Beyond the VPN: Fix the Holes In Your Remote Workforce Security Practices

Macy Cronkrite & Samantha Jean-Baptiste

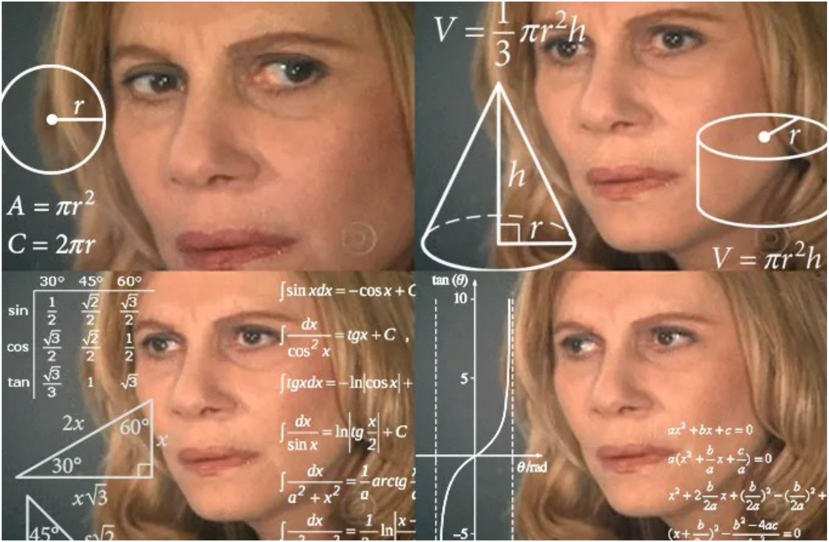
Principal Security Architect & Security Solutions Engineer

Forward-Looking Statements

During the course of this presentation, we may make forward-looking statements regarding future events or plans 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 may differ materially. The forward-looking statements made in the this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, it may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements made herein.

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 functionalities described or to include any such feature or functionality in a future release.

Beyond the VPN

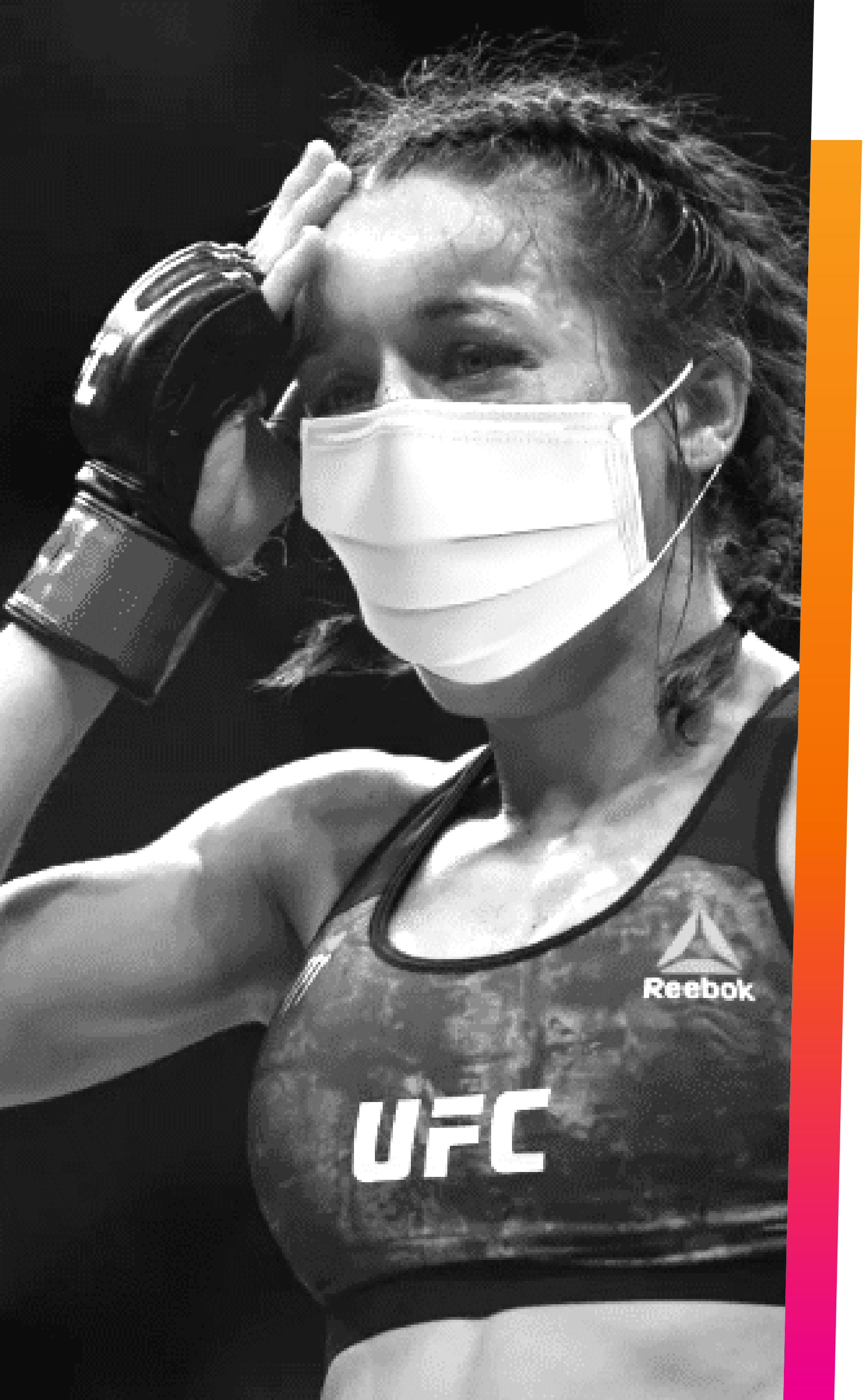


- COVID changed the perimeter
- Map visibility and blind spots
- Communicate with Leadership
- Think about Recovering Safely and Securely

What Did COVID Do to IT?

Incredible changes, short timeframe

- Sudden pivot to remote work made security defense more challenging then ever before.
- Disruption became a new meaning to both work and home life.
- If you didn't think your cyber defense was penetrable then this was the time you would really find out.



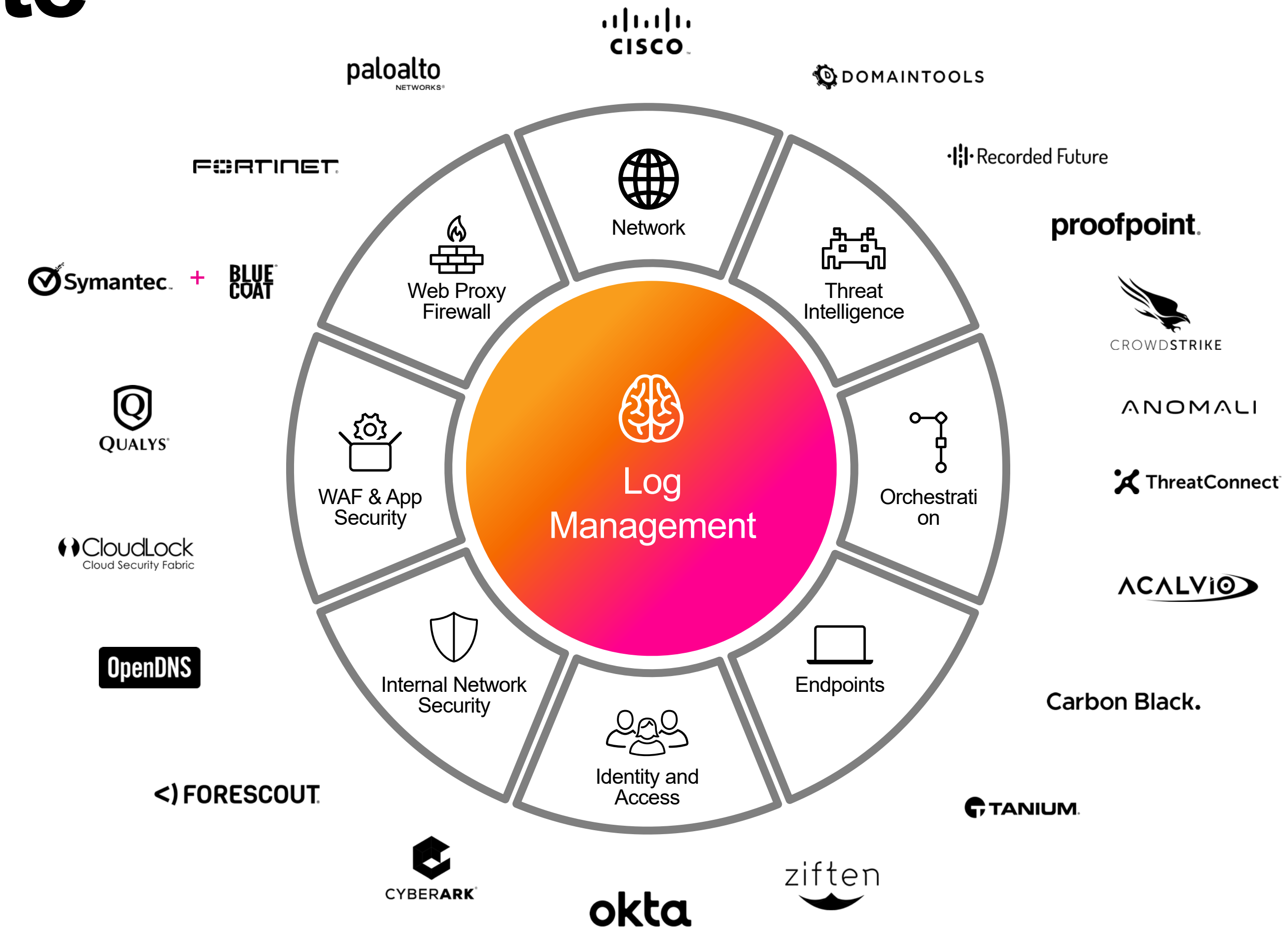
> “Change is difficult, but often essential to survival.”

- Les Brown

Sudden Shift to Remote

SaaS, Shadow IT, BYOD, Token distribution

- We now have an enormous list of remote access option that users can login to corporate networks.
- Hugh potential security gap in end-to-end user activities and interaction with sensitive data.



Legacy Landscape

Why were we limited before the pivot to remote workforce

- SIEM rules probably have VPN
- Support/IT troubleshooting tools might have user to workstation or building but may not have VPN.
- Shift to next gen remote services (VDI, MFA, RDP) may not be incorporated into SIEM or IT Tools.
- How is host and identity resolution achieved with remote user, how many remote paths (mobile/browser only, etc.)?
- How are virtual assets tied to a user?

How Do I Know If We Have This Problem?

What are the chances I need to look at this?

- Along a continuum, broadly.
- Work from home was not allowed or generally not accepted. (1%)
- Executives/VIPs and some IT had remote access (5%)
- Some Work life balance /work from home policy in place
- 10-20% of users deployed.
- Executives/VIPs, IT, Sales, geographically disparate, etc.
- 20-50% of users deployed remotely.

AM I MISSING REMOTE SESSION LOGS
NO, IT'S THE VPN LOGS THAT ARE WRONG
imgflip.com

Assess the Risk / Methodology

How do users access the network, and how do they share resources?

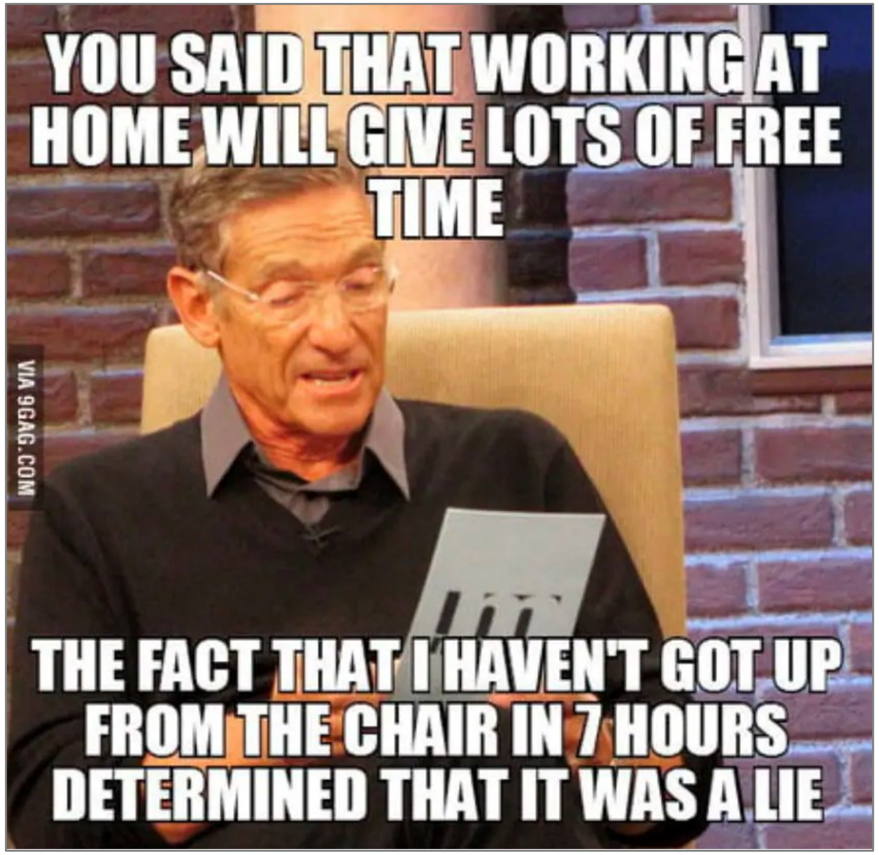
Sooooo...

- Map all known entry points for remote access.
- Verify logs are available for each access system.
- Inspect logs for common user session value key
- Engage Leadership to bridge the gap

New Perimeter – Remote Access

More cloud, more BYOD, more log sources

- Load balancing
- Next Gen Firewalls
- Remote desktop
- Jump Boxes / Bastion hosts / Zero Trust Networks
- Hard / soft tokens
- File Servers, Email
- Chat and Sharing Mobile Device Management
- Cloud VPN technology
- Split Tunneling v Always On VPN
- BYOD , mobile devices, and accessories.
- Private VPN BYOVPN

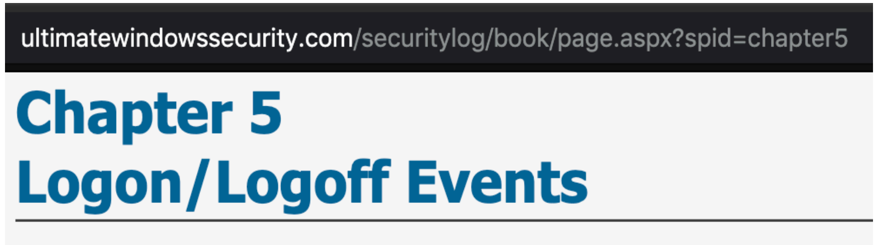

YOU SAID THAT WORKING AT HOME WILL GIVE LOTS OF FREE TIME
THE FACT THAT I HAVEN'T GOT UP FROM THE CHAIR IN 7 HOURS DETERMINED THAT IT WAS A LIE
VIA 9GAG.COM

How to Check Your Environment

If you don't see yourself in the logs…
If you can tie your device to your session.
If you move a file from inside to outside (email, upload web etc.) and can't find the filename.

Then there's a problem

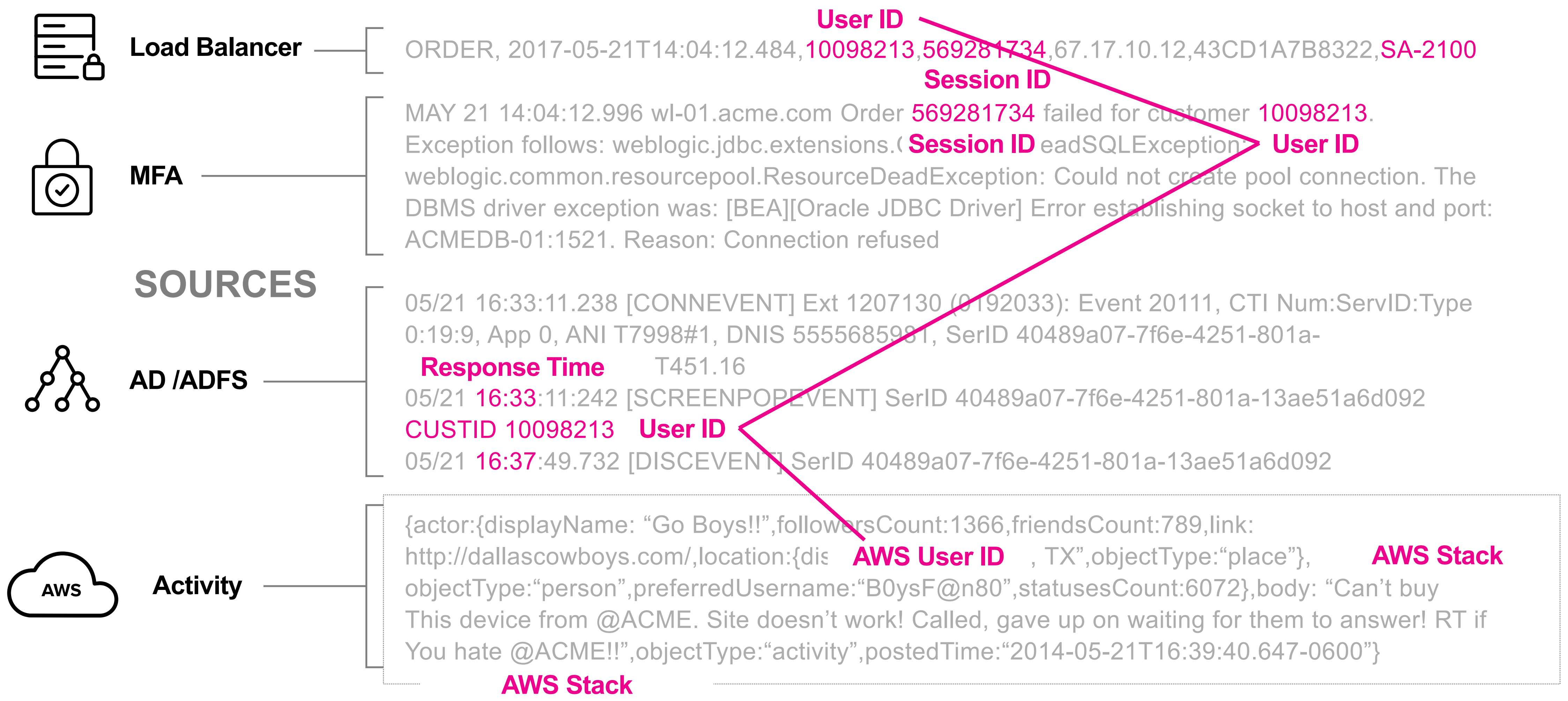
Validate with SME & vendor,
Document gaps and request change fix.



ultimatewindowssecurity.com/securitylog/book/page.aspx?spid=chapter5

Chapter 5
Logon/Logoff Events

Access Data Has Critical Insights



SOURCES

Load Balancer

User ID

```
ORDER, 2017-05-21T14:04:12.484,10098213,569281734,67.17.10.12,43CD1A7B8322,SA-2100
```

Session ID

MFA

```
MAY 21 14:04:12.996 wl-01.acme.com Order 569281734 failed for customer 10098213.
Exception follows: weblogic.jdbc.extensions.( Session ID eadSQLException User ID
weblogic.common.resourcepool.ResourceDeadException: Could not create pool connection. The
DBMS driver exception was: [BEA][Oracle JDBC Driver] Error establishing socket to host and port:
ACMEDB-01:1521. Reason: Connection refused
```

AD /ADFS

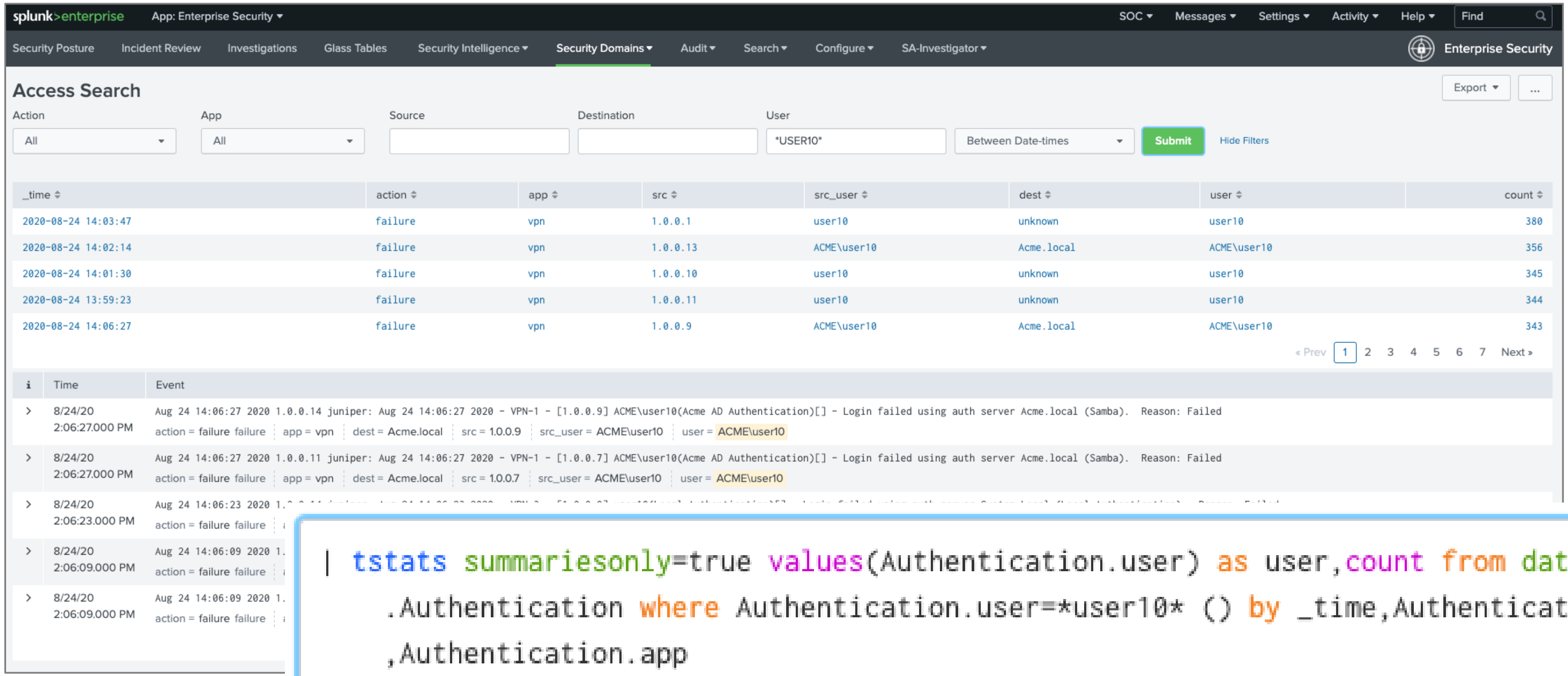
```
05/21 16:33:11.238 [CONNEVENT] Ext 1207130 (0192033): Event 20111, CTI Num:ServID:Type
0:19:9, App 0, ANI T7998#1, DNIS 5555685981, SerID 40489a07-7f6e-4251-801a-
 Response Time      T451.16
05/21 16:33:11:242 [SCREENPOPEVENT] SerID 40489a07-7f6e-4251-801a-13ae51a6d092
CUSTID 10098213   User ID
05/21 16:37:49.732 [DISCEVENT] SerID 40489a07-7f6e-4251-801a-13ae51a6d092
```

Activity

```
{actor:{displayName: "Go Boys!!",followersCount:1366,friendsCount:789,link:
http://dallascowboys.com/,location:{dis AWS User ID , TX",objectType:"place"},      AWS Stack
objectType:"person",preferredUsername:"B0ysF@n80",statusesCount:6072},body: "Can't buy
This device from @ACME. Site doesn't work! Called, gave up on waiting for them to answer! RT if
You hate @ACME!!",objectType:"activity",postedTime:"2014-05-21T16:39:40.647-0600"}
```

AWS Stack

Enterprise Security



Access Search

Action	App	Source	Destination	User			
All ▾	All ▾			*USER10*	Between Date-times ▾	Submit	Hide Filters

_time	action	app	src	src_user	dest	user	count
2020-08-24 14:03:47	failure	vpn	1.0.0.1	user10	unknown	user10	380
2020-08-24 14:02:14	failure	vpn	1.0.0.13	ACME\user10	Acme.local	ACME\user10	356
2020-08-24 14:01:30	failure	vpn	1.0.0.10	user10	unknown	user10	345
2020-08-24 13:59:23	failure	vpn	1.0.0.11	user10	unknown	user10	344
2020-08-24 14:06:27	failure	vpn	1.0.0.9	ACME\user10	Acme.local	ACME\user10	343

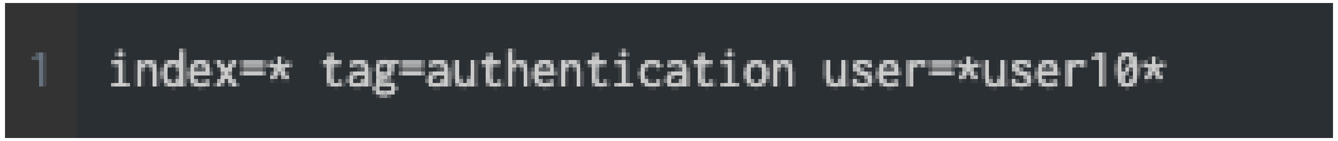
« Prev 1 2 3 4 5 6 7 Next »

i	Time	Event
>	8/24/20 2:06:27.000 PM	Aug 24 14:06:27 2020 1.0.0.14 juniper: Aug 24 14:06:27 2020 - VPN-1 - [1.0.0.9] ACME\user10(Acme AD Authentication)[] - Login failed using auth server Acme.local (Samba). Reason: Failed action = failure failure app = vpn dest = Acme.local src = 1.0.0.9 src_user = ACME\user10 user = ACME\user10
>	8/24/20 2:06:27.000 PM	Aug 24 14:06:27 2020 1.0.0.11 juniper: Aug 24 14:06:27 2020 - VPN-1 - [1.0.0.7] ACME\user10(Acme AD Authentication)[] - Login failed using auth server Acme.local (Samba). Reason: Failed action = failure failure app = vpn dest = Acme.local src = 1.0.0.7 src_user = ACME\user10 user = ACME\user10
>	8/24/20 2:06:23.000 PM	Aug 24 14:06:23 2020 1. action = failure failure
>	8/24/20 2:06:09.000 PM	Aug 24 14:06:09 2020 1. action = failure failure
>	8/24/20 2:06:09.000 PM	Aug 24 14:06:09 2020 1. action = failure failure

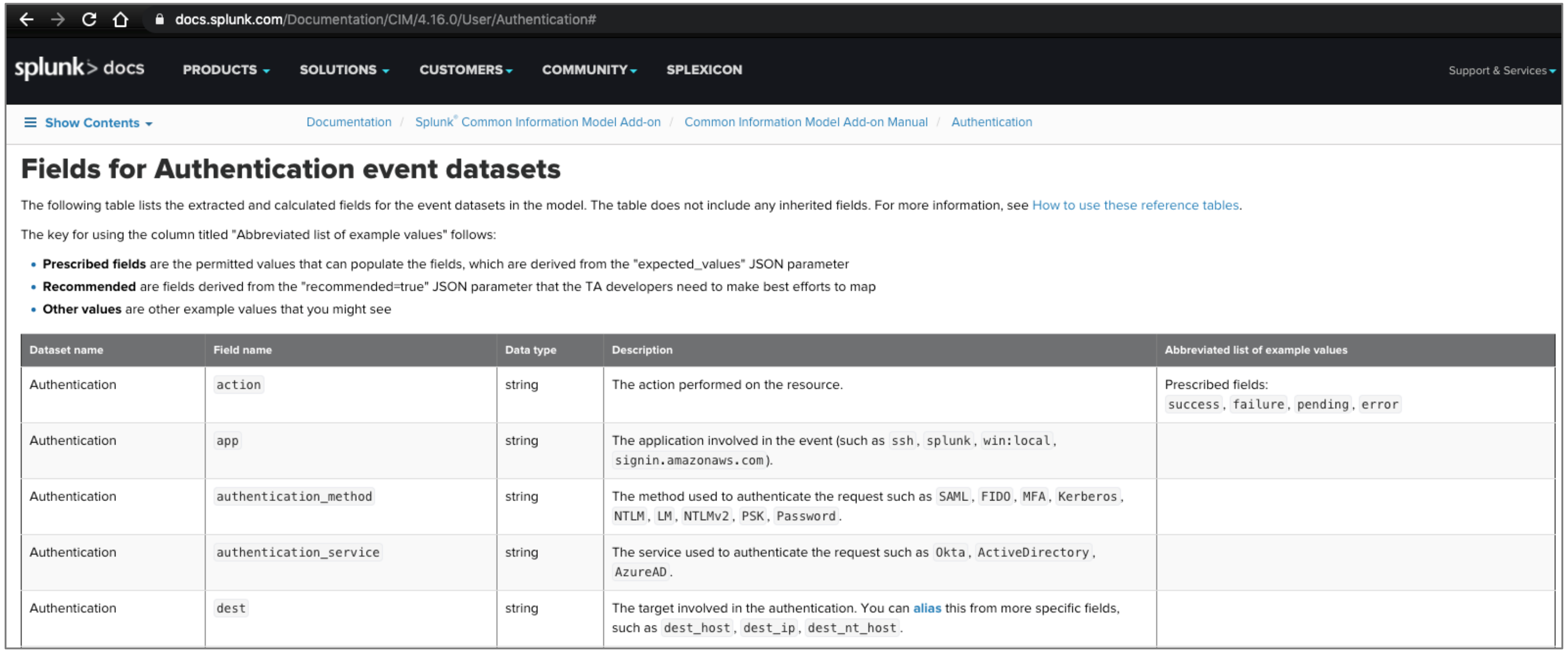
```
| tstats summariesonly=true values(Authentication.user) as user,count from datamodel=Authentication
    .Authentication where Authentication.user=*user10* () by _time,Authentication.src,Authentication.dest
    ,Authentication.app
| rename "Authentication.*" as *
```

Splunk Enterprise and CIM

tag=authentication user=* earliest=-60m



```
index=* tag=authentication user=*user10*
```



docs.splunk.com/Documentation/CIM/4.16.0/User/Authentication#
splunk> docs
PRODUCTS
SOLUTIONS
CUSTOMERS
COMMUNITY
SPLEXICON
Support & Services
Show Contents
Documentation / Splunk® Common Information Model Add-on / Common Information Model Add-on Manual / Authentication

Fields for Authentication event datasets

The following table lists the extracted and calculated fields for the event datasets in the model. The table does not include any inherited fields. For more information, see How to use these reference tables.

The key for using the column titled "Abbreviated list of example values" follows:

- **Prescribed fields** are the permitted values that can populate the fields, which are derived from the "expected_values" JSON parameter
- **Recommended** are fields derived from the "recommended=true" JSON parameter that the TA developers need to make best efforts to map
- **Other values** are other example values that you might see

Dataset name	Field name	Data type	Description	Abbreviated list of example values
Authentication	action	string	The action performed on the resource.	Prescribed fields: success, failure, pending, error
Authentication	app	string	The application involved in the event (such as ssh, splunk, win:local, signin.amazonaws.com).	
Authentication	authentication_method	string	The method used to authenticate the request such as SAML, FIDO, MFA, Kerberos, NTLM, LM, NTLMv2, PSK, Password.	
Authentication	authentication_service	string	The service used to authenticate the request such as Okta, ActiveDirectory, AzureAD.	
Authentication	dest	string	The target involved in the authentication. You can alias this from more specific fields, such as dest_host, dest_ip, dest_nt_host.	

Talk to IT

When modern solutions don't solve modern problems

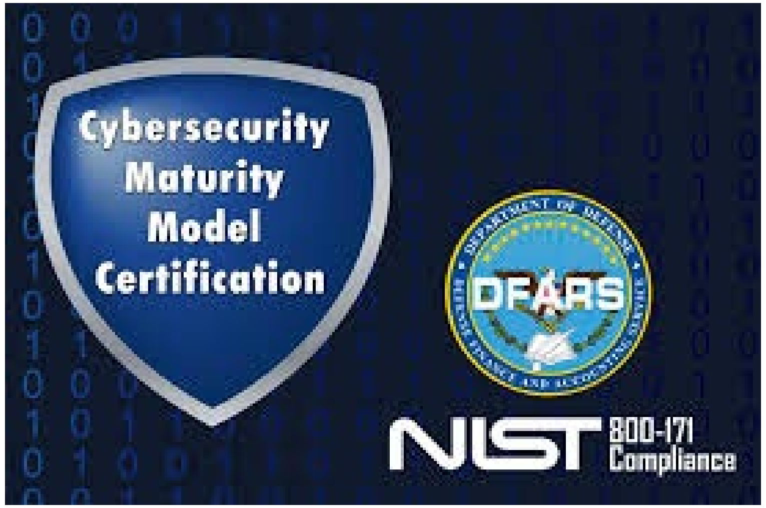
1st law of ~~robotics~~ IT

HR/ Legal will ask the executives for something on a remote user and IT won't have it.

Performance on remote infrastructure or troubleshooting remote access issues will come up, so systems will update soon.

Tools to Help

Back to basics of compliance assets and identities



Zero Trust Network Mindset

NIST
CMMC
CIS20

PROJECT DESCRIPTION

IMPLEMENTING A ZERO TRUST ARCHITECTURE

NIST Special Publication 800-63B

Digital Identity Guidelines

Authentication and Lifecycle Management

CIS Controls™ • CIS Control 6 *This is a basic Control*

Collect, manage, and analyze audit logs of events that could help detect, understand, or recover from an attack.

Leadership – How to Engage

What do they need to accept the risk

Questions they will ask us:

- Explanation of why now and not before?
- How can the cost be offset?
- What steps are being taken to mitigate additional risk to fix.

Answers:

- Rapid shift, priority was functionality, not visibility.
- Covers potential risk leaking, New use cases for reopening plans
- Teamwork is needed Security and IT are aligned.

Leadership – What Do They Want?

What do executives really want vs. technical

Broadly:

- To reduce risk (employees, data, assets, outages)
- Have coverage for HR/Legal Data requests.
- (Data Exfil, User Activity tracing)

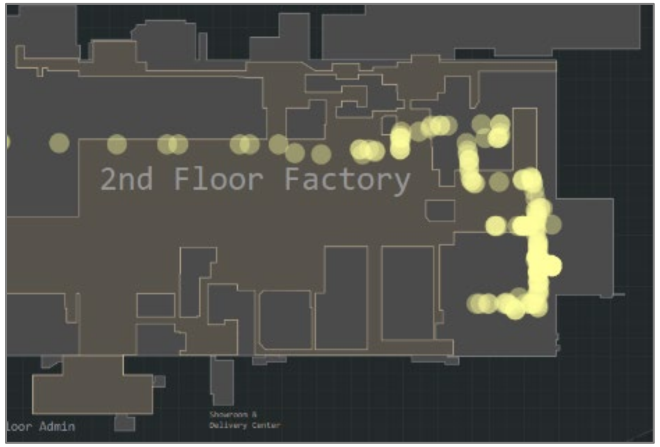
Executive KPIs

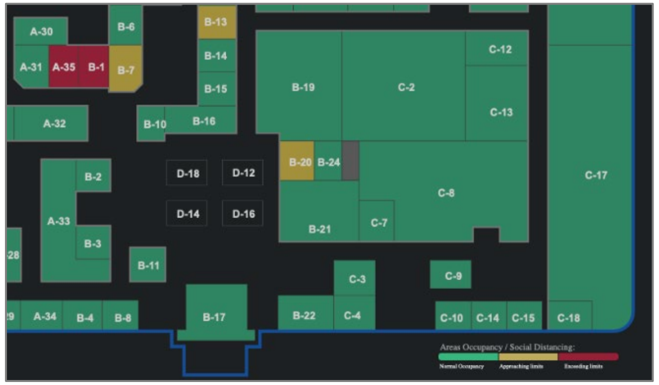
- How many users are being logged, is it correct?
- Productivity (App Access) by user type
- Dashboards with GEO location of employees
- Inside the Building & Around the world
- Connectivity errors for sessions by user type

Leadership – Leverages New Capabilities

What potential benefits from additional logging and analysis

- Recovery – Re-opening in Phases
- Badge In/Out with Wireless Access Point data
- can provide Heatmap inside Buildings
- Device to user heuristic mapping
- Link personal and corporate devices to improve heatmapping.
- Re-opening and Re-closing support
- Help support Social Distancing
- Help support Contact Tracing





Beyond the VPN

- COVID changed the perimeter.
- Map visibility and blind spots
- Communicate with Leadership
- Think about Recovering Safely and Securely

Map your new perimeter | Assume it's all set

Thank You

Please provide feedback via the

SESSION SURVEY