

Version 2.0 and Next Steps…

- Automate!
  - –Speed up IR
  - –Score > **80** = send alert!
  - –Score > **50** + other alert = **IR Gatherer!**
  - –Score > **90** + other alert = **Quarantine!**
- Gamification
  - – What’s my Score?
  - – What is my score compared to my peers?
  - – How can I make it better?
  - – Team Scoreboards

CONTROL YOUR FUTURE

TANIUM

CONVERGE 17

Questions?