BizWIT

Focus On Security

Advanced Security Monitoring for SMBs without breaking the Bank…

www.bizwit.us

Why Audit Logs Monitoring & Visibility Matters?

1. Are your user’s credentials compromised? How would you know?
2. Who is accessing your emails, email server or file shares? Only authenticated users?
3. Are devices accessing your systems “healthy” or infected?
4. Are suspicious/ malicious programs running on your devices?
5. Are you seeing a lot of failed logon attempts?
6. Are your devices being attacked with brute force or password spray attacks?
7. Are any audit logs being deleted on your servers?
8. Are your servers / devices communicating with suspicious IPs?

These events could be **Indicators of Attack** or **Indicators of Compromise**

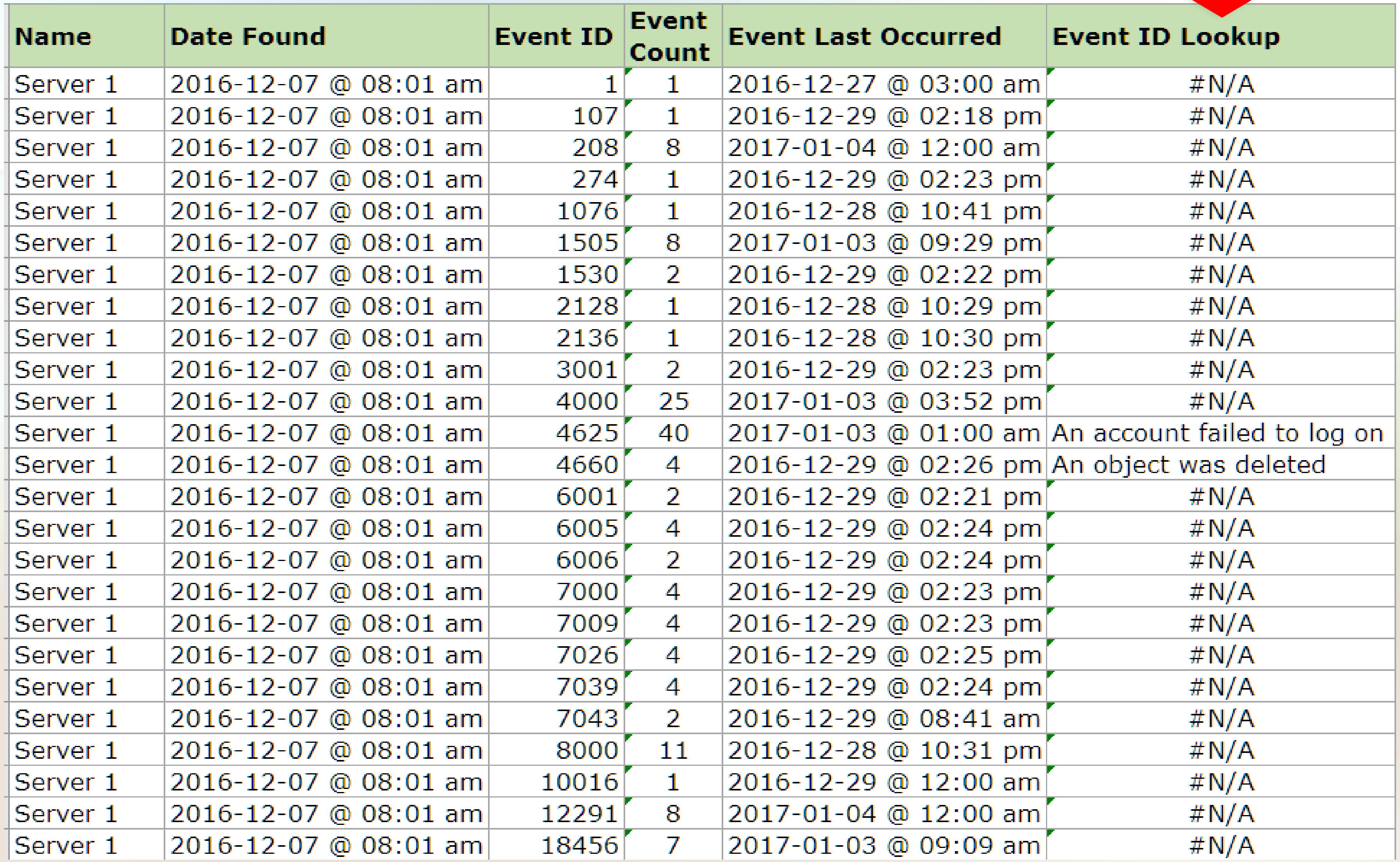
And you want to know about them ASAP!

Not doing Audit Logs Monitoring because of THIS

Audit Logs Monitoring and Analysis

The old way:

- Tedious
- Time consuming
- Ineffective
- Inefficient
- Reactive
- NOT actionable

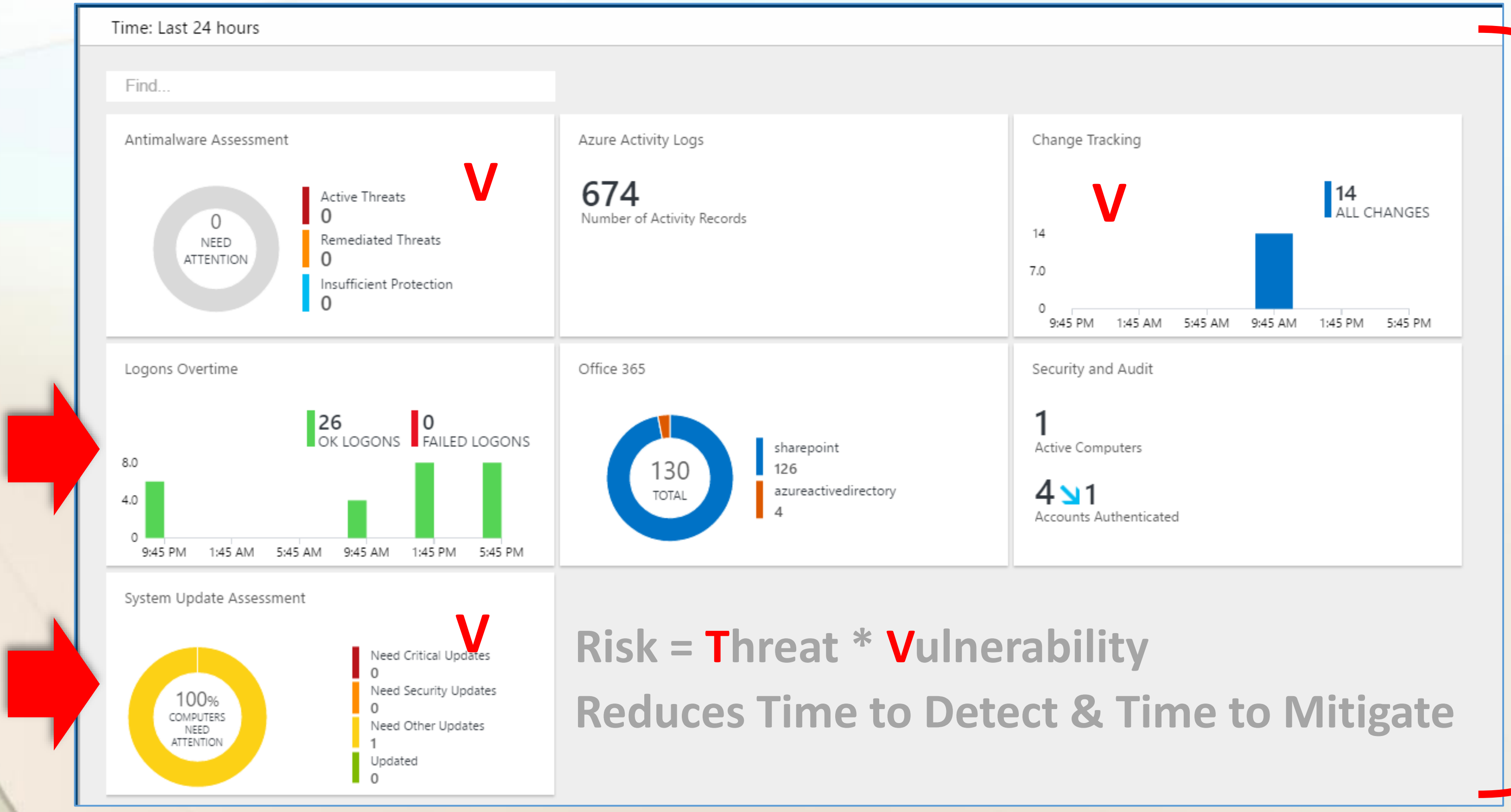


Name	Date Found	Event ID	Event Count	Event Last Occurred	Event ID Lookup
Server 1	2016-12-07 @ 08:01 am	1	1	2016-12-27 @ 03:00 am	#N/A
Server 1	2016-12-07 @ 08:01 am	107	1	2016-12-29 @ 02:18 pm	#N/A
Server 1	2016-12-07 @ 08:01 am	208	8	2017-01-04 @ 12:00 am	#N/A
Server 1	2016-12-07 @ 08:01 am	274	1	2016-12-29 @ 02:23 pm	#N/A
Server 1	2016-12-07 @ 08:01 am	1076	1	2016-12-28 @ 10:41 pm	#N/A
Server 1	2016-12-07 @ 08:01 am	1505	8	2017-01-03 @ 09:29 pm	#N/A
Server 1	2016-12-07 @ 08:01 am	1530	2	2016-12-29 @ 02:22 pm	#N/A
Server 1	2016-12-07 @ 08:01 am	2128	1	2016-12-28 @ 10:29 pm	#N/A
Server 1	2016-12-07 @ 08:01 am	2136	1	2016-12-28 @ 10:30 pm	#N/A
Server 1	2016-12-07 @ 08:01 am	3001	2	2016-12-29 @ 02:23 pm	#N/A
Server 1	2016-12-07 @ 08:01 am	4000	25	2017-01-03 @ 03:52 pm	#N/A
Server 1	2016-12-07 @ 08:01 am	4625	40	2017-01-03 @ 01:00 am	An account failed to log on
Server 1	2016-12-07 @ 08:01 am	4660	4	2016-12-29 @ 02:26 pm	An object was deleted
Server 1	2016-12-07 @ 08:01 am	6001	2	2016-12-29 @ 02:21 pm	#N/A
Server 1	2016-12-07 @ 08:01 am	6005	4	2016-12-29 @ 02:24 pm	#N/A
Server 1	2016-12-07 @ 08:01 am	6006	2	2016-12-29 @ 02:24 pm	#N/A
Server 1	2016-12-07 @ 08:01 am	7000	4	2016-12-29 @ 02:23 pm	#N/A
Server 1	2016-12-07 @ 08:01 am	7009	4	2016-12-29 @ 02:23 pm	#N/A
Server 1	2016-12-07 @ 08:01 am	7026	4	2016-12-29 @ 02:25 pm	#N/A
Server 1	2016-12-07 @ 08:01 am	7039	4	2016-12-29 @ 02:24 pm	#N/A
Server 1	2016-12-07 @ 08:01 am	7043	2	2016-12-29 @ 08:41 am	#N/A
Server 1	2016-12-07 @ 08:01 am	8000	11	2016-12-28 @ 10:31 pm	#N/A
Server 1	2016-12-07 @ 08:01 am	10016	1	2016-12-29 @ 12:00 am	#N/A
Server 1	2016-12-07 @ 08:01 am	12291	8	2017-01-04 @ 12:00 am	#N/A
Server 1	2016-12-07 @ 08:01 am	18456	7	2017-01-03 @ 09:09 am	#N/A

Audit Logs Monitoring and Analysis –The Right Way

Security Incident and Event Management – SIEM

Provides Situational Awareness and Actionable Information



Time: Last 24 hours

Find...

Antimalware Assessment

0 NEED ATTENTION

Active Threats 0

Remediated Threats 0

Insufficient Protection 0

Azure Activity Logs

674 Number of Activity Records

Change Tracking

14 ALL CHANGES

Logons Overtime

26 OK LOGONS

0 FAILED LOGONS

Office 365

130 TOTAL

sharepoint 126

azureactivedirectory 4

Security and Audit

1 Active Computers

4 ↘ 1 Accounts Authenticated

System Update Assessment

100% COMPUTERS NEED ATTENTION

Need Critical Updates 0

Need Security Updates 0

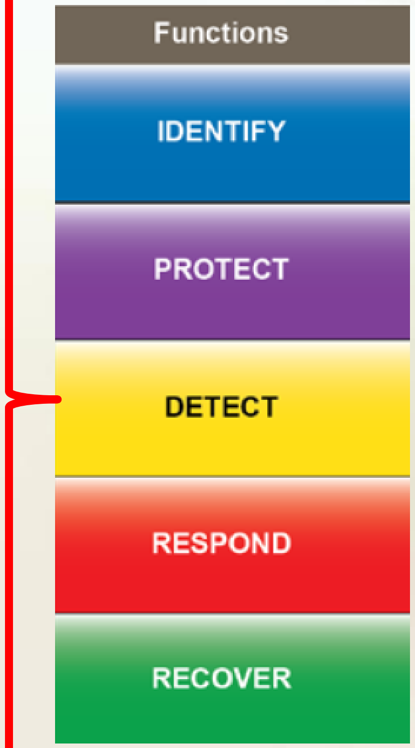
Need Other Updates 1

Updated 0

Risk = Threat * Vulnerability

Reduces Time to Detect & Time to Mitigate

NIST CSF



Functions

IDENTIFY

PROTECT

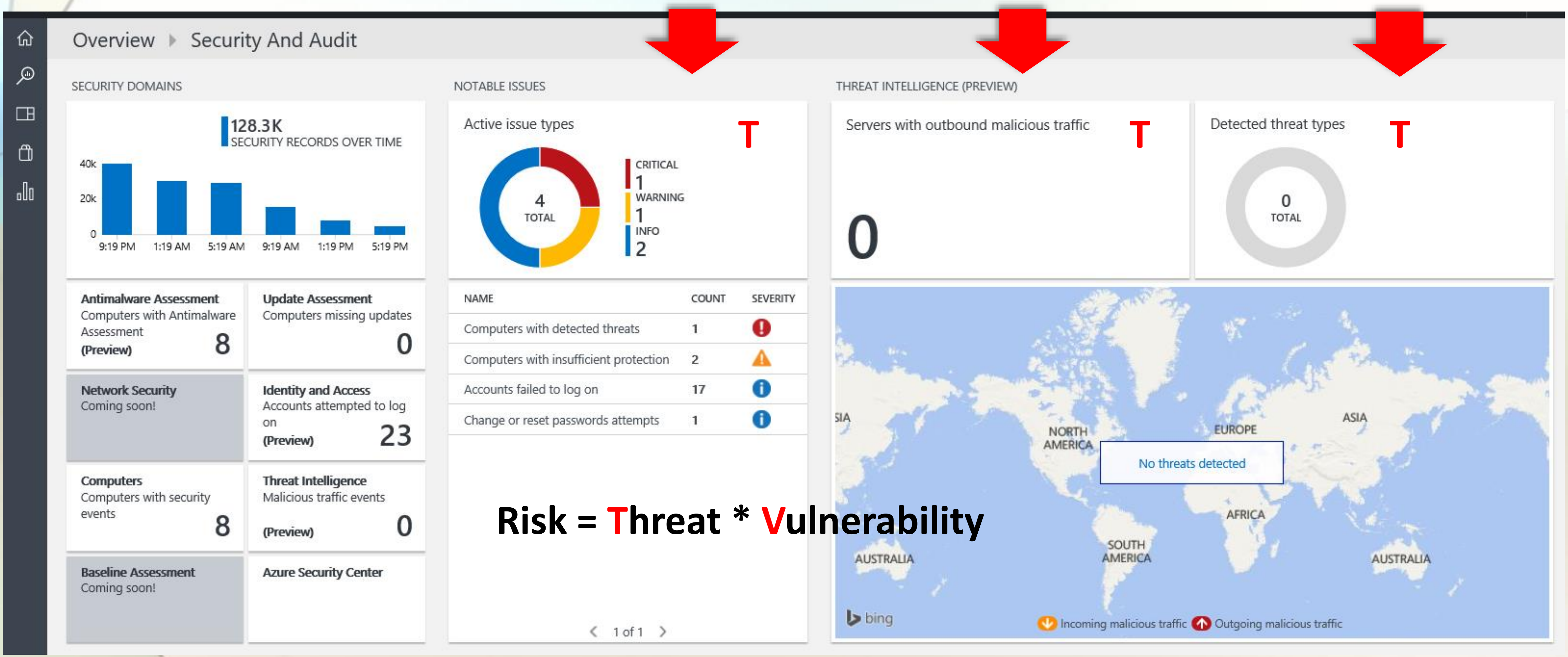
DETECT

RESPOND

RECOVER

Visibility Reduces Impact and Cost of Incident Response

Time to Detect => Time to Mitigate => Cost of Security Incident



Overview ▸ Security And Audit

SECURITY DOMAINS

128.3K
SECURITY RECORDS OVER TIME

Antimalware Assessment
Computers with Antimalware Assessment
(Preview) 8

Update Assessment
Computers missing updates 0

Network Security
Coming soon!

Identity and Access
Accounts attempted to log on
(Preview) 23

Computers
Computers with security events 8

Threat Intelligence
Malicious traffic events
(Preview) 0

Baseline Assessment
Coming soon!

Azure Security Center

NOTABLE ISSUES

Active issue types **T**

4
TOTAL

CRITICAL
1
WARNING
1
INFO
2

NAME	COUNT	SEVERITY
Computers with detected threats	1	!
Computers with insufficient protection	2	⚠
Accounts failed to log on	17	ℹ
Change or reset passwords attempts	1	ℹ

‹ 1 of 1 ›

THREAT INTELLIGENCE (PREVIEW)

Servers with outbound malicious traffic **T**

0

Detected threat types **T**

0
TOTAL

No threats detected

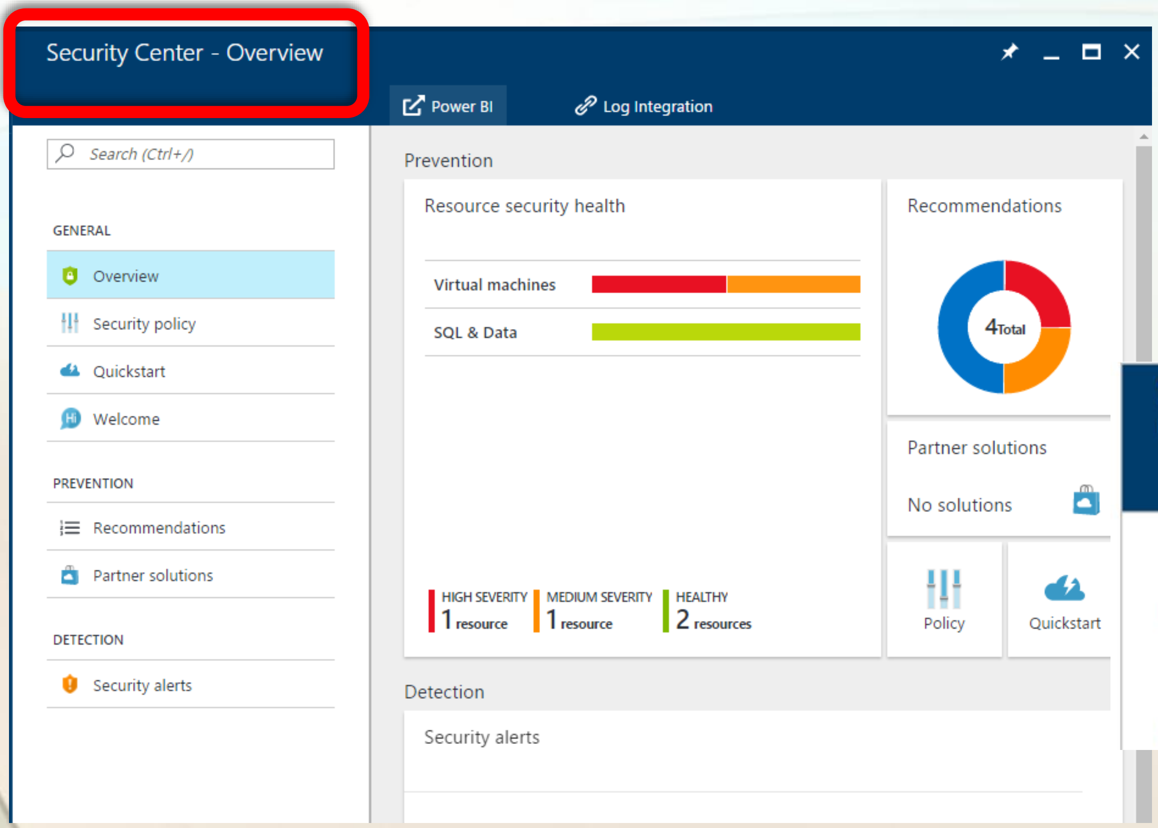
Incoming malicious traffic
Outgoing malicious traffic

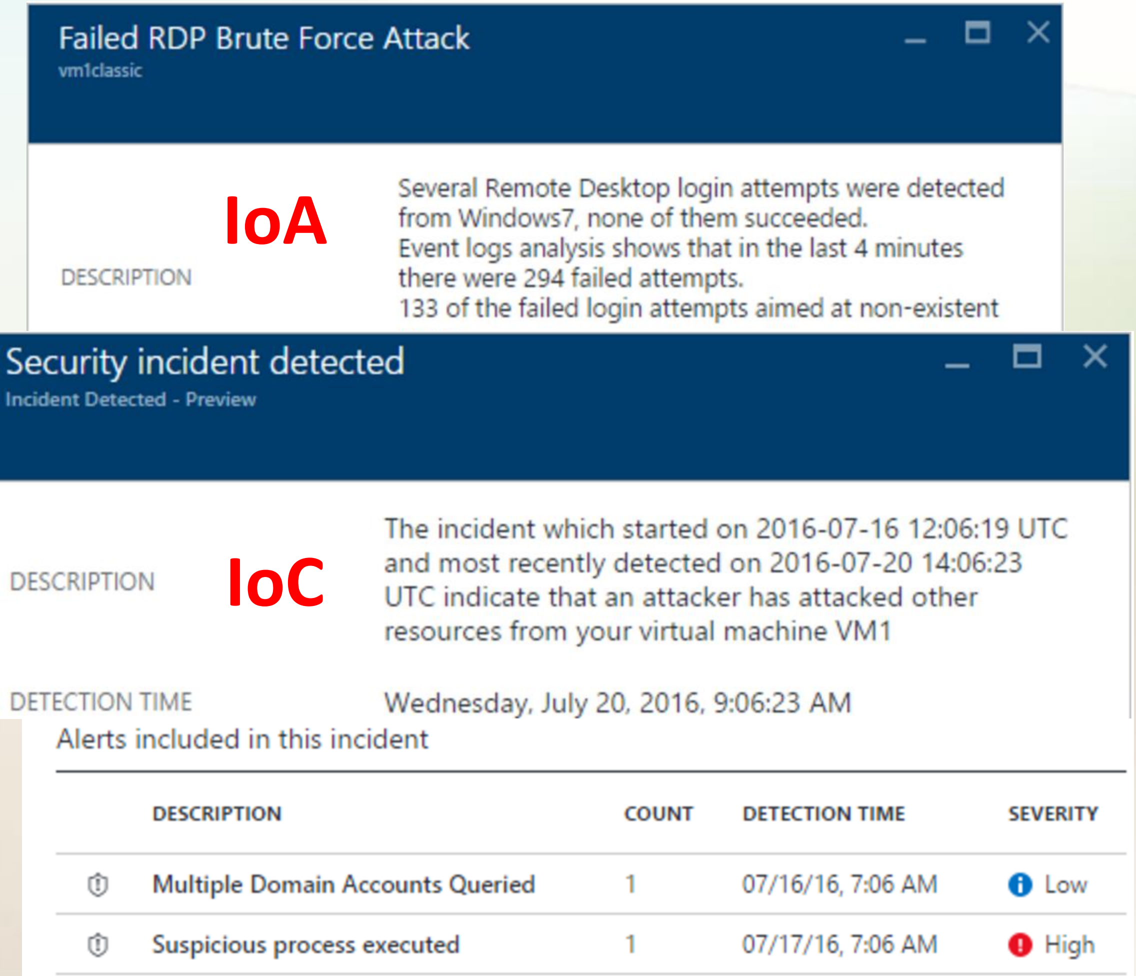
Risk = Threat * Vulnerability

Incident Detection in the Cloud – Automation

IoA – Indicators of Attack

IoC - Indicators of Compromise




Failed RDP Brute Force Attack
vm1classic

IoA

DESCRIPTION: Several Remote Desktop login attempts were detected from Windows7, none of them succeeded. Event logs analysis shows that in the last 4 minutes there were 294 failed attempts. 133 of the failed login attempts aimed at non-existent

Security incident detected
Incident Detected - Preview

IoC

DESCRIPTION: The incident which started on 2016-07-16 12:06:19 UTC and most recently detected on 2016-07-20 14:06:23 UTC indicate that an attacker has attacked other resources from your virtual machine VM1

DETECTION TIME: Wednesday, July 20, 2016, 9:06:23 AM

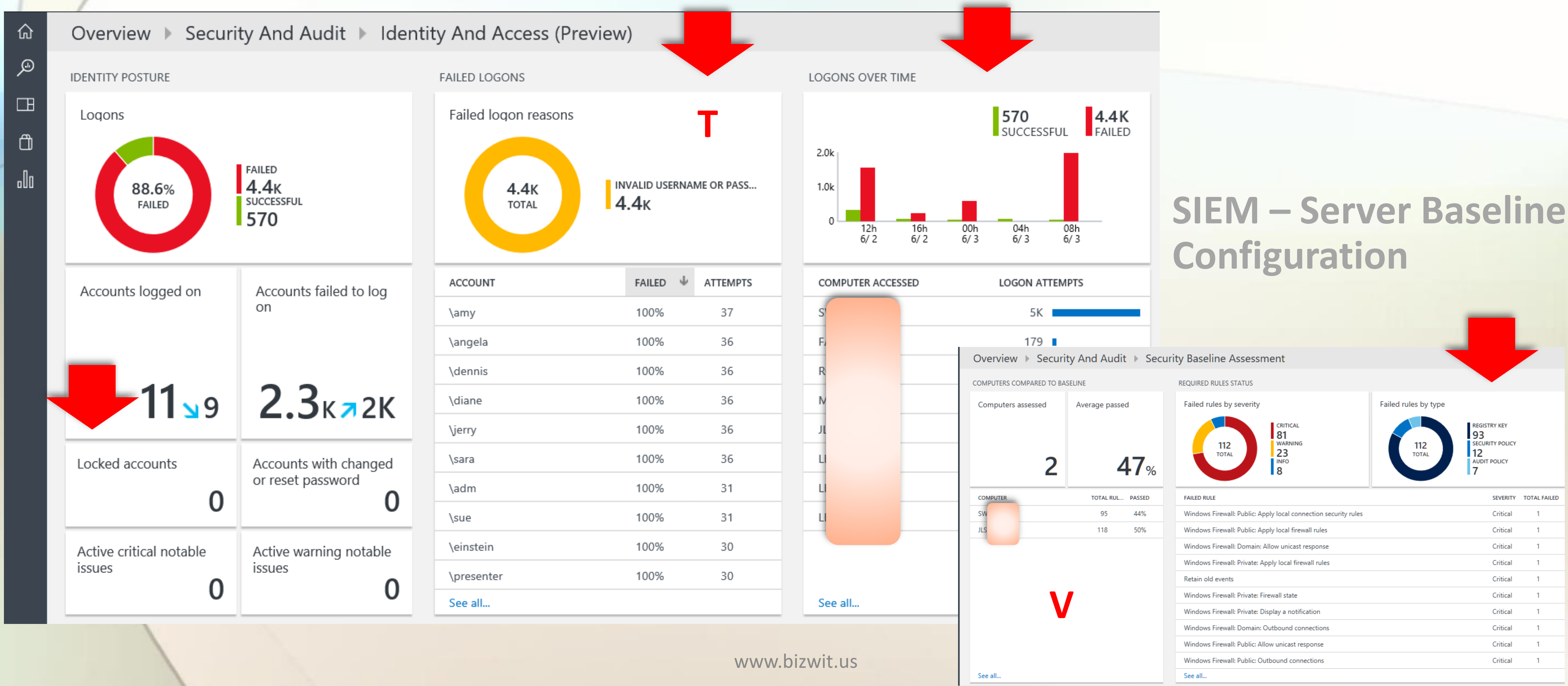
Alerts included in this incident

DESCRIPTION	COUNT	DETECTION TIME	SEVERITY
Multiple Domain Accounts Queried	1	07/16/16, 7:06 AM	Low
Suspicious process executed	1	07/17/16, 7:06 AM	High

www.bizwit.us

Incident Detection on Premises - Automation

Access Controls & Identity Management – Actionable Information



Overview › Security And Audit › Identity And Access (Preview)

IDENTITY POSTURE

Logons

Accounts logged on	Accounts failed to log on
11 ↘ 9	2.3K ↗ 2K

Locked accounts	Accounts with changed or reset password
0	0

Active critical notable issues	Active warning notable issues
0	0

FAILED LOGONS

Failed logon reasons

T

ACCOUNT	FAILED	ATTEMPTS
\amy	100%	37
\angela	100%	36
\dennis	100%	36
\diane	100%	36
\jerry	100%	36
\sara	100%	36
\adm	100%	31
\sue	100%	31
\einstein	100%	30
\presenter	100%	30

See all...

LOGONS OVER TIME

COMPUTER ACCESSED	LOGON ATTEMPTS
[redacted]	5K
[redacted]	179
[redacted]	
[redacted]	
[redacted]	
[redacted]	
[redacted]	
[redacted]	

See all...

SIEM – Server Baseline Configuration

Overview › Security And Audit › Security Baseline Assessment

COMPUTERS COMPARED TO BASELINE

Computers assessed	Average passed
2	47%

COMPUTER	TOTAL RUL...	PASSED
SW[redacted]	95	44%
JLS[redacted]	118	50%

V

See all...

REQUIRED RULES STATUS

Failed rules by severity

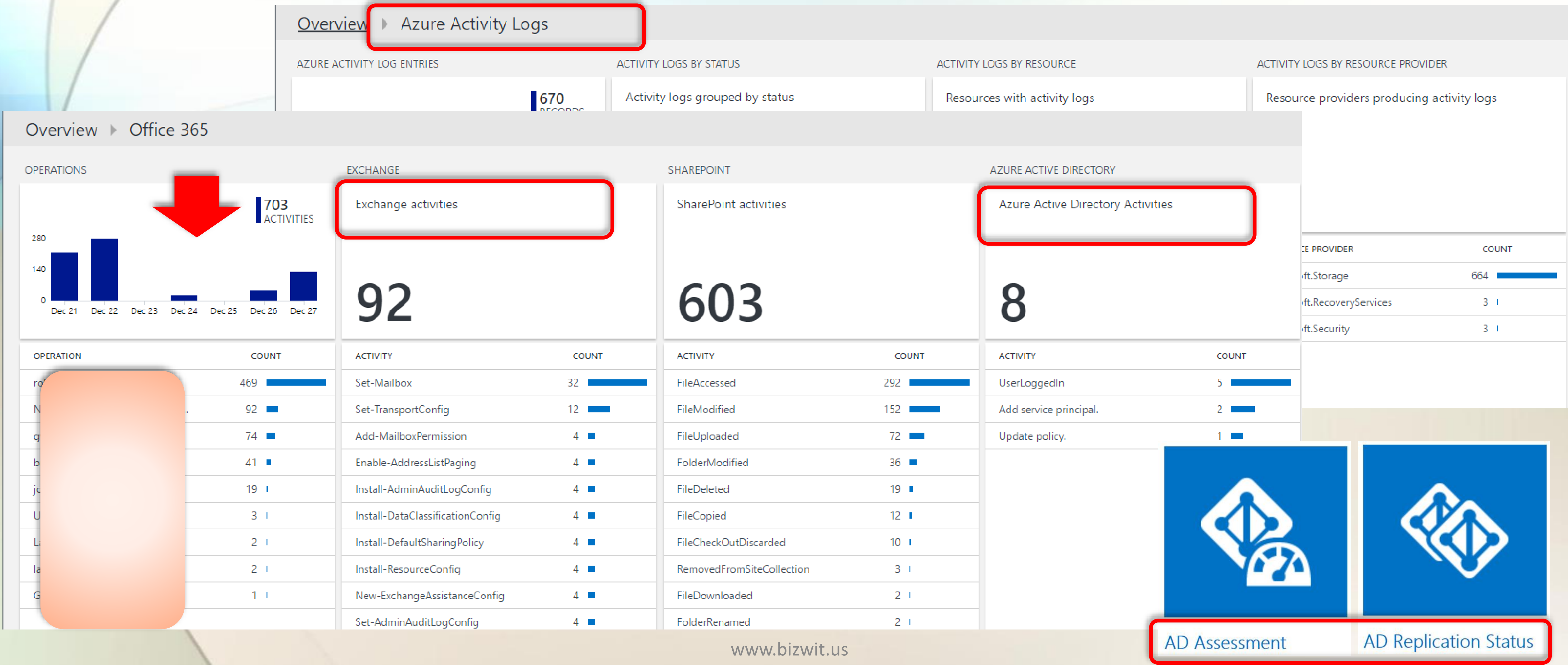
Failed rules by type

FAILED RULE	SEVERITY	TOTAL FAILED
Windows Firewall: Public: Apply local connection security rules	Critical	1
Windows Firewall: Public: Apply local firewall rules	Critical	1
Windows Firewall: Domain: Allow unicast response	Critical	1
Windows Firewall: Private: Apply local firewall rules	Critical	1
Retain old events	Critical	1
Windows Firewall: Private: Firewall state	Critical	1
Windows Firewall: Private: Display a notification	Critical	1
Windows Firewall: Domain: Outbound connections	Critical	1
Windows Firewall: Public: Allow unicast response	Critical	1
Windows Firewall: Public: Outbound connections	Critical	1

See all...

Cloud Infrastructure Security Visibility

SIEM – Visibility into Operations, Azure, AD and Office 365 and Devices



Overview ▸ Azure Activity Logs

AZURE ACTIVITY LOG ENTRIES

670 RECORDS

ACTIVITY LOGS BY STATUS

Activity logs grouped by status

ACTIVITY LOGS BY RESOURCE

Resources with activity logs

ACTIVITY LOGS BY RESOURCE PROVIDER

Resource providers producing activity logs

E PROVIDER	COUNT
ft.Storage	664
ft.RecoveryServices	3
ft.Security	3

Overview ▸ Office 365

OPERATIONS

703 ACTIVITIES

OPERATION	COUNT
[redacted]	469
[redacted]	92
[redacted]	74
[redacted]	41
[redacted]	19
[redacted]	3
[redacted]	2
[redacted]	2
[redacted]	1

EXCHANGE

Exchange activities

92

ACTIVITY	COUNT
Set-Mailbox	32
Set-TransportConfig	12
Add-MailboxPermission	4
Enable-AddressListPaging	4
Install-AdminAuditLogConfig	4
Install-DataClassificationConfig	4
Install-DefaultSharingPolicy	4
Install-ResourceConfig	4
New-ExchangeAssistanceConfig	4
Set-AdminAuditLogConfig	4

SHAREPOINT

SharePoint activities

603

ACTIVITY	COUNT
FileAccessed	292
FileModified	152
FileUploaded	72
FolderModified	36
FileDeleted	19
FileCopied	12
FileCheckOutDiscarded	10
RemovedFromSiteCollection	3
FileDownloaded	2
FolderRenamed	2

AZURE ACTIVE DIRECTORY

Azure Active Directory Activities

8

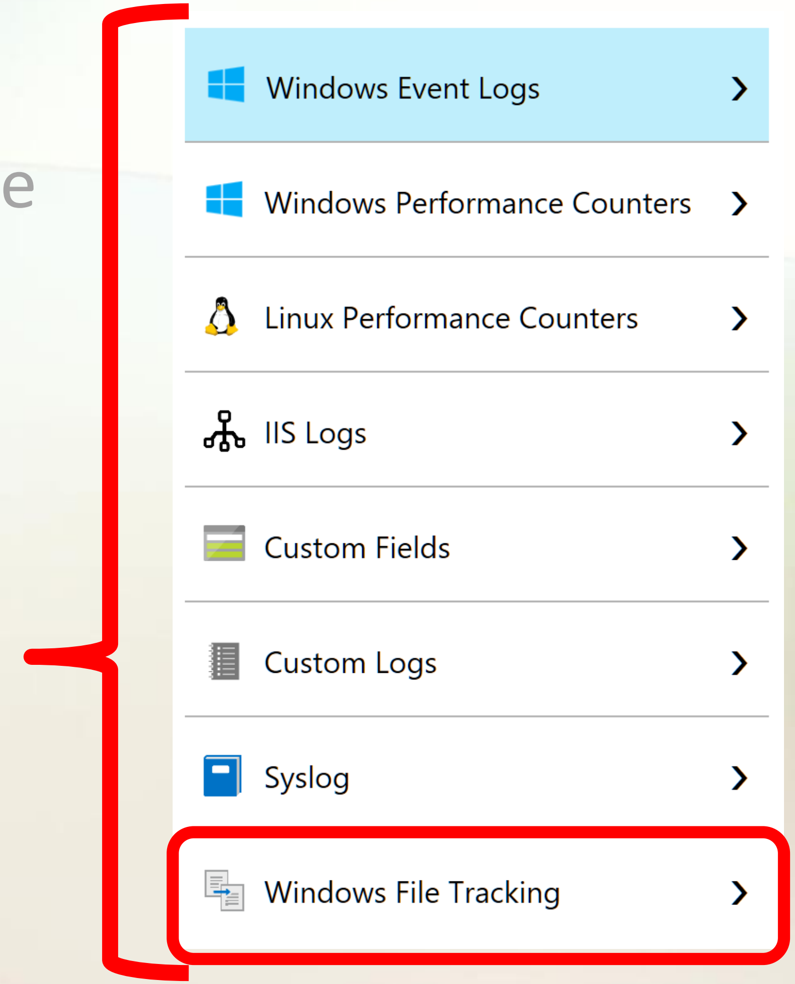
ACTIVITY	COUNT
UserLoggedIn	5
Add service principal.	2
Update policy.	1

AD Assessment

AD Replication Status

Security on Premises and in the Cloud
Automation Reduces Cost

- **Professional configuration** of Office 365 / Azure AD/ Azure or any Cloud environment (policies)
- **Secured privileged** and **remote** access – MFA Multi Factor Authentication
- **Robust data collection, storage, reporting and auditing**
- **Automated visibility** – incident Prevention & Detection
- **Ongoing monitoring & incident response**



Seeing is Believing ;o)

BizwIT
Focus On Security

Robert Brzezinski CISA, CHPS
Bizwit LLC
Columbus, Ohio
Robert.Brzezinski@bizwit.us

QUALYS®

Microsoft Partner