



XYGATE SecurityOne® All Systems Dashboard

Recent Activity
Last Logon on 7/21/2020

Overview

[Customize](#)

24 [^]

Critical Incidents occurred today

8 [^]

EXPAND Operations since last logon

31 [^]

Collection Aborted since last logon

COMPLIANCE

System is Compliant as of 9/4/2020 ⓘ

423 [^]

Alerts on 9/4/2020

249 [^]

Incidents on 9/4/2020

Alerts (423)

Added (159) Removed (134) Modified (145)

Top 5 results

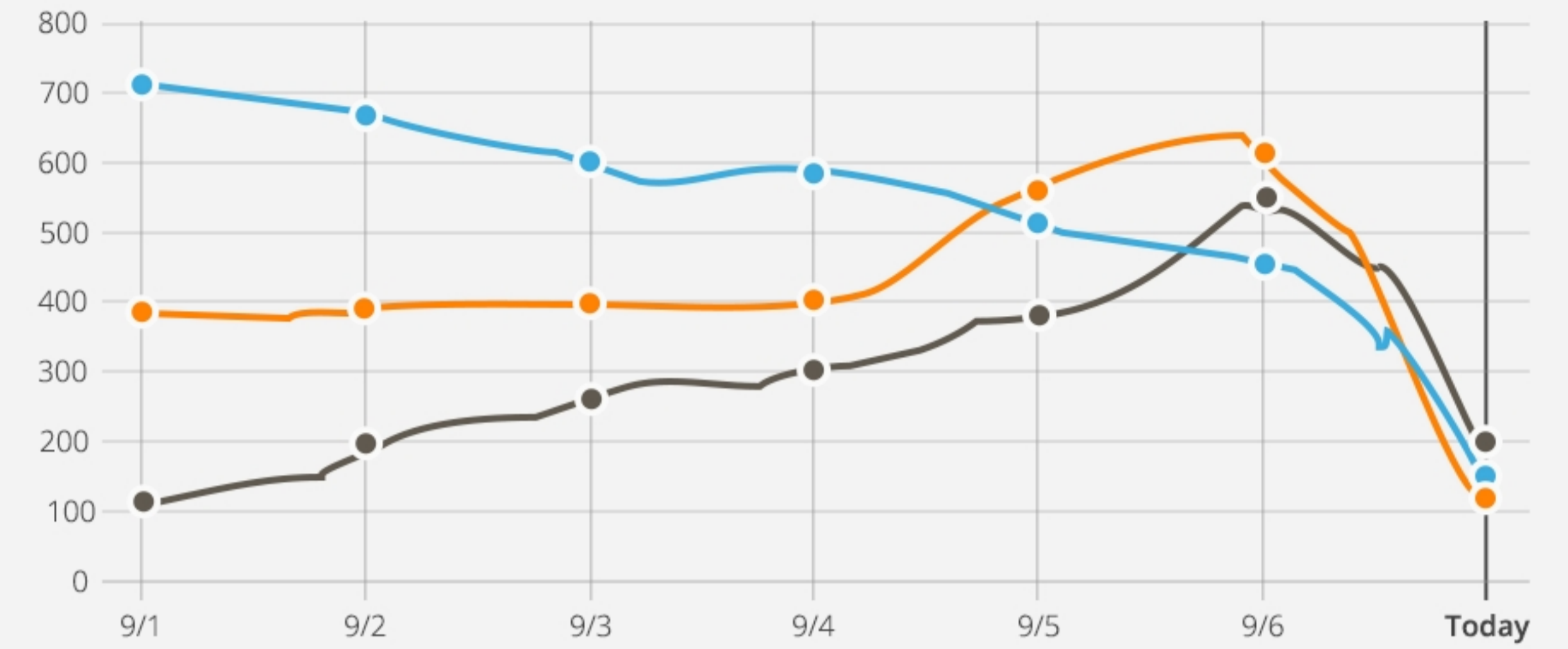
Most Recent ▾

- APconnectionPool-Test 1
- AP-User
- AP Connection Test Pool Test 2
- AP GuardianFile Connection Pool test 3
- APIAuditPoolSF

[View all](#)

Total activity last week

Last Scan: 2019-09-13 00:00:00.000 UTC



ASM

CLIM
Devices ⓘ



NSC
Devices ⓘ



Incidents (692)

Critical (140) Major (76) Minor (33)

Top 5 results

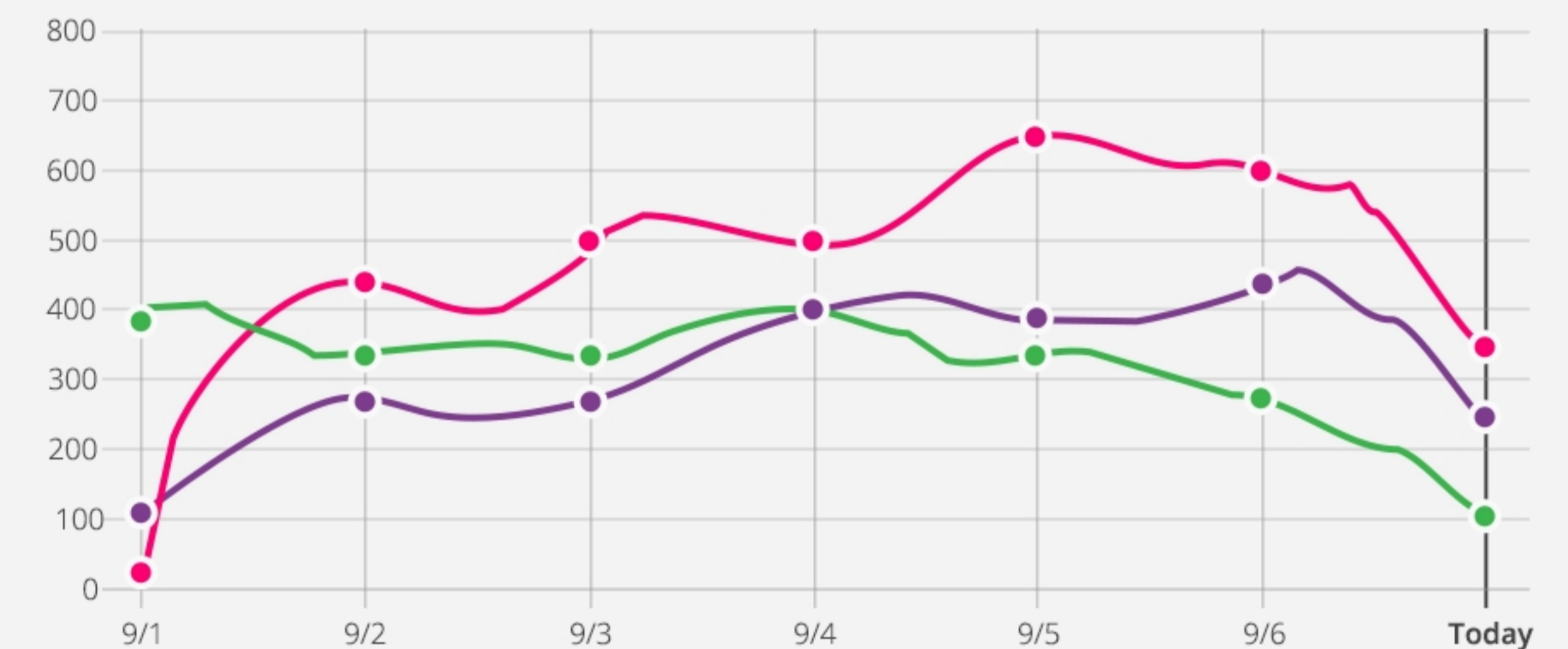
Criticality ▾

- Successful log on after multiple failed attempts
- A file READ across EXPAND was detected
- NonStop user sessions multiple failed attempts
- Unauthorized NonStop file changes
- NonStop user logged on as SUPER.SUPER

[View all](#)

Total activity last week

Last Scan: 2019-09-13 00:00:00.000 UTC



Compliance

Passed Failed Error Not Scanned

Status	Framework	Time of scan	Previous scan
ⓘ	HPE NonStop Security Hardening Guide See Results	4 days ago 10/25/2019 at 01:50AM UTC	34 days ago 09/26/2019 at 11:14AM UTC
✔	PCI-DSS 3.2.1 See Results	4 days ago 10/25/2019 at 11:50PM UTC	5 days ago 10/24/2019 at 11:50PM UTC

CONTENT PROPAGATED BY INTERACTION WITH RESULT ACTIVITY FROM

- GLOBAL SEARCH RESULTS
- ACTIVE UI ELEMENTS INTERACTION
- RESULTS USER INTERACTED WITH



XYGATE SecurityOne® All Systems Dashboard

Recent Activity
Last Logon on 7/21/2020

Overview

[Customize](#)

24 [⤴]

Critical Incidents occurred today

8 [⤴]

EXPAND Operations since last logon

31 [⤴]

Collection Aborted since last logon

COMPLIANCE

System is Compliant as of 9/4/2020 ⓘ

423 [⤴]

Alerts on 9/4/2020

249 [⤴]

Incidents on 9/4/2020

Alerts (423)

Added (159) Removed (134) Modified (145)

Top 5 results

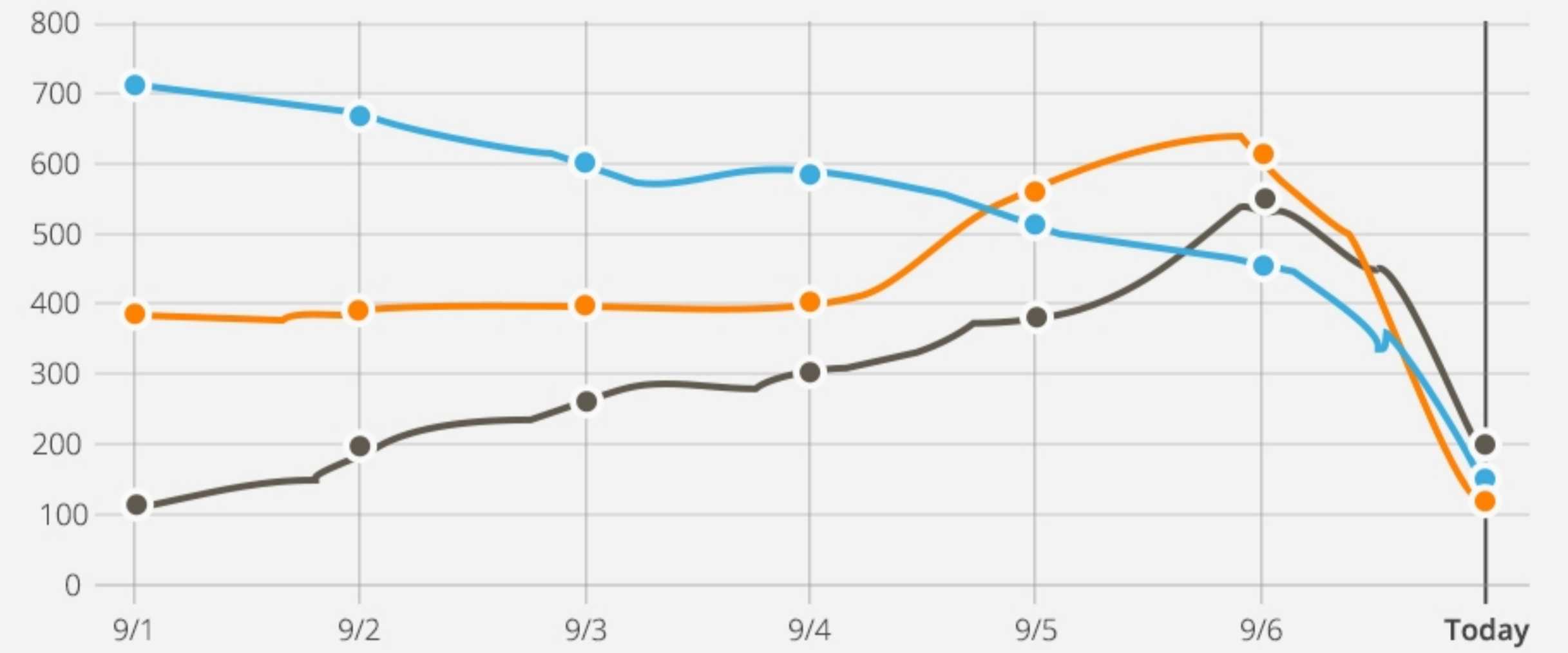
Most Recent ▾

- APconnectionPool-Test 1
- AP-User
- AP Connection Test Pool Test 2
- AP GuardianFile Connection Pool test 3
- APIAuditPoolSF

[View all](#)

Total activity last week

Last Scan: 2019-09-13 00:00:00.000 UTC



ASM

CLIM
Devices ⓘ

NSC
Devices ⓘ



Incidents (692)

Critical (140) Major (76) Minor (33)

Top 5 results

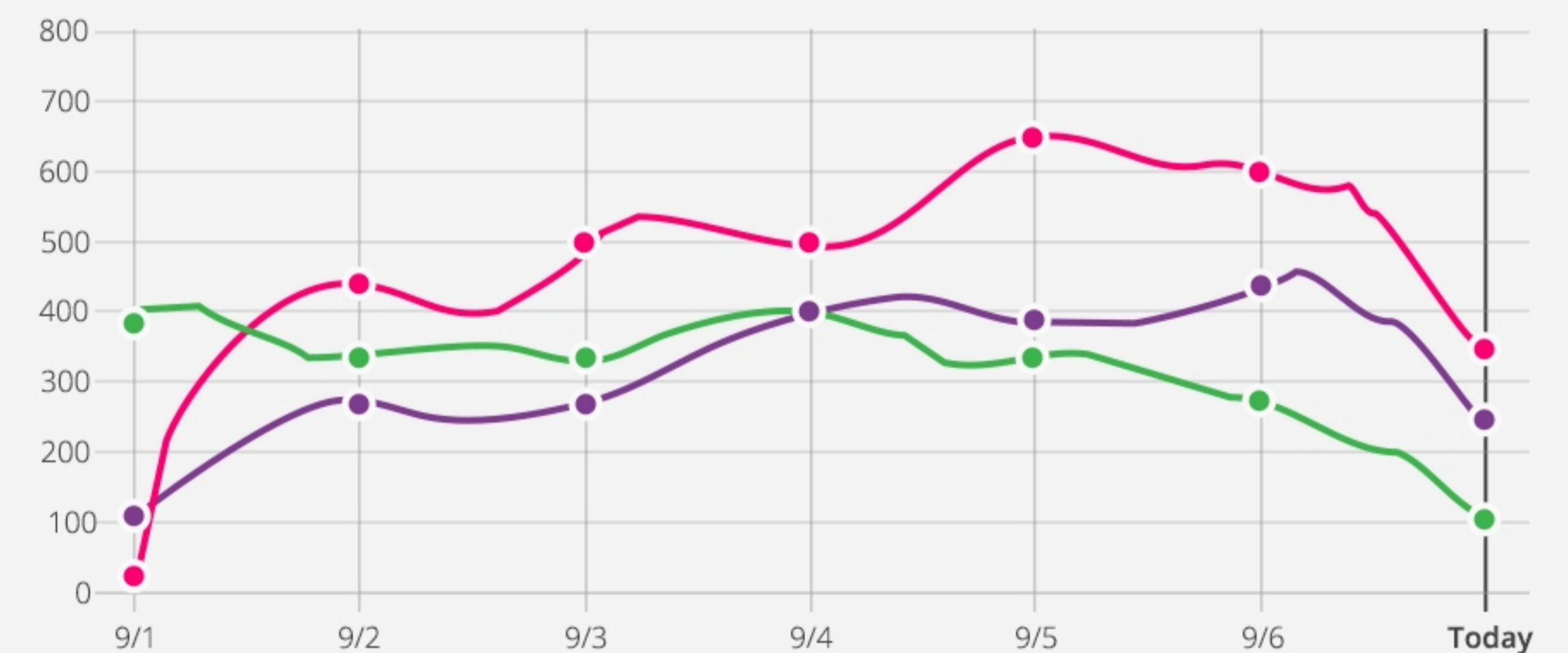
Criticality ▾

- Successful log on after multiple failed attempts
- A file READ across EXPAND was detected
- NonStop user sessions multiple failed attempts
- Unauthorized NonStop file changes
- NonStop user logged on as SUPER.SUPER

[View all](#)

Total activity last week

Last Scan: 2019-09-13 00:00:00.000 UTC



Compliance

Passed Failed Error Not Scanned

Status	Framework	Time of scan	Previous scan
ⓘ	HPE NonStop Security Hardening Guide See Results	4 days ago 10/25/2019 at 01:50AM UTC	34 days ago 09/26/2019 at 11:14AM UTC
✔	PCI-DSS 3.2.1 See Results	4 days ago 10/25/2019 at 11:50PM UTC	5 days ago 10/24/2019 at 11:50PM UTC

CONTENT PROPAGATED BY INTERACTION WITH RESULT ACTIVITY FROM

- GLOBAL SEARCH RESULTS
- ACTIVE UI ELEMENTS INTERACTION
- RESULTS USER INTERACTED WITH



XYGATE SecurityOne® All Systems Dashboard

"ON THIS SCREEN" CAN BE A MOUSEOVER SHOWING RESULTS -AND- A CLICK THROUGH

ON THIS SCREEN FOUND 18 MATCHING DATA POINTS

VOLUMES FOUND ON 4 DIFFERENT HOSTS

HOSTS 63 USES WERE FOUND

Recent Activity Last Logon on 7/21/2020

Overview

Customize

24

Critical Incidents occurred today

8

EXPAND Operations since last logon

31

Collection Aborted since last logon

COMPLIANCE

System is Compliant as of 9/4/2020

423

Alerts on 9/4/2020

249

Incidents on 9/4/2020

Alerts (423)

Top 5 results

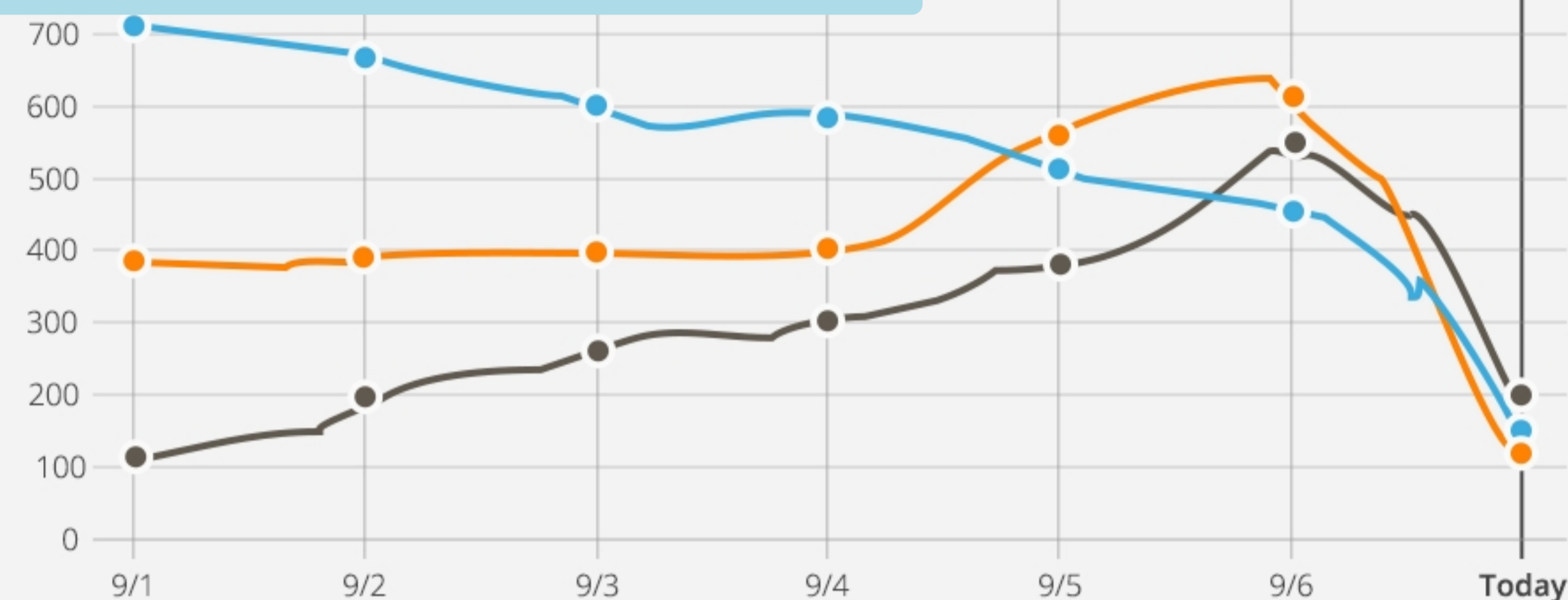
Most Recent

- APconnectionPool-Test 1
- AP-User
- AP Connection Test Pool Test 2
- AP GuardianFile Connection Pool test 3
- APIAuditPoolSF

View all

Removed (134) Modified (145)

Last Scan: 2019-09-13 00:00:00.000 UTC



ASM

CLIM Devices



NSC Devices



Incidents (692)

Top 5 results

Criticality

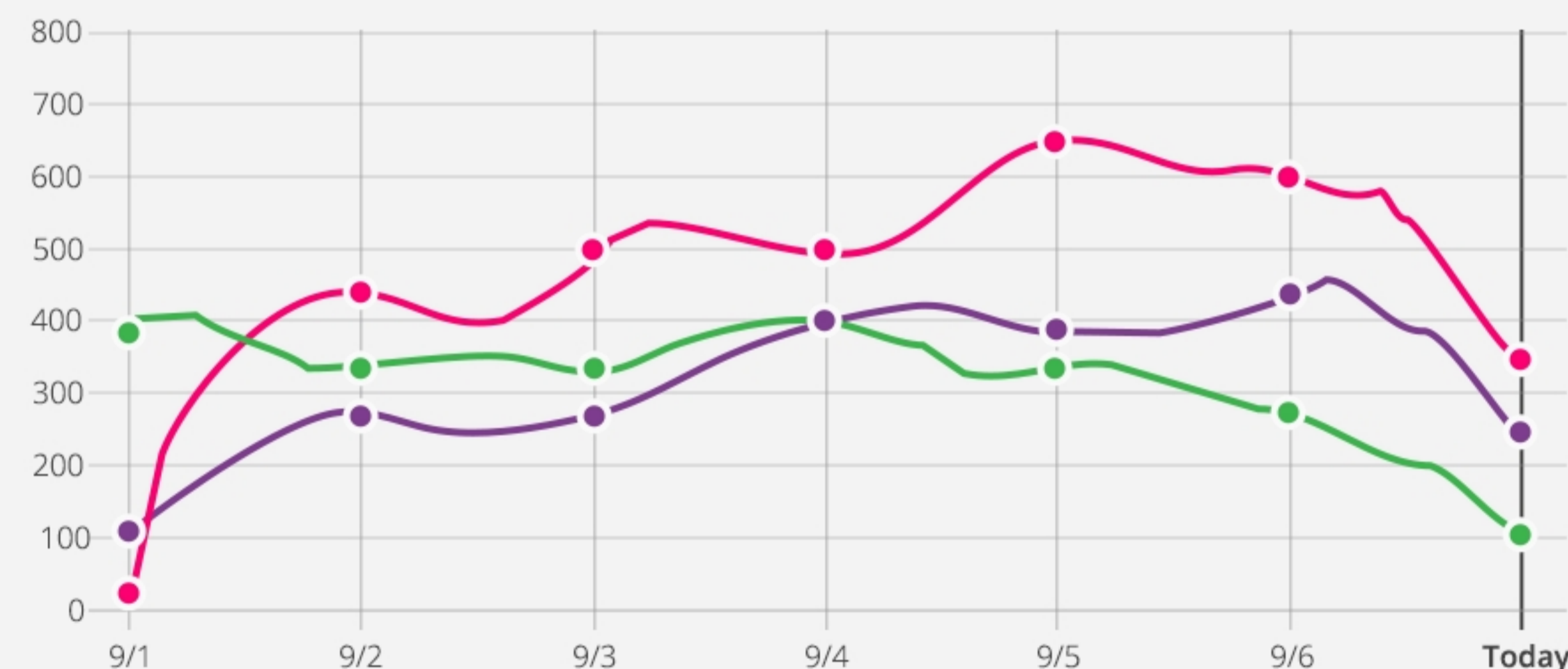
- Successful log on after multiple failed attempts
- A file READ across EXPAND was detected
- NonStop user sessions multiple failed attempts
- Unauthorized NonStop file changes
- NonStop user logged on as SUPER.SUPER

View all

Critical (140) Major (76) Minor (33)

Total activity last week

Last Scan: 2019-09-13 00:00:00.000 UTC



Compliance

Passed Failed Error Not Scanned

Status	Framework	Time of scan	Previous scan
Failed	HPE NonStop Security Hardening Guide See Results	4 days ago 10/25/2019 at 01:50AM UTC	34 days ago 09/26/2019 at 11:14AM UTC
Passed	PCI-DSS 3.2.1 See Results	4 days ago 10/25/2019 at 11:50PM UTC	5 days ago 10/24/2019 at 11:50PM UTC

CONTENT PROPAGATED BY INTERACTION WITH RESULT ACTIVITY FROM

- GLOBAL SEARCH RESULTS
- ACTIVE UI ELEMENTS INTERACTION
- RESULTS USER INTERACTED WITH



XYGATE SecurityOne® All Systems Dashboard

Recent Activity
Last Logon on 7/21/2020

18 DATA POINTS MATCHING \$VNCA X

Overview

[Customize](#)

24 [^]

Critical Incidents occurred today

8 [^]

EXPAND Operations since last logon

31 [^]

Collection Aborted since last logon

COMPLIANCE

System is Compliant as of 9/4/2020 ⓘ

15 [^]

Alerts on 9/4/2020

249 [^]

Incidents on 9/4/2020

Alerts (3)

Added (2) Removed (0) Modified (1)

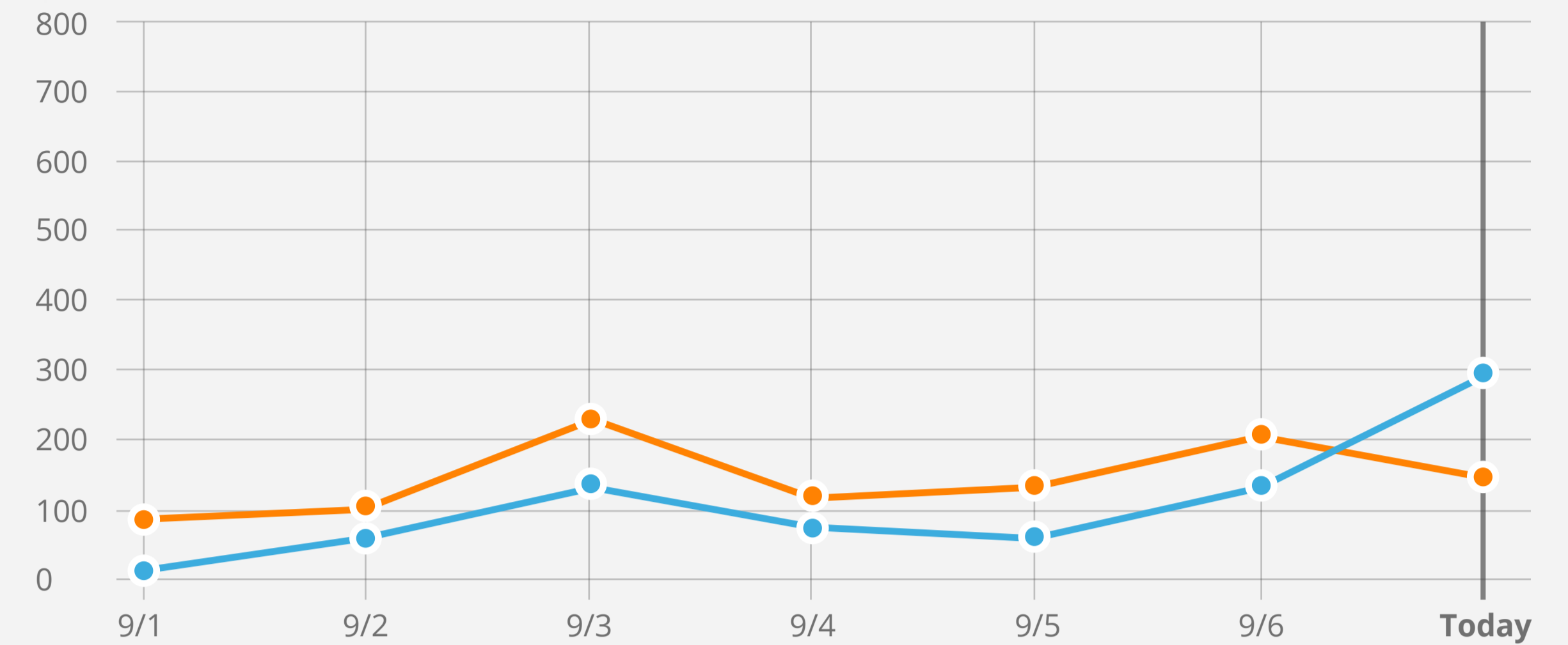
Top 5 results

Most Recent ▾

- \$SYSTEM.XYGATE Monitor
- \$SYSTEM.XYGATE.OSACL Monitor

Total activity last week

Last Scan: 2019-09-13 00:00:00.000 UTC



ASM

CLIM
Devices ⓘ



NSC
Devices ⓘ



Incidents (692)

Critical (140) Major (76) Minor (33)

Top 5 results

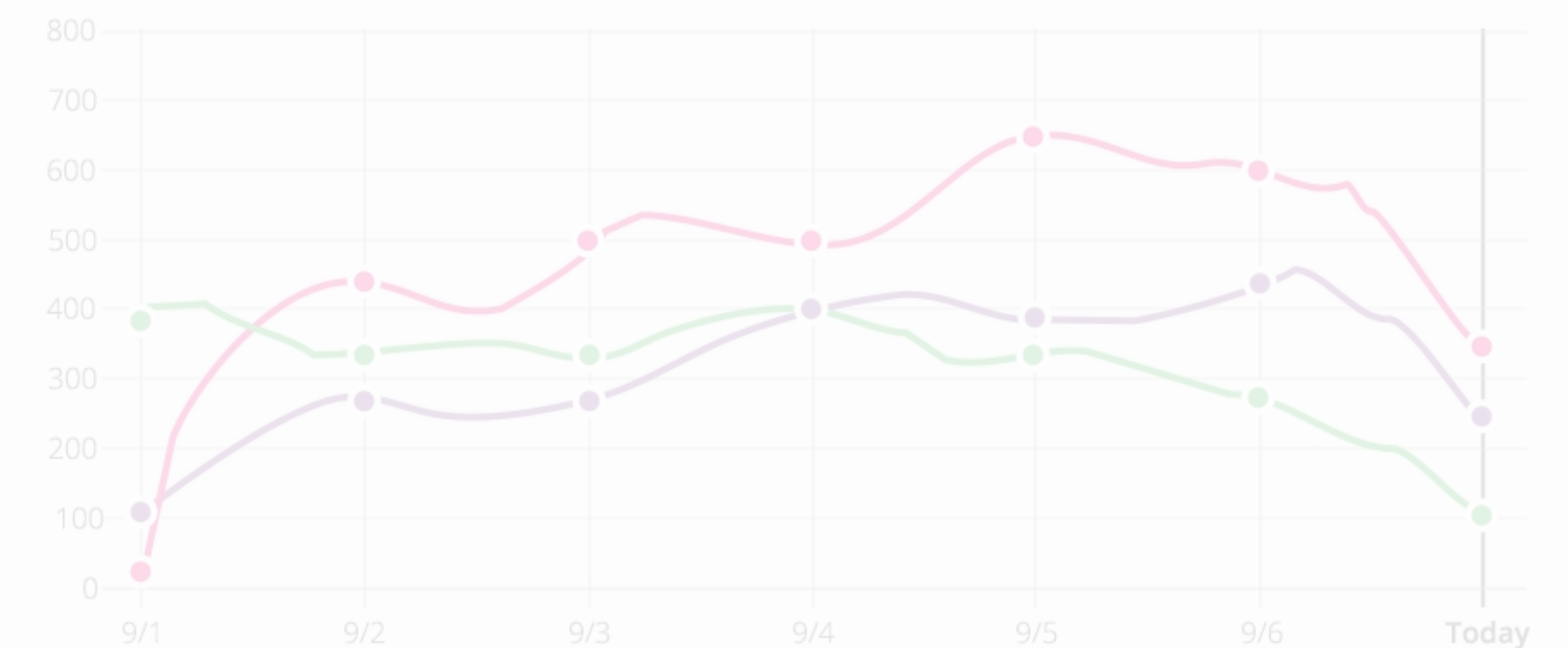
Criticality ▾

- Successful log on after multiple failed attempts
- A file READ across EXPAND was detected
- NonStop user sessions multiple failed attempts
- Unauthorized NonStop file changes
- NonStop user logged on as SUPER.SUPER

[View all](#)

Total activity last week

Last Scan: 2019-09-13 00:00:00.000 UTC



Compliance

Passed Failed Error Not Scanned

Status	Framework	Time of scan	Previous scan
ⓘ	HPE NonStop Security Hardening Guide See Results	4 days ago 10/25/2019 at 01:50AM UTC	34 days ago 09/26/2019 at 11:14AM UTC
✔	PCI-DSS 3.2.1 See Results	4 days ago 10/25/2019 at 11:50PM UTC	5 days ago 10/24/2019 at 11:50PM UTC



Overview

[Customize](#)

24[^]

Critical Incidents occurred today

8[^]

EXPAND Operations since last logon

31[^]

Collection Aborted since last logon

COMPLIANCE

System is Compliant as of 9/4/2020 ⓘ

423[^]

Alerts on 9/4/2020

249[^]

Incidents on 9/4/2020

Alerts (423)

Added (159) Removed (134) Modified (145)

Top 5 results

Most Recent ▾

APconnectionPool-Test 1 🔍

AP-User

AP Connection Test Pool Test 2

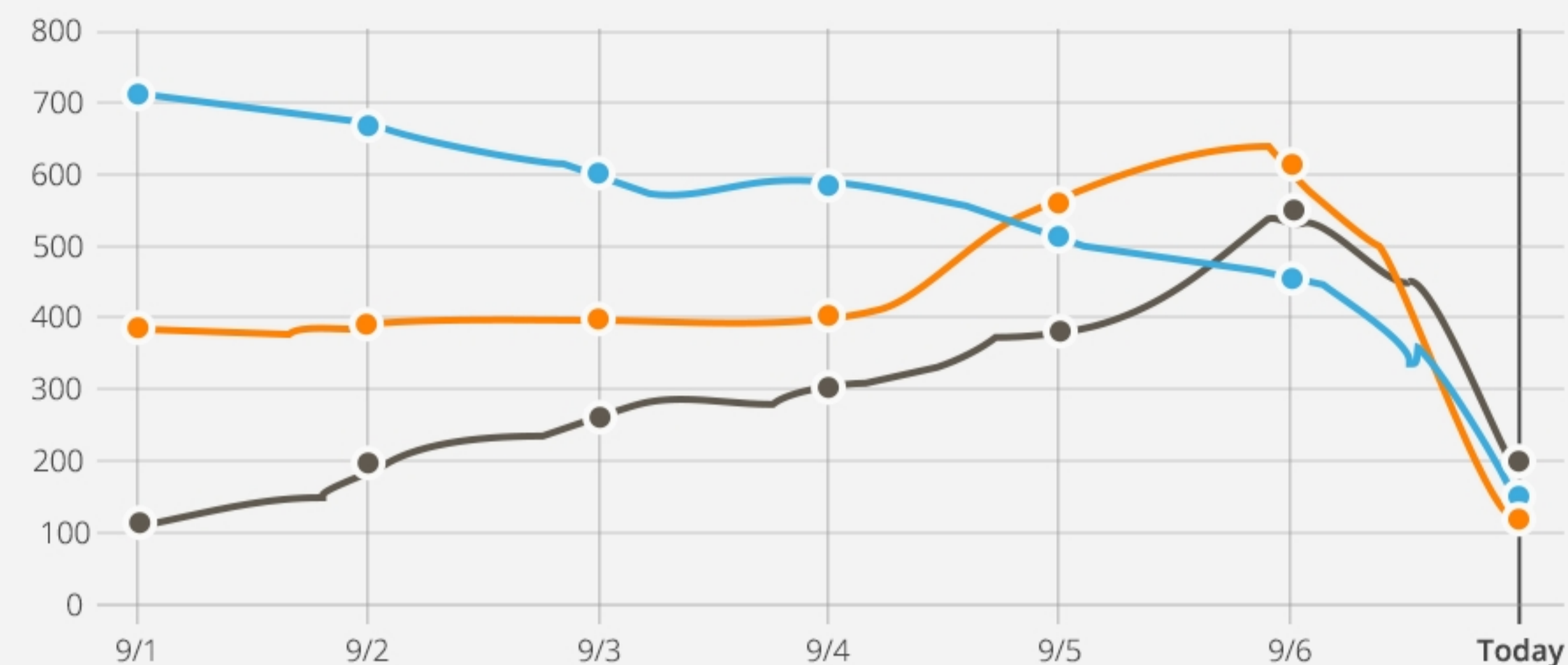
AP GuardianFile Connection Pool test 3

APIAuditPoolSF

[View all](#)

Total activity last week

Last Scan: 2019-09-13 00:00:00.000 UTC



ASM

CLIM

Devices ⓘ



NSC

Devices ⓘ



Incidents (692)

Critical (140) Major (76) Minor (33)

Top 5 results

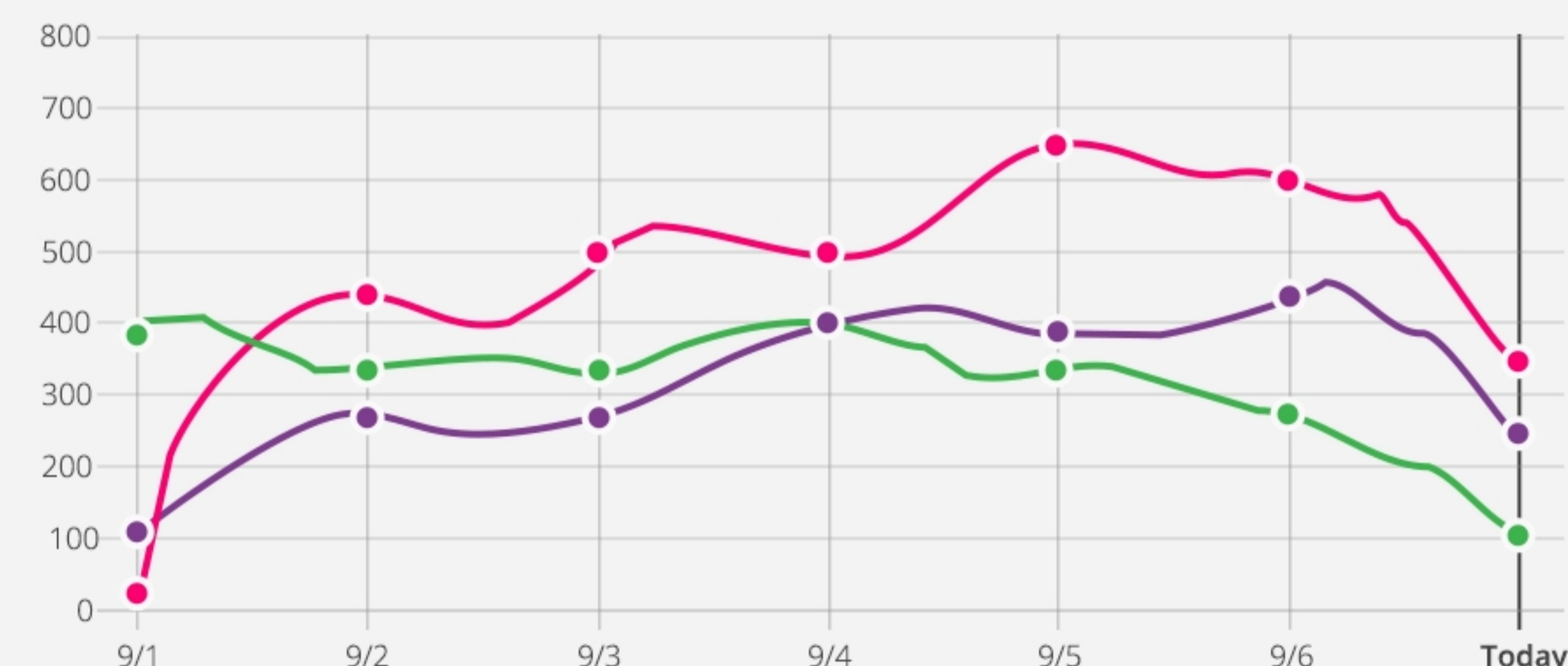
Criticality ▾

- Successful log on after multiple failed attempts
- A file READ across EXPAND was detected
- NonStop user sessions multiple failed attempts
- Unauthorized NonStop file changes
- NonStop user logged on as SUPER.SUPER

[View all](#)

Total activity last week

Last Scan: 2019-09-13 00:00:00.000 UTC



Compliance

Passed Failed Error Not Scanned

Status	Framework	Time of scan	Previous scan
ⓘ	HPE NonStop Security Hardening Guide See Results	4 days ago 10/25/2019 at 01:50AM UTC	34 days ago 09/26/2019 at 11:14AM UTC
✔	SPECIFIC CONTENT IS IDENTIFIED AS SEARCHABLE IN INTERFACE VIA MOUSEOVER / HIGHLIGHT WITH CTA SHORTCUT TO SEARCH - USER INITIATES See Results	4 days ago 10/25/2019 at 11:50PM UTC	5 days ago 10/24/2019 at 11:50PM UTC

CONTENT PROPAGATED BY INTERACTION WITH RESULT ACTIVITY FROM

- GLOBAL SEARCH RESULTS
- ACTIVE UI ELEMENTS INTERACTION
- RESULTS USER INTERACTED WITH

FIGURE 32

-SEARCH ELEMENT GOES ACTIVE AND PRODUCES MATCHES
-THIS IS THROUGHOUT THE ENTIRE APP
-CREATES A WONDERFUL FEEDBACK LOOP OF INTERACTIVITY
-INITIAL ROLLOUT COULD BE LIMITED TO TABLES AND THEN SUBSEQUENT COMPONENTS IN A LATER PHASE

-ALL ACTIVE ELEMENTS COULD BE HIGHLIGHTED ON MOUSEOVER
-OTHERS MAY BE GRAYED OUT AND LESS OPAQUE
-STATE MAY BE INDICATED BY COMPONENT OR WHOLE PAGE IF DESIRED



XYGATE SecurityOne® All Systems Dashboard

THIS IS A DISAMBIGUATION STEP
LIKE TERMS - WHICH THE USER
PREFERS TO SEARCH ON
E.G. USERID VS USER

THIS MAKES THE NEXT STEP STREAMLINED

VOLUMES
63 USES WERE FOUND

FILES
292 USES WERE FOUND

USERS
16 USERS HAVE ACCESS

PROCESSES
48 PROCESSES UTILIZE THIS FILE

HOSTS
FOUND ON 4 DIFFERENT HOSTS

ASSETS

MONITORS

INCIDENTS

ASM

COMPLIANCE

Recent Activity
Last Logon on 7/21/2020

Overview

[Customize](#)

24 [^]

Critical Incidents
occurred today

8 [^]

EXPAND Operations
since last logon

31 [^]

Collection Aborted
since last logon

COMPLIANCE

System is Compliant
as of 9/4/2020 ⓘ

423 [^]

Alerts
on 9/4/2020

249 [^]

Incidents
on 9/4/2020

Alerts (423)

Top 5 results

Most Recent

APconnectionPool-Test 1

AP-User

AP Connection Test Pool Test 2

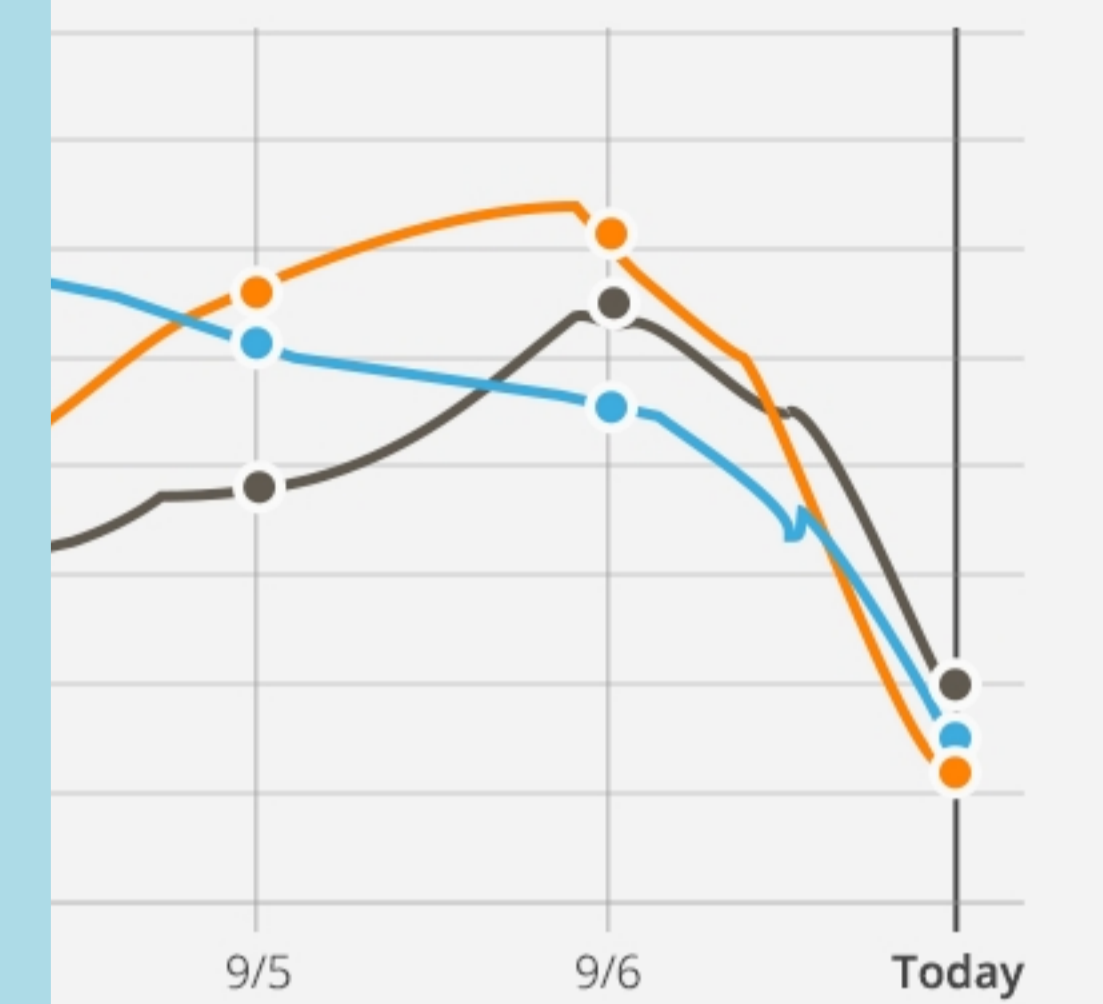
AP GuardianFile Connection Pool test 3

APIAuditPoolSF

[View all](#)

Removed (134) Modified (145)

Last Scan: 2019-09-13 00:00:00.000 UTC



ASM

CLIM
Devices ⓘ



NSC
Devices ⓘ



Incidents (692)

Top 5 results

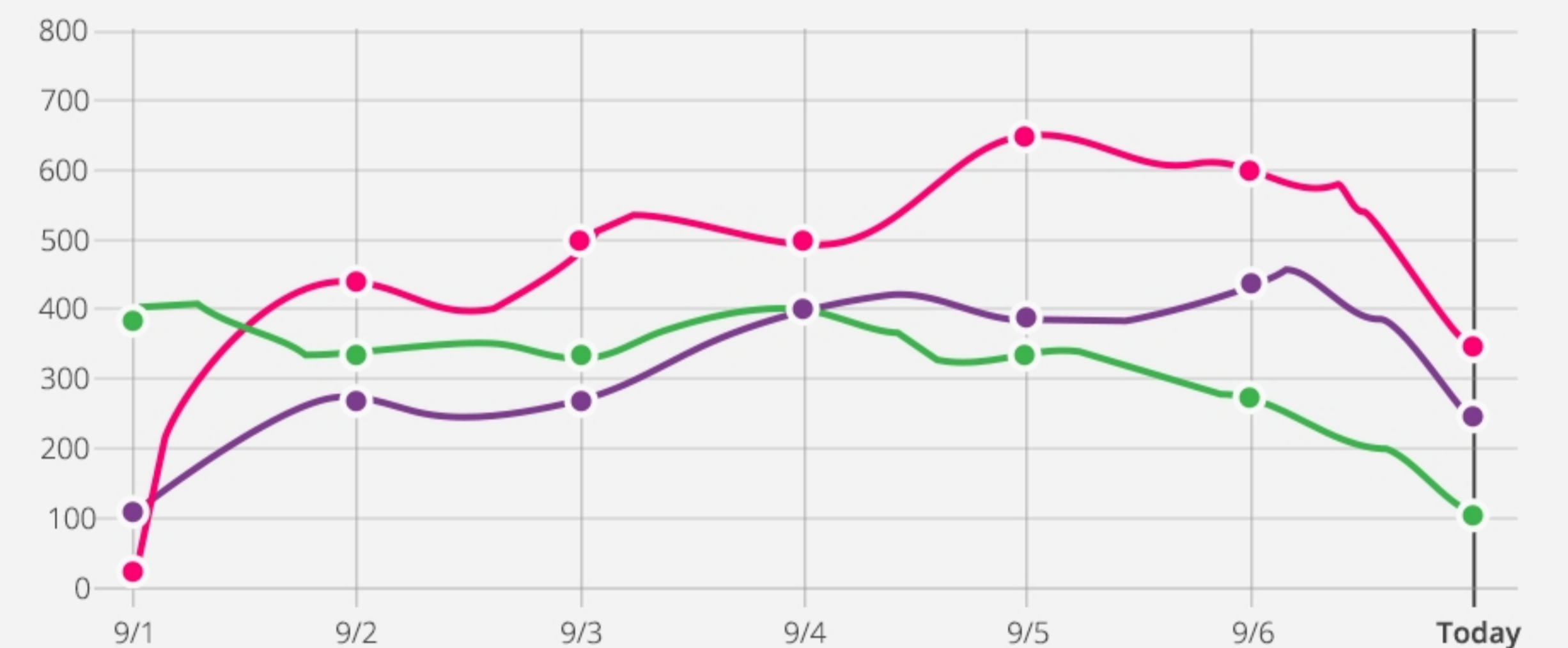
Criticality

- Successful log on after multiple failed attempts
- A file READ across EXPAND was detected
- NonStop user sessions multiple failed attempts
- Unauthorized NonStop file changes
- NonStop user logged on as SUPER.SUPER

[View all](#)

Total activity last week

Last Scan: 2019-09-13 00:00:00.000 UTC



Compliance

Passed Failed Error Not Scanned

Status	Framework	Time of scan	Previous scan
ⓘ	HPE NonStop Security Hardening Guide See Results	4 days ago 10/25/2019 at 01:50AM UTC	34 days ago 09/26/2019 at 11:14AM UTC
✔	PCI-DSS 3.2.1 See Results	4 days ago 10/25/2019 at 11:50PM UTC	5 days ago 10/24/2019 at 11:50PM UTC



XYGATE SecurityOne® All Systems Dashboard

Recent Activity
Last Logon on 7/21/2020

Overview

24[^]

Critical Incidents
occurred today

8

EXPAND Open
since last lo

COMPLIANCE

System is Compliant
as of 9/4/2020 ⓘ

423

Alerts
on 9/4/20

ASM

CLIM
Devices ⓘ



RESULTS



\$SYSTEM.XYGATE.OSACL (292)

COMPARING ATTRIBUTES FOR A FILE ACROSS ALL HOSTS ▾

HIGHLIGHT

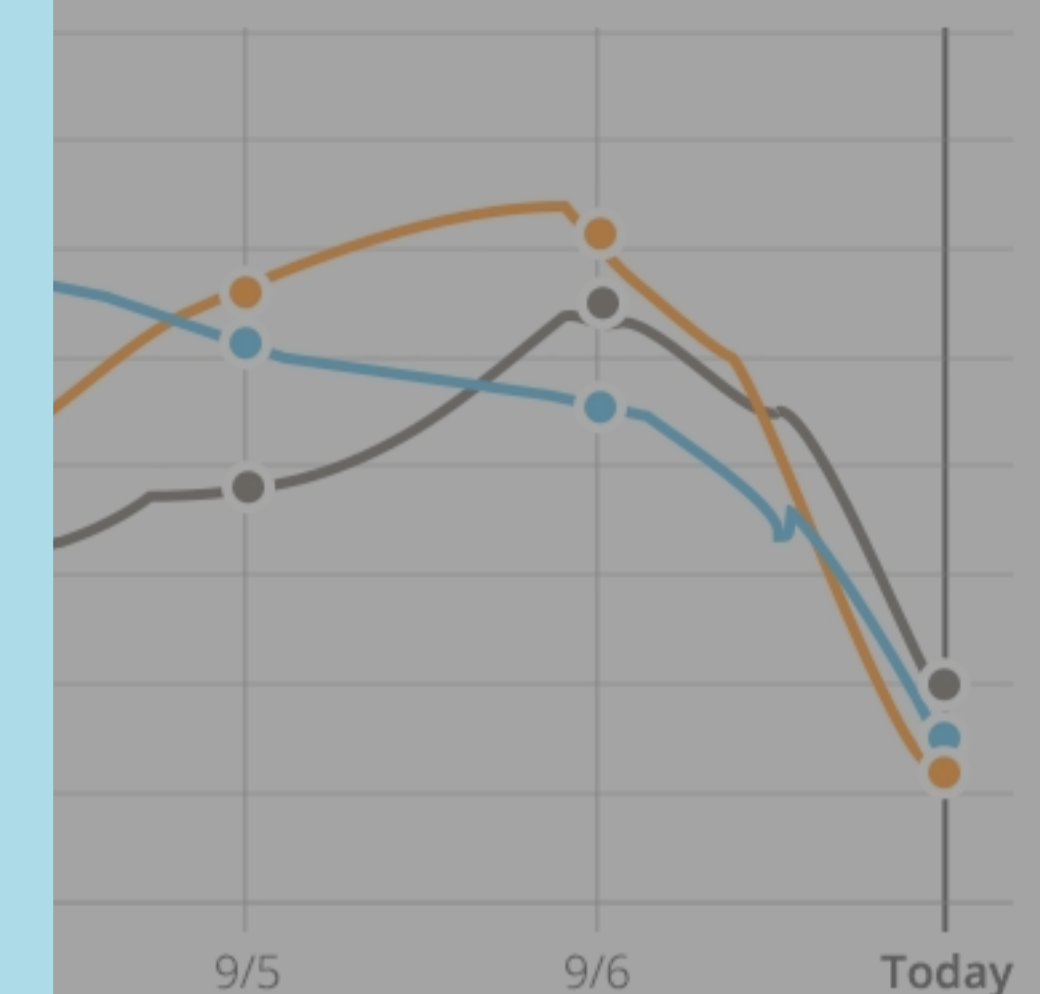
FILTER BY DIFF ▾

<input type="checkbox"/>	HOST	DETAIL 1	DETAIL 2	ATTRB 1	ATTRB 2	ATTRB 3	ATTRB 4
<input type="checkbox"/>	HOST	DETAIL X	DETAIL 2	ATTRB 1	ATTRB 2	ATTRB 3	ATTRB 4
<input type="checkbox"/>	HOST	DETAIL 1	DETAIL 2	ATTRB 1	ATTRB 2	ATTRB 3	ATTRB 4
<input type="checkbox"/>	HOST	DETAIL X	DETAIL 2	ATTRB 1	ATTRB 2	ATTRB 3	ATTRB 4
<input type="checkbox"/>	HOST	DETAIL 1	DETAIL 2	ATTRB 1	ATTRB 2	ATTRB 3	ATTRB 4
<input type="checkbox"/>	HOST	DETAIL 1	DETAIL 2	ATTRB 1	ATTRB 2	ATTRB 3	ATTRB 4
<input type="checkbox"/>	HOST	DETAIL X	DETAIL 2	ATTRB 1	ATTRB 2	ATTRB 3	ATTRB 4
<input type="checkbox"/>	HOST	DETAIL X	DETAIL 2	ATTRB 1	ATTRB 2	ATTRB 3	ATTRB 4
<input type="checkbox"/>	HOST	DETAIL 1	DETAIL 2	ATTRB 1	ATTRB 2	ATTRB 3	ATTRB 4
<input type="checkbox"/>	HOST	DETAIL 1	DETAIL 2	ATTRB 1	ATTRB 2	ATTRB 3	ATTRB 4
<input type="checkbox"/>	HOST	DETAIL 1	DETAIL 2	ATTRB 1	ATTRB 2	ATTRB 3	ATTRB 4
<input type="checkbox"/>	HOST	DETAIL 1	DETAIL 2	ATTRB 1	ATTRB 2	ATTRB 3	ATTRB 4

EXPORT

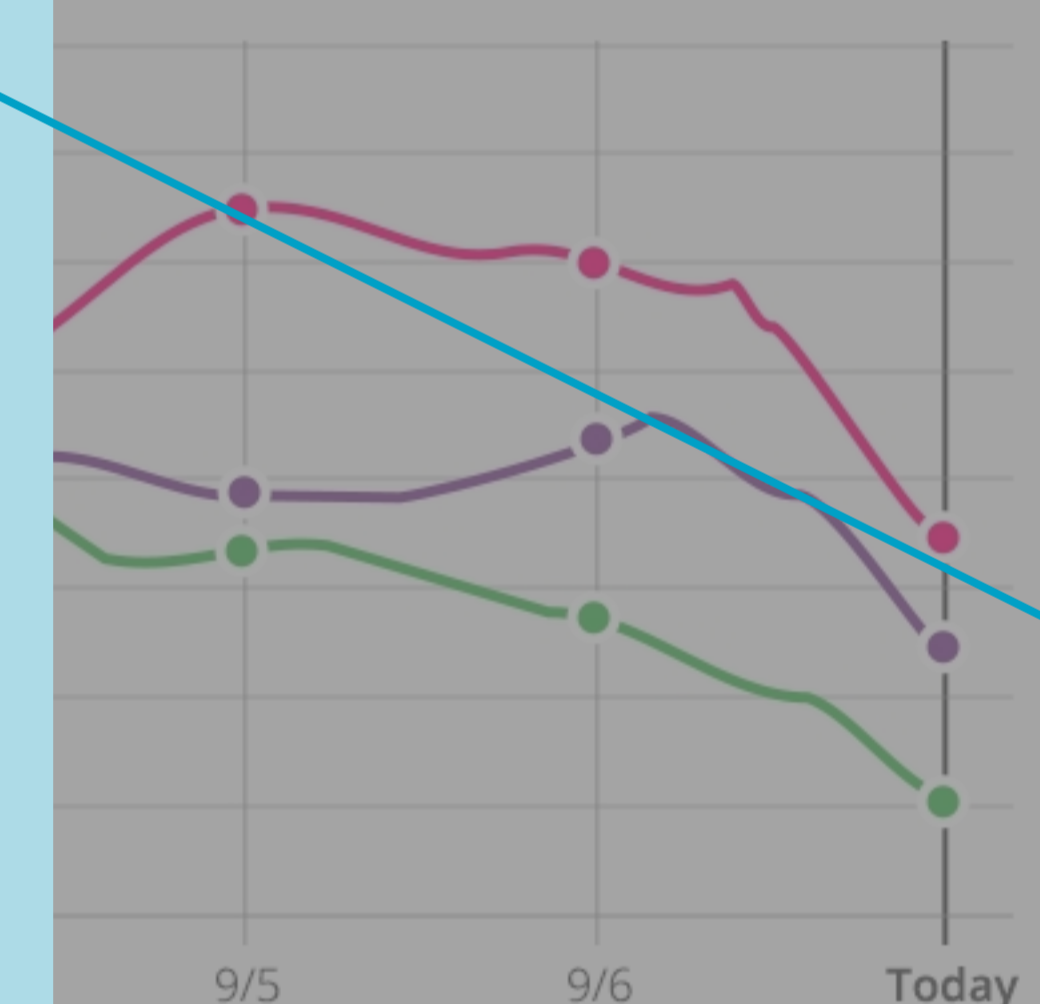
Removed (134) Modified (145)

Last Scan: 2019-09-13 00:00:00.000 UTC



Minor (140) Major (76) Minor (33)

Last Scan: 2019-09-13 00:00:00.000 UTC



Failed Error Not Scanned

Previous scan



HPE NonStop Security Hardening Guide
[See Results](#)

4 days ago
10/25/2019 at 01:50AM UTC

34 days ago
09/26/2019 at 11:14AM UTC



PCI-DSS 3.2.1
[See Results](#)

4 days ago
10/25/2019 at 11:50PM UTC

5 days ago
10/24/2019 at 11:50PM UTC

XYGATE SecurityOne®
All Systems Dashboard

ACTION ADDED TO GN : SEARCH

Recent Activity
Last Logon on 7/21/2020

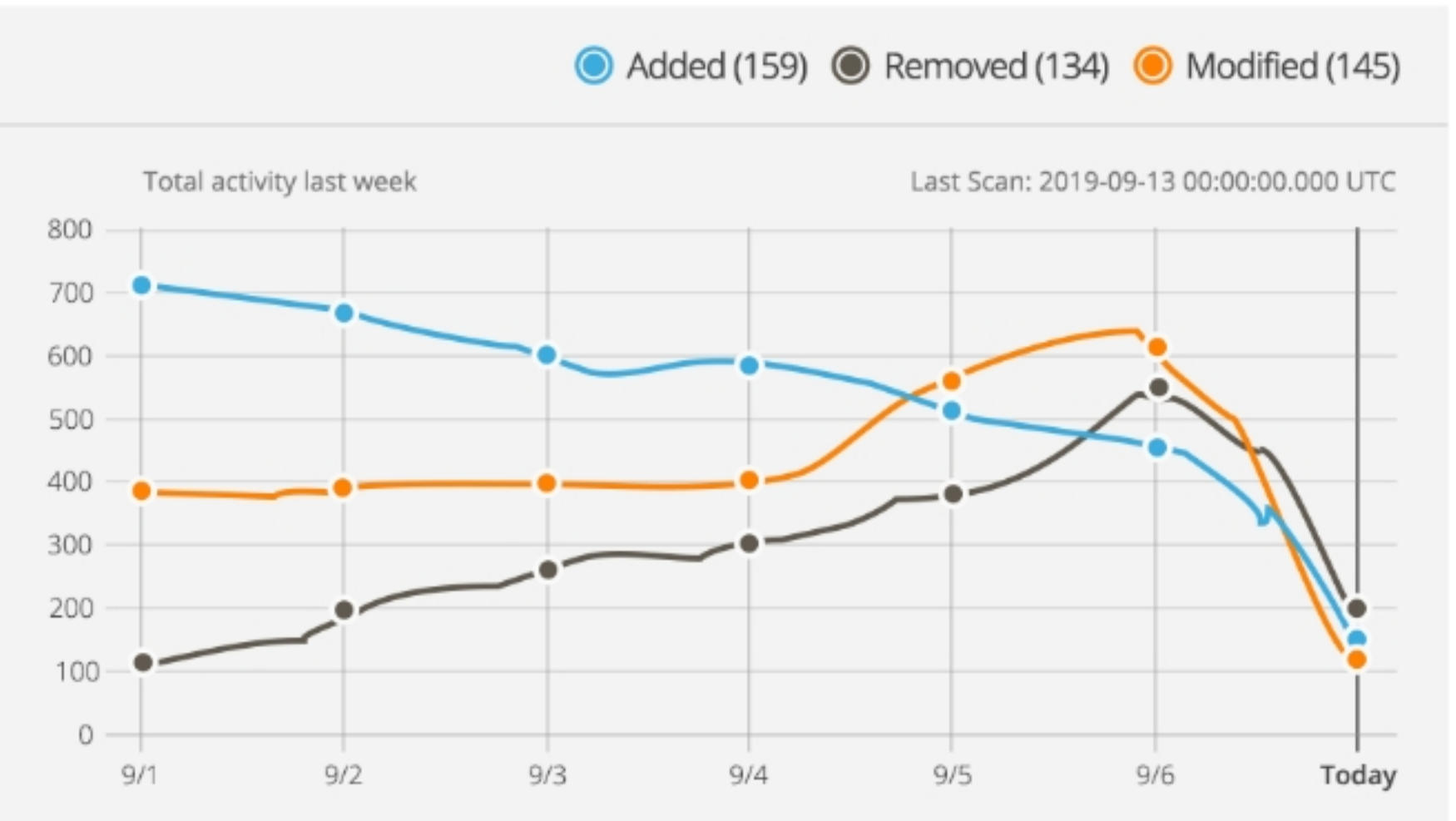
Overview Customize

<p>24 [^]</p> <p>Critical Incidents occurred today</p>	<p>8 [^]</p> <p>EXPAND Operations since last logon</p>	<p>31 [^]</p> <p>Collection Aborted since last logon</p>
<p>COMPLIANCE</p> <p>System is Compliant as of 9/4/2020 ⓘ</p>	<p>423 [^]</p> <p>Alerts on 9/4/2020</p>	<p>249 [^]</p> <p>Incidents on 9/4/2020</p>

Alerts (423)

Top 5 results Most Recent

- APconnectionPool-Test 1
- AP-User
- AP Connection Test Pool Test 2
- AP GuardianFile Connection Pool test 3
- APIAuditPoolSF



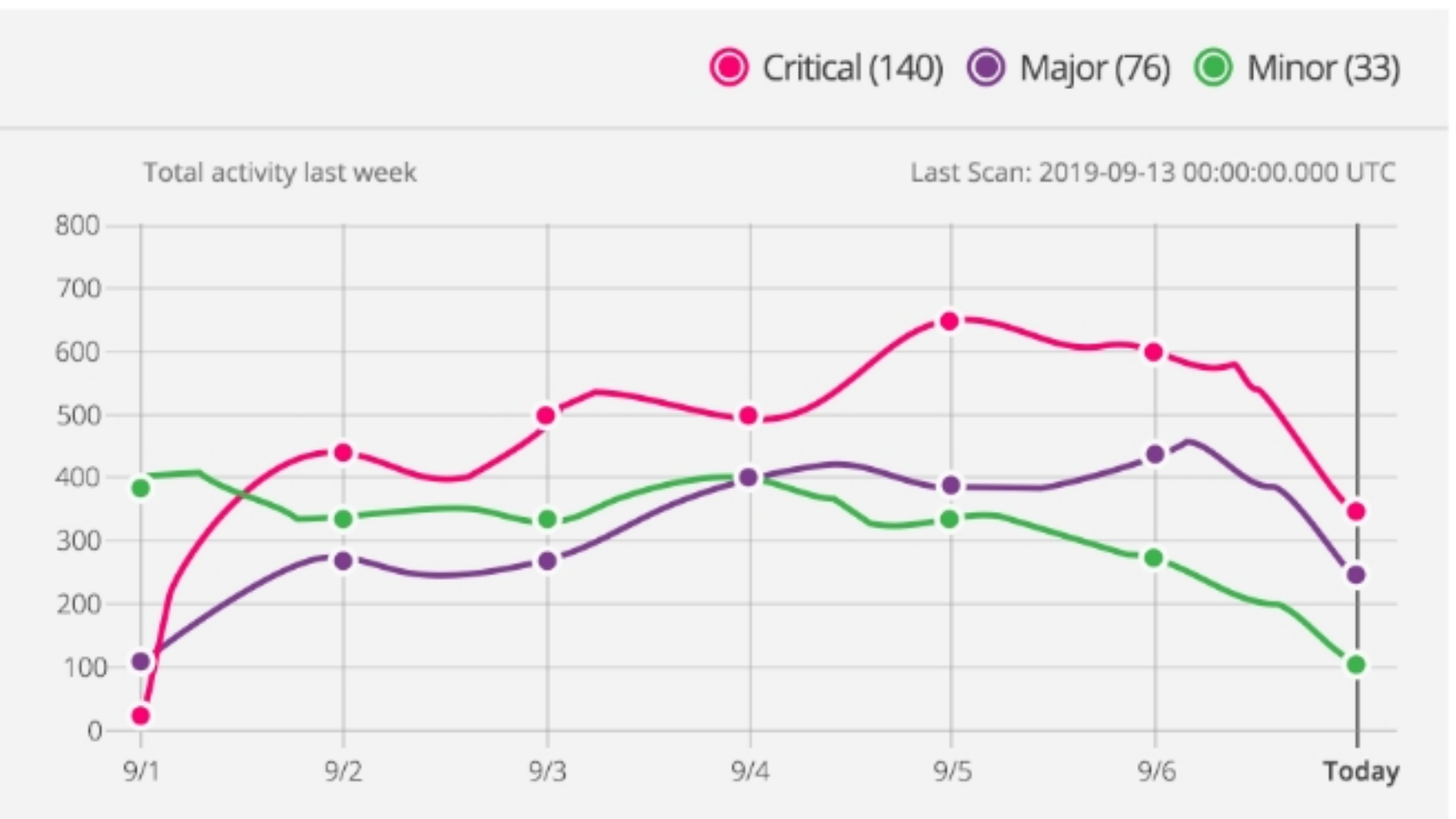
ASM

<p>CLIM</p> <p>Devices ⓘ</p> <p>9 At-Risk</p>	<p>NSC</p> <p>Devices ⓘ</p> <p>3 Stable</p>
-------------------------------------------------------------	-----------------------------------------------------------

Incidents (692)

Top 5 results Criticality

- Successful log on after multiple failed attempts
- A file READ across EXPAND was detected
- NonStop user sessions multiple failed attempts
- Unauthorized NonStop file changes
- NonStop user logged on as SUPER.SUPER



SPECIFIC CONTENT IS IDENTIFIED AS SEARCHABLE IN INTERFACE
 -VIA MOUSOVER / HIGHLIGHT WITH CTA SHORTCUT TO SEARCH
 -USER INITIATES
 -SEARCH ELEMENT GOES ACTIVE AND PRODUCES MATCHES
 -THIS IS THROUGHOUT THE ENTIRE APP
 -CREATES A WONDERFUL FEEDBACK LOOP OF INTERACTIVITY
 -INITIAL ROLLOUT COULD BE LIMITED TO TABLES AND THEN SUBSEQUENT COMPONENTS IN A LATER PHASE

Compliance

Passed
 Failed
 Error
 Not Scanned

Status	Framework	Time of scan	Previous scan
ⓘ	HPE NonStop Security Hardening Guide See Results	4 days ago 10/25/2019 at 01:50AM UTC	34 days ago 09/26/2019 at 11:14AM UTC
✔	PCI DSS 3.2.1 See Results	4 days ago 10/25/2019 at 11:50PM UTC	5 days ago 10/24/2019 at 11:50PM UTC

SEARCH KNOWS WHAT IT IS LOOKING AT
E.G. FILE, FOLDER, SUB FOLDER, DEVICE, ETC.

VERY SPECIFIC LANGUAGE (MATCH TO CATEGORY)
OR
GENERAL MATCH LANGUAGE

GSC - Focus and Auto-Suggest

XYGATE SecurityOne®
All Systems Dashboard

SEARCH: \$VNCIA.CCL.CATFILE

THIS IS A DISAMBIGUATION STEP LIKE TERMS - WHICH THE USER PREFERS TO SEARCH ON E.G. USERID VS USER

THIS MAKES THE NEXT STEP STREAMLINED

Alerts (423)

Top 5 results

- APconnectionPool-Test 1
- AP-User
- AP Connection Test Pool Test 2
- AP GuardianFile Connection Pool test 3
- APIAuditPoolSF

Incidents (692)

Top 5 results

- Successful log on after multiple failed attempts
- A file READ across EXPAND was detected
- NonStop user sessions multiple failed attempts
- Unauthorized NonStop file changes
- NonStop user logged on as SUPER.SUPER

Compliance

Status	Framework	Time of scan	Previous scan
ⓘ	HPE NonStop Security Hardening Guide See Results	4 days ago 10/25/2019 at 01:50AM UTC	34 days ago 09/26/2019 at 11:14AM UTC
✔	PCI-DSS 3.2.1 See Results	4 days ago 10/25/2019 at 11:50PM UTC	5 days ago 10/24/2019 at 11:50PM UTC

Overview

- 24 Critical Incidents occurred today
- 8 EXPAND Operations since last logon
- 31 Collection Aborted since last logon
- COMPLIANCE System is Compliant as of 9/4/2020 ⓘ
- 423 Alerts on 9/4/2020
- 249 Incidents on 9/4/2020

ASM

- CLIM Devices: 9 At-Risk
- NSC Devices: 3 Stable

Recent Activity

Last Logon on 7/21/2020

Removed (134) Modified (145)

Last Scan: 2019-09-13 00:00:00.000 UTC

Total activity last week

Last Scan: 2019-09-13 00:00:00.000 UTC

Legend: ⓧ Passed, ❌ Failed, ⓘ Error, ⓪ Not Scanned

COMMON PIVOTS (E.G. INCIDENTS, MONITORS)
-CAN BE USER DEFINED

SIMILAR (DEFAULT)
DIFFERENT
ALL
HIGHLIGHT (DEFAULT)

CLOSE, TERM STILL RESIDES IN SEARCH FORM IN GN

GSC - Results

XYGATE SecurityOne®
All Systems Dashboard

Overview

24[^] Critical Incidents occurred today

8[^] EXPAND Open since last

COMPLIANCE
System is Compliant as of 9/4/2020

423 Alerts on 9/4/20

ASM

CLIM
Devices

9 At-Risk

RESULTS

\$VNCA.CCL.CATFILEC (292)

COMPARING ATTRIBUTES FOR A FILE ACROSS ALL HOSTS

HIGHLIGHT
FILTER BY DIFF

<input type="checkbox"/>	HOST	DETAIL 1	DETAIL 2	ATTRB 1	ATTRB 2	ATTRB 3	ATTRB 4
<input type="checkbox"/>	HOST	DETAIL X	DETAIL 2	ATTRB 1	ATTRB 2	ATTRB 3	ATTRB 4
<input type="checkbox"/>	HOST	DETAIL 1	DETAIL 2	ATTRB 1	ATTRB 2	ATTRB 3	ATTRB 4
<input type="checkbox"/>	HOST	DETAIL X	DETAIL 2	ATTRB 1	ATTRB 2	ATTRB 3	ATTRB 4
<input type="checkbox"/>	HOST	DETAIL 1	DETAIL 2	ATTRB 1	ATTRB 2	ATTRB 3	ATTRB 4
<input type="checkbox"/>	HOST	DETAIL 1	DETAIL 2	ATTRB 1	ATTRB 2	ATTRB 3	ATTRB 4
<input type="checkbox"/>	HOST	DETAIL X	DETAIL 2	ATTRB 1	ATTRB 2	ATTRB 3	ATTRB 4
<input type="checkbox"/>	HOST	DETAIL X	DETAIL 2	ATTRB 1	ATTRB 2	ATTRB 3	ATTRB 4
<input type="checkbox"/>	HOST	DETAIL 1	DETAIL 2	ATTRB 1	ATTRB 2	ATTRB 3	ATTRB 4
<input type="checkbox"/>	HOST	DETAIL 1	DETAIL 2	ATTRB 1	ATTRB 2	ATTRB 3	ATTRB 4
<input type="checkbox"/>	HOST	DETAIL 1	DETAIL 2	ATTRB 1	ATTRB 2	ATTRB 3	ATTRB 4
<input type="checkbox"/>	HOST	DETAIL 1	DETAIL 2	ATTRB 1	ATTRB 2	ATTRB 3	ATTRB 4
<input type="checkbox"/>	HOST	DETAIL 1	DETAIL 2	ATTRB 1	ATTRB 2	ATTRB 3	ATTRB 4
<input type="checkbox"/>	HOST	DETAIL 1	DETAIL 2	ATTRB 1	ATTRB 2	ATTRB 3	ATTRB 4
<input type="checkbox"/>	HOST	DETAIL 1	DETAIL 2	ATTRB 1	ATTRB 2	ATTRB 3	ATTRB 4
<input type="checkbox"/>	HOST	DETAIL 1	DETAIL 2	ATTRB 1	ATTRB 2	ATTRB 3	ATTRB 4

EXPORT

Recent Activity
Last Logon on 7/21/2020

Removed (134) Modified (145)

Last Scan: 2019-09-13 00:00:00.000 UTC

al (140) Major (76) Minor (33)

Last Scan: 2019-09-13 00:00:00.000 UTC

Failed Error Not Scanned

Previous scan

ⓘ HPE NonStop Security Hardening Guide	4 days ago 10/25/2019 at 01:50AM UTC	34 days ago 09/26/2019 at 11:14AM UTC
✅ PCI-DSS 3.2.1	4 days ago 10/25/2019 at 11:50PM UTC	5 days ago 10/24/2019 at 11:50PM UTC

Add Mask

Select an option below to add a mask. You can browse the Nonstop filesystem or leverage the power of a wildcard.

\$QA1P19QAAG1DICTMAP

Preview

Tips to using the above wildcard selection ...

VOLUMES	SUBVOLUMES	FILES
\$AUDIT	P19QAAC	APPSYNC
\$AUX01	P19QAACL	DICTALT
\$BASE24	P19QAAG1	DICTCDF
\$DATAA	P19QAAG2	DICTDDF
\$DATAB	P19QAAG2	DICTKDF
\$DATAC	P19QAAS	DICTMAP
\$DSMSCM	P19QACNF	DICTOBL
\$EMPTY	P19QADB0	DICTODF
\$MAXCHAR	P19QADB1	DICTOTF
\$OSS00	P19QADB2	DICTOUF
\$Q	P19QADB3	DICTOUK
\$Q00000	P19QADB4	DICTRDF
\$QA1	P19QADB5	DICTTKN
\$QA2	P19QADB6	DICTTYP
\$QCTEST	P19QADB7	DICTVER
\$SYSTEM	P19QADB8	EMSBUILD
\$VAXH	P19QADB9	EMSDDL
\$VAXJ	P19QAFLA	EMSTEMP
\$VAXR	P19QAFLF	EXPADD
\$VBWD	P19QAFUP	EXPCHK
\$VBXB	P19QAINP	LICCHK
\$VCLASS	P19QALGB	LOGDDL
\$VCXG	P19QALOG	NETKEY
\$VCXS	P19QAMON	NETPASS
\$VDAC	P19QAQIN	P15F001
\$VDBF	P19QAQOUT	PASSHELP

Select

DETAILS AND ATTRIBUTES CAN BE SELECTED BY USER

THERE IS ALWAYS AN NEXT STEP ACTION FROM HERE