SECURITY INCIDENT REPORT - WIDGET CO

Course: EAS [redacted] Cybersecurity Analytics

Instructor: [redacted]

April 23, 2025

Team Profile and Case Background

Advisory Group Members:

Raghavi Ayyathurai

[redacted]

This report presents a detailed investigation into the **cybersecurity breach** that impacted **Widget Co.** in **October**. The breach involved unauthorized access to enterprise systems through methods such as phishing, MFA bypass, and credential compromise.

Utilizing **Splunk** as the core analysis platform, the team looked into log data from multiple systems, including **VPN**, **MFA**, **DNS**, **Password Vault**, **Cloud**, and **internal applications**. Through correlation of log events and timeline reconstruction, the team identified, attacker persistence, privilege escalation, and infrastructure evasion techniques.

The findings in this report are intended to support both technical remediation and strategic decision-making. In addition to identifying the root causes and techniques used by the attacker, the report also provides separate recommendations tailored for IT/Security Operations and Executive Leadership.

Contents

1 Executive Summary

In **October**, **Widget Co.** experienced a cybersecurity breach that leveraged **phishing**, **MFA bypass**, and **credential abuse** to gain unauthorized access to critical enterprise systems. The attack originated from two exploited user accounts - **BDRVLS** and **DDDXUB** and spanned across various services, including **billing software**, **cloud**, **administrative portal**, and the company's **password vault**. This was not an isolated event, but rather a methodical, staged operation involving sustained access attempts and evolving attacker techniques.

Our investigative team used **Splunk's** robust correlation and visualization tools to analyze the dataset from multiple log sources. Through custom queries and timeline construction, we were able to trace each step of the **attacker's movement**, document **exploitation techniques**, and identify vulnerabilities in authentication mechanisms. The findings highlight the importance of cross-system visibility, real time monitoring, and organizational readiness for coordinated attack mitigation.

2 Investigation Methodology

The investigation began by reviewing **DNS logs** for signs of contact with known **malicious IOCs**. Although other phishing links may have been present earlier, the first confirmed malicious action occurred on **October 12**, when user **BDRVLS** accessed **glasslu.com**, a domain listed in the IOC dataset (see **Appendix A2**). This activity is considered the likely **point of initial compromise**, particularly because **BDRVLS** was not enrolled in **MFA**, making the account more vulnerable to **phishing-based credential theft**.

Shortly after the phishing domain access, the same **IOC IP 180.76.54.93** appeared in successful login entries to internal systems, including the Billing Software and Password Vault (See **Appendix A8** and **A13**). The Vault access on **October 13** was the first confirmed use of stolen credentials for accessing sensitive data.

The investigation then focused on **VPN logs**, where **failed login attempts** from previously unseen external IPs - including **107.175.94.203**, **158.69.59.92**, and **87.123.144.71** - were observed between **October 3** and **October 10** (See **Appendix A10** and **A11**). These attempts were likely early brute-force probes aimed at credential discovery.

On **October 15**, signs of a second account compromise emerged. User **DDDXUB** accessed the IT Admin portal from the same IOC IP with a successful result, followed shortly by an MFA **"Bypass"** during login to the Cloud platform (See **Appendix A18**). These events indicated that the attacker had **escalated privileges** and gained deeper access into the environment.

The attacker maintained access through **October 24** to **31**, switching infrastructure and logging in from a new IP address, 104.227.59.62, which was not flagged initially. All findings were based on provided log data, and further supporting screenshots of key queries and outputs are included in the Appendix.

3 Breach Timeline and Analysis

This section outlines the chronological progression of events that led to and followed the cybersecurity breach at Widget Co. The timeline was constructed using log data from multiple sources. The analysis captures attacker behavior from **initial contact** through to **lateral movement**, **privilege escalation**, and **sustained access** using multiple compromised accounts. By mapping each key event, this timeline provides clarity on how the breach unfolded and highlights the stages where detection and mitigation opportunities were either missed or bypassed.

3.1 Detailed Timeline of the Breach and Unauthorized Access Attempts

Date & Time	**Event Description**
October 12, 4:57 PM	User **BDRVLS** accesses a malicious domain **glasslu.com**, flagged in the IOC list. This marks the first confirmed compromise, likely via **phishing**.
October 12, 4:59 PM	Two minutes later, **BDRVLS** logs into **Billing Software** from IOC IP **180.76.54.93**. **MFA** result is marked **N/A**, suggesting MFA was not enforced.
October 12, Evening	**10+ failed login** attempts to **WidgetApp** from the same IOC IP, indicating attacker activity.
October 13, 9:05 AM	**BDRVLS** successfully accesses the **Password Vault** from the same IOC IP. This confirms access to sensitive data using compromised credentials.
October 14 - 18	Multiple failed Password Vault logins occur from various IPs like **204.44.83.30**. These reflect attempts to reuse or test stolen credentials.
October 15, 10:49 AM	User **DDDXUB** logs into **IT Admin Portal** successfully from IOC IP **180.76.54.93**. This marks the second confirmed compromise.
October 15, 3:06 PM	Cloud access occurs from the same IOC IP. MFA result shows Bypass, indicating the attacker compromised MFA too.
October 24	MFA bypass events continue for Cloud and IT Admin Portal, confirming ongoing attacker access using the same infrastructure.
October 25 - 31	Attacker switches to new infrastructure using IP 104.227.59.62 (not flagged as IOC). Multiple successful and failed logins from this IP suggest persistent access attempts.

4 Dashboard Development and Insights

As part of the breach investigation process, a series of dashboards were created in Splunk to enhance **visibility** across different stages of the attack. These dashboards were designed to guide the investigation from initial detection to deeper user activity correlation, with each dashboard serving a distinct analytical purpose.

4.1 Dashboard 1 – IOC and User Visibility Overview

The first dashboard was developed to help identify which **users** interacted with known **malicious domains** within the IOC dataset. By filtering **DNS logs** against known phishing and malware-related URLs, this dashboard surfaced all **internal users** who accessed **suspicious infrastructure**. It also provides **timestamped** access details and summarized the most frequently contacted IOCs within the environment. This dashboard served as the starting point for investigation by helping narrow down which users and endpoints warranted further analysis (See **Appendix B1** and **B2**).

4.2 Dashboard 2 – User-Centric MFA and IP Investigation

Once potentially compromised users were identified in Dashboard 1, the second dashboard was used to dive deeper into their **authentication behavior**. This dashboard displayed **MFA activity per user**, including the result of each authentication (e.g., Pass, Fail, N/A) and the associated IP addresses. By observing inconsistencies - such as successful logins from external or IOC-tagged IPs, or repeated MFA "Bypass" results - investigators could assess whether an account had been compromised. This dashboard played a critical role in detecting **privilege escalation** and **credential misuse** (See **Appendix B3** and **B4**).

4.3 Dashboard 3 – Cross-Application Authentication Monitoring

The third dashboard provided a comprehensive view of authentication activity across all enterprise applications. It showed login attempts by **user account**, and **source IP**, allowing analysts to detect patterns of lateral movement and unauthorized access. If multiple users were logging in from the same suspicious IP address, or if a user was **authenticating** across **unrelated systems**, these anomalies could be flagged for further inspection. Additionally, usernames identified in this dashboard could be traced back to Dashboard 2 to review their MFA logs in more detail (See **Appendix B5** and **B6**).

Together, these three dashboards created a structured workflow for threat detection and incident analysis. Investigators could move from broad IOC detection to focused user activity review, and finally to comprehensive access correlation across systems. This layered approach ensured that suspicious patterns were not only detected but also contextualized, allowing for evidence-based conclusions about **user compromise**, and **persistence**.

5 Strategic Recommendations

This section outlines high-level strategic recommendations to strengthen Widget Co.'s overall security posture. These recommendations are designed to address both technical and organizational gaps that contributed to the breach. The recommendations are divided into two categories: **technical remediation** steps for the IT/Security team and **policy-level reforms** for executive leadership.

5.1 Technical Remediation (IT/Security Operations)

- Enforce **network-based geo-restrictions** for privileged account logins.
- Enable behavioral alerting for **MFA results** and **failed logins** using Splunk or SOAR tools.
- **Patch Systems** to avoid MFA misconfigurations and reduce likelihood of bypass exploits.
- Revalidate **user roles** and **reset credentials** with mandatory password rotation.
- Update **IOC blocklists**and **threat feeds weekly**.

5.2 Organizational Policy Reform (Executive Management)

- Launch mandatory employee **security awareness training** with emphasis on phishing and social engineering.
- Develop an executive-level breach **response plan** with CISO coordination.
- Integrate **cybersecurity risk metrics** into board-level reporting.
- Conduct red/blue team exercises to simulate incident scenarios semi-annually.

6 Conclusion

This investigation confirmed that Widget Co. was the target of an organized cyber attack. The attacker used a mix of common and stealthy techniques to break into systems. Over the course of 30 days, they were able to steal credentials, get around multi-factor authentication (MFA), and move from one system to another to gain deeper access. Each stage of this attack was carefully executed.

Splunk played a key role in helping us understand what happened. It acted as our central investigation tool. By combining data from many sources, we were able to connect the dots. We used the IOCs such as suspicious IP addresses and domains to track attacker behaviour and confirm when and where systems were accessed.

The detailed analysis revealed several areas where the company's security could be improved. Some weaknesses were technical, like allowing MFA to be bypassed or not catching unusual login behavior. Others were procedural, such as not training employees enough on how to spot phishing emails. Our recommendations include strengthening MFA policies, setting up smarter alerting for unusual behaviour, blocking known threat actors using updated threat intelligence , and conducting regular security training for staff.

By fixing these issues, Widget Co. can go beyond simply reacting to threats. Instead, the company can move toward predicting and stopping attacks before they succeed. Our goal is to improve both day-to-day defenses and long term readiness so that organization is better protected against future threats.

7 Appendix

7.1 Splunk Queries and Outputs

```
index=final_project source="dns.csv"
| eval dns_lower=lower('DNS Hit')
| lookup IOC_lookup_URL_file.csv value AS dns_lower OUTPUT value AS Matched_ioc
| where isnotnull(Matched_ioc)
| sort "Machine Assignment", "DNS Hit"
| table "Machine Assignment", Date, "DNS Hit"
```

Figure A1: DNS Log Query for IOC Matching

Machine Assignment	Date	DNS Hit
BDRVLS	10/12/22	https://glasslu.com
CSSDEH	10/2/22	https://kugk.ml
CVNMWA	10/3/22	http://golang666.xyz
CVNMWA	10/1/22	https://xo176.com
CYPFUK	10/2/22	https://admin102rbc.top/raiffeisen-hu/direkt/
CYPFUK	10/5/22	https://lakeuthfreddie.buzz/well-fargo-rd5em%20(2)%20(1).zip
CYPFUK	10/15/22	https://lakeuthfreddie.buzz/xbalti%20v5%20+/
DMEHYS	10/25/22	https://collinsburgh.buzz/pol/adobe2020/
DSJVOU	10/7/22	https://collab-land.exchange
DTEQNT	10/23/22	https://ectc-change.myvnc.com
DTEQNT	10/22/22	https://postofficeservices.info/

Figure A2: Matched DNS Hits with Known Malicious Domains

DTEQNT	10/30/22	https://yvonnesprings.buzz/auntmarthas/
DYHOPL	10/11/22	https://aeon.co.jp.xo176.com
ECXYIM	10/10/22	https://cliente-suporte2via.xyz
ECXYIM	10/23/22	https://ect-manage.serveirc.com
GYDTBY	10/18/22	https://ibank-nbg.info/gr/
GYDTBY	10/25/22	https://porttadsumme.buzz/bid/dds.zip
KDRDKK	10/26/22	http://postofficeservices.info/
LMZDLG	10/7/22	https://smbc.co.jp.celikcatici.com
LMZDLG	10/8/22	https://vital-ameli-assur.fr

Figure A3: Additional DNS Hits to Malicious Domains

Machine Assignment	Date	DNS Hit
LPCMZW	10/19/22	https://www.celikcatici.com
MJQRQN	10/16/22	http://cflix.work/
MJQRQN	10/20/22	https://etc-wrong.myvnc.com
MJQRQN	10/3/22	https://www.eki-net-member.wd9k5td.cn
MOSNTB	10/22/22	https://www.smbc-zard.shop
ONUWQY	10/25/22	https://aeon.co.jp.gosgod.com
ORLPHK	10/25/22	https://ecr.serveirc.com
PDFUFA	10/20/22	https://admin99101938.buzz/raiffeisen/hu/
PQCCZM	10/8/22	https://payment-receipt.buzz/keybank.zip
PUXGPA	10/5/22	https://manage-ect.servebeer.com
QZUROY	10/4/22	https://mairie-socx.com
RUDONQ	10/14/22	http://elitemaxx.online/elite.apk

Figure A4: Continued DNS Activity from Multiple Hosts to IOC-Flagged Domains

SBVXFQ	10/23/22	http://bridge-wallet.xyz/
SBVXFQ	10/15/22	https://gregfurturt.buzz/doc/
SHTFOY	10/27/22	https://www.paidy.clzikjf.cn
SWKJKJ	10/16/22	http://32868.port0.org/st/
TCNCHM	10/30/22	http://linkgrupwavirallhot2022.duckdns.org/
TCNCHM	10/12/22	https://inemocharlieg.buzz/viewdocs/
TCNCHM	10/14/22	https://scottwayhigh.buzz/gb/adobe2020/
TIIYAW	10/29/22	http://aaron1988.net/content/aaron_resume.docx

Figure A5: DNS Hits to Malicious Domains Continued

Machine Assignment	Date	DNS Hit
TIIYAW	10/19/22	https://metamask-recovery.site
TIIYAW	10/14/22	https://www.aeon.jp.co.glasslu.com
TNZRYD	10/30/22	https://aeon.jp.xo176.com
TNZRYD	10/20/22	https://davidgerard.co.uk
UCKIVO	10/26/22	https://www.jcb.parnknx.cn
VFMXOJ	10/28/22	https://newuthcarol.buzz/viewdocs/
VMQNMJ	10/30/22	http://tradingcoinsolution.space/wallet.html
VMQNMJ	10/22/22	https://mitchellre.buzz/col/file365.zip
WNPDEY	10/7/22	https://ajudacliente-2via.xyz
XEPHHE	10/19/22	https://febenvi.duckdns.org:2050
XEPHHE	10/25/22	https://royalpromy.site/installer/royalpro.apk
XEPHHE	10/27/22	https://smbc-nger.shop
YUQFQN	10/7/22	https://www.mb75.cn/
ZTMURG	10/25/22	https://www.dbl5pzt.cn

Figure A6: Additional Malicious Domain Hits

```
index=final_project source="mfa.csv"
Username="BDRVLS"
| eval event_time = strptime(Date." ".Time, "%m/%d/%y %I:%M:%S %p")
| eval Date_Time = strftime(event_time, "%Y-%m-%d %H:%M:%S")
| sort event_time
| table Date_Time, source, Username, Application, Result, "IP Address"
```

Figure A7: MFA Log Query for USer BDRVLS

Date_Time	source	Username	Application	Result	IP Address
2022-10-01 15:10:05	MFA.csv	BDRVLS	Billing Software	N/A	70.107.95.217
2022-10-02 08:26:53	MFA.csv	BDRVLS	Productivity Suite	N/A	70.107.95.217
2022-10-02 10:01:55	MFA.csv	BDRVLS	Productivity Suite	N/A	70.107.95.217
2022-10-03 15:28:48	MFA.csv	BDRVLS	Billing Software	N/A	70.107.95.217
2022-10-06 13:04:48	MFA.csv	BDRVLS	Productivity Suite	N/A	70.107.95.217
2022-10-12 16:59:59	MFA.csv	BDRVLS	Billing Software	N/A	180.76.54.93
2022-10-13 09:06:12	MFA.csv	BDRVLS	Productivity Suite	N/A	180.76.54.93
2022-10-15 18:00:00	MFA.csv	BDRVLS	Productivity Suite	N/A	70.107.95.217
2022-10-22 13:24:58	MFA.csv	BDRVLS	Billing Software	N/A	70.107.95.217
2022-10-25 17:31:12	MFA.csv	BDRVLS	Billing Software	N/A	70.107.95.217
2022-10-26 12:31:41	MFA.csv	BDRVLS	Widget Application	N/A	70.107.95.217
2022-10-28 09:20:10	MFA.csv	BDRVLS	Widget Application	N/A	70.107.95.217
2022-10-31 13:49:26	MFA.csv	BDRVLS	Billing Software	N/A	70.107.95.217

Figure A8: MFA Log Events for User BDRVLS

```
index=final_project source="vpn.csv" Username="BDRVLS"
| eval Date_Time = strftime(strptime(Date." ".Time, "%m/%d/%y %I:%M:%S %p"), "%Y-%m-%d %H:%M:%S")
| sort Date_Time
| table Date_Time, Username, Source_IP, Result
```

Figure A9: VPN Log Query for User BDRVLS

Date_Time	Username	Source_IP	Result
2022-10-01 09:41:46	BDRVLS	107.175.94.203	FAIL
2022-10-04 10:52:19	BDRVLS	70.107.95.217	LOGIN
2022-10-04 14:45:36	BDRVLS	70.107.95.217	LOGIN
2022-10-05 11:31:12	BDRVLS	70.107.95.217	LOGIN
2022-10-07 12:30:14	BDRVLS	70.107.95.217	LOGIN
2022-10-10 10:07:41	BDRVLS	158.69.59.92	FAIL
2022-10-10 14:09:36	BDRVLS	87.123.144.71	FAIL
2022-10-11 17:19:41	BDRVLS	81.70.29.244	FAIL
2022-10-12 10:19:12	BDRVLS	155.94.235.128	FAIL
2022-10-16 16:03:22	BDRVLS	70.107.95.217	LOGIN

Figure A10: Login Attempts for User BDRVLS with Multiple External IP

2022-10-17 12:57:36	BDRVLS	70.107.95.217	LOGIN
2022-10-19 14:28:19	BDRVLS	96.45.169.106	FAIL
2022-10-20 14:52:48	BDRVLS	70.107.95.217	LOGIN
2022-10-21 09:41:46	BDRVLS	70.107.95.217	LOGIN
2022-10-24 09:40:19	BDRVLS	70.107.95.217	LOGIN
2022-10-26 10:22:05	BDRVLS	113.193.77.6	FAIL
2022-10-28 08:03:50	BDRVLS	45.95.11.34	FAIL
2022-10-28 12:10:05	BDRVLS	115.144.69.8	FAIL
2022-10-29 14:06:43	BDRVLS	70.107.95.217	LOGIN

Figure A11: VPN Login Activity for User BDRVLS

```
index=final_project source="passwordvault.csv" Username="BDRVLS"
| eval Date_Time = strftime(strptime(Date." ".Time, "%m/%d/%y %I:%M:%S %p"), "%Y-%m-%d %H:%M:%S")
| table Date_Time, Date, Time, Src_IP, Username, Authentication
| sort Date_Time
```

Figure A12: Password Vault Log Query for User BDRVLS

Date_Time	Date	Time	Src_IP	Username	Authentication
2022-10-02 08:12:29	10/2/22	8:12:29 AM	107.172.134.54	BDRVLS	Fail
2022-10-04 17:32:38	10/4/22	5:32:38 PM	37.140.192.211	BDRVLS	Fail
2022-10-07 09:02:53	10/7/22	9:02:53 AM	70.107.95.217	BDRVLS	Fail
2022-10-10 14:52:48	10/10/22	2:52:48 PM	212.107.17.182	BDRVLS	Fail
2022-10-11 09:14:24	10/11/22	9:14:24 AM	70.107.95.217	BDRVLS	Success
2022-10-13 09:05:09	10/13/22	9:05:09 AM	180.76.54.93	BDRVLS	Success
2022-10-13 15:51:50	10/13/22	3:51:50 PM	34.92.83.202	BDRVLS	Fail
2022-10-14 10:16:19	10/14/22	10:16:19 AM	204.44.83.30	BDRVLS	Fail
2022-10-14 13:17:46	10/14/22	1:17:46 PM	70.107.95.217	BDRVLS	Fail
2022-10-18 09:48:58	10/18/22	9:48:58 AM	70.107.95.217	BDRVLS	Success
2022-10-18 16:43:41	10/18/22	4:43:41 PM	70.107.95.217	BDRVLS	Success

Figure A13: Password Vault Access Attempts for User BDRVLS

2022-10-22 10:00:29	10/22/22	10:00:29 AM	108.166.201.112	BDRVLS	Fail
2022-10-22 11:09:36	10/22/22	11:09:36 AM	1.117.152.37	BDRVLS	Fail
2022-10-24 11:32:38	10/24/22	11:32:38 AM	70.107.95.217	BDRVLS	Fail
2022-10-25 13:06:14	10/25/22	1:06:14 PM	70.107.95.217	BDRVLS	Success
2022-10-25 13:22:05	10/25/22	1:22:05 PM	70.107.95.217	BDRVLS	Success
2022-10-26 11:28:19	10/26/22	11:28:19 AM	70.107.95.217	BDRVLS	Fail
2022-10-28 12:00:00	10/28/22	12:00:00 PM	119.136.24.157	BDRVLS	Fail

Figure A14: Continued Password Vault Access Attempts

```
index=final_project source="widgetapp.csv" User="BDRVLS"
| eval Date_Time = strftime(strptime(Date." ".Time, "%m/%d/%y %I:%M:%S %p"), "%Y-%m-%d %H:%M:%S")
| table Date_Time, IP_Add, User, Auth
| sort Date_Time
```

Figure A15: WidgetApp Log Query for User BDRVLS

Date_Time	IP_Add	User	Auth
2022-10-04 17:49:55	40.121.241.79	BDRVLS	Fail
2022-10-04 17:49:55	40.121.241.79	BDRVLS	Fail
2022-10-12 17:03:02	180.76.54.93	BDRVLS	Fail
2022-10-12 17:03:02	180.76.54.93	BDRVLS	Fail
2022-10-12 17:05:02	180.76.54.93	BDRVLS	Fail
2022-10-12 17:05:02	180.76.54.93	BDRVLS	Fail
2022-10-12 17:05:29	180.76.54.93	BDRVLS	Fail
2022-10-12 17:05:29	180.76.54.93	BDRVLS	Fail
2022-10-12 17:05:41	180.76.54.93	BDRVLS	Fail
2022-10-12 17:05:41	180.76.54.93	BDRVLS	Fail
2022-10-12 17:05:59	180.76.54.93	BDRVLS	Fail
2022-10-12 17:05:59	180.76.54.93	BDRVLS	Fail
2022-10-26 12:31:41	70.107.95.217	BDRVLS	Pass
2022-10-26 12:31:41	70.107.95.217	BDRVLS	Pass
2022-10-28 09:20:10	70.107.95.217	BDRVLS	Pass
2022-10-28 09:20:10	70.107.95.217	BDRVLS	Pass

Figure A16: WidgetApp Authentication Attempts for User BDRVLS

```
index=final_project source="mfa.csv"
Username="DDDXUB"
| eval event_time = strptime(Date." ".Time, "%m/%d/%y %I:%M:%S %p")
| eval Date_Time = strftime(event_time, "%Y-%m-%d %H:%M:%S")
| sort event_time
| table Date_Time, source, Username, Application, Result, "IP Address"
```

Figure A17: MFA Log Query for User DDDXUB

Date_Time	source	Username	Application	Result	IP Address
2022-10-02 16:40:48	MFA.csv	DDDXUB	Productivity Suite	Pass	104.227.59.62
2022-10-04 16:39:22	MFA.csv	DDDXUB	Widget Application	Pass	104.227.59.62
2022-10-06 09:11:31	MFA.csv	DDDXUB	Productivity Suite	Pass	104.227.59.62
2022-10-11 13:37:55	MFA.csv	DDDXUB	Ticketing System	Pass	104.227.59.62
2022-10-13 17:51:22	MFA.csv	DDDXUB	Productivity Suite	Pass	104.227.59.62
2022-10-15 10:49:01	MFA.csv	DDDXUB	IT Admin Portal	Pass	180.76.54.93
2022-10-15 15:06:00	MFA.csv	DDDXUB	Cloud	Pass	180.76.54.93
2022-10-18 15:28:48	MFA.csv	DDDXUB	Widget Application	Pass	104.227.59.62
2022-10-24 14:48:06	MFA.csv	DDDXUB	IT Admin Portal	Pass	180.76.54.93
2022-10-24 14:56:45	MFA.csv	DDDXUB	Cloud	Pass	180.76.54.93
2022-10-25 13:24:58	MFA.csv	DDDXUB	Ticketing System	Pass	104.227.59.62
2022-10-25 18:38:53	MFA.csv	DDDXUB	Ticketing System	Pass	104.227.59.62
2022-10-27 10:50:53	MFA.csv	DDDXUB	IT Admin Portal	Fail	104.227.59.62
2022-10-29 09:57:36	MFA.csv	DDDXUB	IT Admin Portal	Fail	104.227.59.62
2022-10-31 14:58:34	MFA.csv	DDDXUB	IT Admin Portal	Pass	104.227.59.62

Figure A18: MFA Log Activity for User DDDXUB

```
index=final_project source="vpn.csv" Username="DDDXUB"
| eval Date_Time = strftime(strptime(Date." ".Time, "%m/%d/%y %I:%M:%S %p"), "%Y-%m-%d %H:%M:%S")
| sort Date_Time
| table Date_Time, Username, Source_IP, Result
```

Figure A19: VPN Log Query for User DDDXUB

Date_Time	Username	Source_IP	Result
2022-10-01 13:49:26	DDDXUB	104.227.59.62	LOGIN
2022-10-02 10:50:53	DDDXUB	107.175.64.68	FAIL
2022-10-03 12:01:26	DDDXUB	104.227.59.62	LOGIN
2022-10-06 08:13:55	DDDXUB	104.227.59.62	LOGIN
2022-10-07 16:24:58	DDDXUB	34.82.215.174	FAIL
2022-10-11 11:57:07	DDDXUB	104.227.59.62	LOGIN
2022-10-15 14:51:22	DDDXUB	104.227.59.62	LOGIN
2022-10-16 13:12:00	DDDXUB	104.227.59.62	LOGIN
2022-10-19 16:22:05	DDDXUB	107.174.64.49	FAIL
2022-10-23 10:24:58	DDDXUB	31.44.184.187	FAIL
2022-10-23 14:02:24	DDDXUB	104.227.59.62	LOGIN
2022-10-23 16:36:29	DDDXUB	104.227.59.62	LOGIN
2022-10-25 11:22:34	DDDXUB	104.227.59.62	LOGIN
2022-10-25 17:22:34	DDDXUB	202.61.137.79	FAIL
2022-10-26 17:54:14	DDDXUB	104.227.59.62	LOGIN
2022-10-28 16:48:00	DDDXUB	104.227.59.62	LOGIN

Figure A20: VPN Login Activity for User DDDXUB with IOC IP Usage

```
index=final_project source="passwordvault.csv" Username="DDDXUB"
| eval Date_Time = strftime(strptime(Date." ".Time, "%m/%d/%y %I:%M:%S %p"), "%Y-%m-%d %H:%M:%S")
| table Date_Time, Date, Time, Src_IP, Username, Authentication
| sort Date_Time
```

Figure A21: Password Vault Log Query for User DDDXUB

Date_Time	Date	Time	Src_IP	Username	Authentication
2022-10-01 10:22:05	10/1/22	10:22:05 AM	45.130.41.33	DDDXUB	Fail
2022-10-02 11:48:29	10/2/22	11:48:29 AM	104.227.59.62	DDDXUB	Success
2022-10-08 17:41:17	10/8/22	5:41:17 PM	47.100.131.229	DDDXUB	Fail
2022-10-09 09:56:10	10/9/22	9:56:10 AM	104.227.59.62	DDDXUB	Fail
2022-10-11 10:23:31	10/11/22	10:23:31 AM	104.227.59.62	DDDXUB	Success
2022-10-11 17:12:29	10/11/22	5:12:29 PM	104.227.59.62	DDDXUB	Success
2022-10-12 15:23:02	10/12/22	3:23:02 PM	192.161.55.124	DDDXUB	Fail
2022-10-14 09:15:50	10/14/22	9:15:50 AM	155.94.144.43	DDDXUB	Fail
2022-10-16 09:46:05	10/16/22	9:46:05 AM	124.223.185.141	DDDXUB	Fail
2022-10-16 16:52:19	10/16/22	4:52:19 PM	104.227.59.62	DDDXUB	Fail
2022-10-16 17:38:24	10/16/22	5:38:24 PM	104.227.59.62	DDDXUB	Success

Figure A22: Password Vault Access Attempts

2022-10-17 09:01:26	10/17/22	9:01:26 AM	144.202.49.189	DDDXUB	Fail
2022-10-20 08:18:14	10/20/22	8:18:14 AM	8.211.138.50	DDDXUB	Fail
2022-10-22 09:15:50	10/22/22	9:15:50 AM	107.175.94.203	DDDXUB	Fail
2022-10-24 10:49:26	10/24/22	10:49:26 AM	103.140.150.196	DDDXUB	Fail
2022-10-25 11:34:05	10/25/22	11:34:05 AM	104.227.59.62	DDDXUB	Success
2022-10-25 12:33:07	10/25/22	12:33:07 PM	159.75.249.102	DDDXUB	Fail
2022-10-25 15:56:10	10/25/22	3:56:10 PM	104.227.59.62	DDDXUB	Success
2022-10-26 09:10:05	10/26/22	9:10:05 AM	104.227.59.62	DDDXUB	Success
2022-10-31 15:04:19	10/31/22	3:04:19 PM	155.94.228.110	DDDXUB	Fail

Figure A23: Continued Password Vault Access Attempts for User DDDXUB

```
index=final_project source="ticketing.csv" Username="DDDXUB"
| eval event_time=strptime(Date." ".Time, "%m/%d/%y %I:%M:%S %p")
| eval Date_Time=strftime(event_time, "%Y-%m-%d %H:%M:%S")
| sort event_time
| table Date_Time, Username, Src_IP, Result
```

Figure A24: Ticketing System Log Query for DDDXUB

Date_Time	Username	Src_IP	Result
2022-10-02 15:38:53	DDDXUB	96.43.94.227	Fail
2022-10-09 11:41:17	DDDXUB	150.158.214.246	Fail
2022-10-11 13:37:55	DDDXUB	104.227.59.62	Success
2022-10-25 13:24:58	DDDXUB	104.227.59.62	Success
2022-10-25 18:38:53	DDDXUB	104.227.59.62	Success

Figure A25: Ticketing System Access Attempts

```
index=final_project source="widgetapp.csv" User="DDDXUB"
| eval Date_Time = strftime(strptime(Date." ".Time, "%m/%d/%y %I:%M:%S %p"), "%Y-%m-%d %H:%M:%S")
| table Date_Time, IP_Add, User, Auth
| sort Date_Time
```

Figure A26: WidgetApp Log Query for User DDDXUB

Date_Time	IP_Add	User	Auth
2022-10-04 16:39:22	104.227.59.62	DDDXUB	Pass
2022-10-04 16:39:22	104.227.59.62	DDDXUB	Pass
2022-10-07 14:16:48	118.163.107.217	DDDXUB	Fail
2022-10-07 14:16:48	118.163.107.217	DDDXUB	Fail
2022-10-18 15:28:48	104.227.59.62	DDDXUB	Pass
2022-10-18 15:28:48	104.227.59.62	DDDXUB	Pass

Figure A27: WidgetApp Access Events for User DDDXUB

```
index=final_project source="itadmin.csv" Username="DDDXUB"
| eval Date_Time = strftime(strptime(Date." ".Time, "%m/%d/%y %I:%M:%S %p"), "%Y-%m-%d %H:%M:%S")
| table Date_Time, IP, Username, "Login Status"
| sort Date_Time
```

Figure A28: IT Admin Portal Log Query for User DDDXUB

Date_Time	IP	Username	Login Status
2022-10-03 14:36:58	45.249.94.56	DDDXUB	Fail
2022-10-12 17:45:36	104.129.12.238	DDDXUB	Fail
2022-10-15 10:49:01	180.76.54.93	DDDXUB	Success
2022-10-24 14:48:06	180.76.54.93	DDDXUB	Success
2022-10-27 10:50:53	104.227.59.62	DDDXUB	Success
2022-10-29 09:57:36	104.227.59.62	DDDXUB	Success
2022-10-31 14:58:34	104.227.59.62	DDDXUB	Success

Figure A29: IT Admin Portal Login Events for User DDDXUB

7.2 Dashboards and Insights

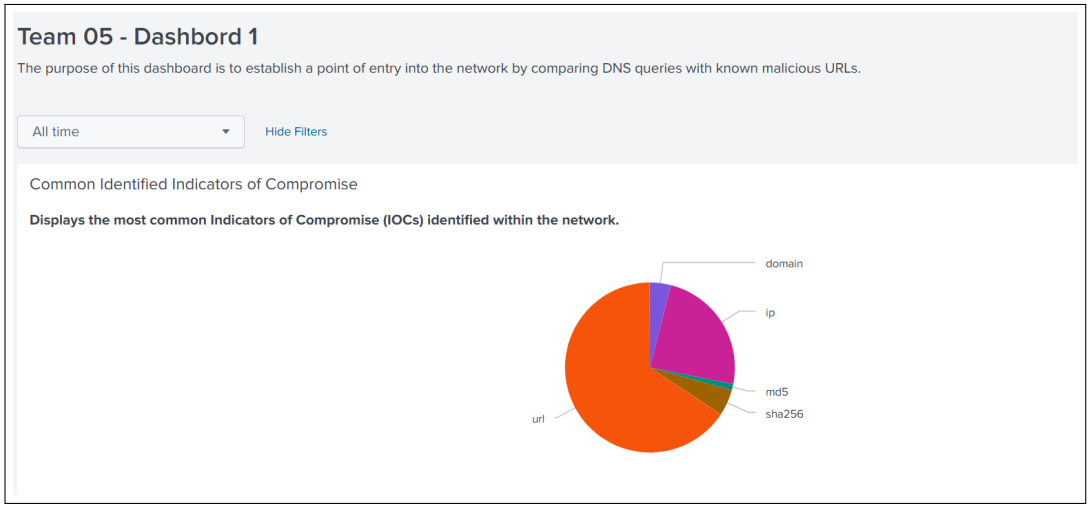
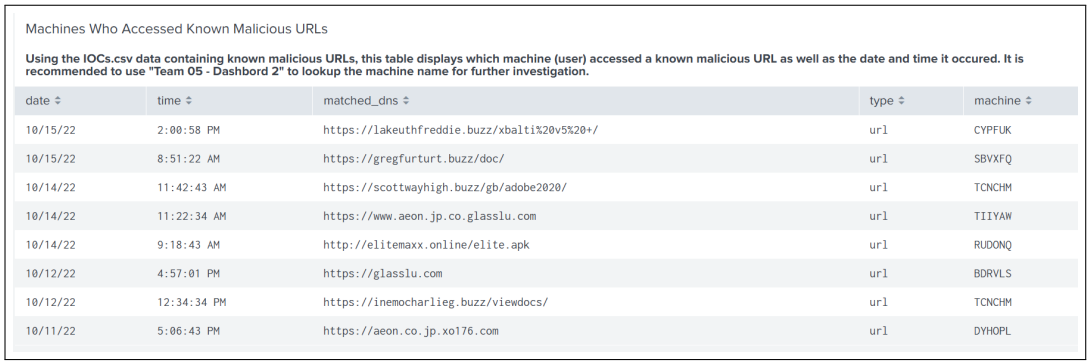


Figure B1: Dashboard 01 – Entry Point Identification via DNS IOC Correlation



Machines Who Accessed Known Malicious URLs

Using the IOCs.csv data containing known malicious URLs, this table displays which machine (user) accessed a known malicious URL as well as the date and time it occured. It is recommended to use "Team 05 - Dashbord 2" to lookup the machine name for further investigation.

date	time	matched_dns	type	machine
10/15/22	2:00:58 PM	https://lakeuthfreddie.buzz/xbalti%20v5%20+/	url	CYPFUK
10/15/22	8:51:22 AM	https://gregfurturt.buzz/doc/	url	SBVXFQ
10/14/22	11:42:43 AM	https://scottwayhigh.buzz/gb/adobe2020/	url	TCNCHM
10/14/22	11:22:34 AM	https://www.aeon.jp.co.glasslu.com	url	TIIYAW
10/14/22	9:18:43 AM	http://elitemaxx.online/elite.apk	url	RUDONQ
10/12/22	4:57:01 PM	https://glasslu.com	url	BDRVLS
10/12/22	12:34:34 PM	https://inemocharlieg.buzz/viewdocs/	url	TCNCHM
10/11/22	5:06:43 PM	https://aeon.co.jp.xo176.com	url	DYHOPL

Figure B2: Dashboard 01 – Table of Machines Accessing Known Malicious URLs

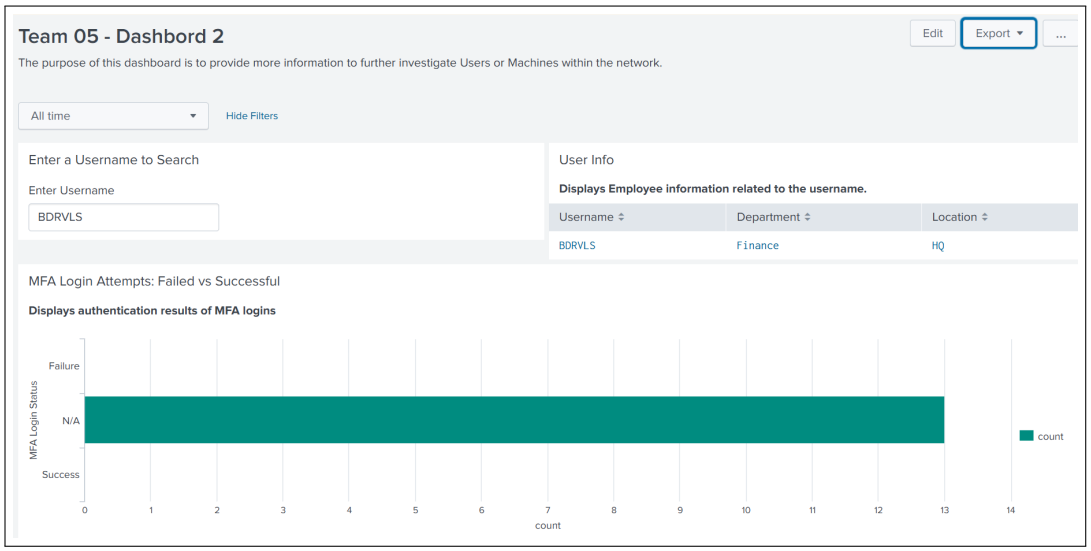
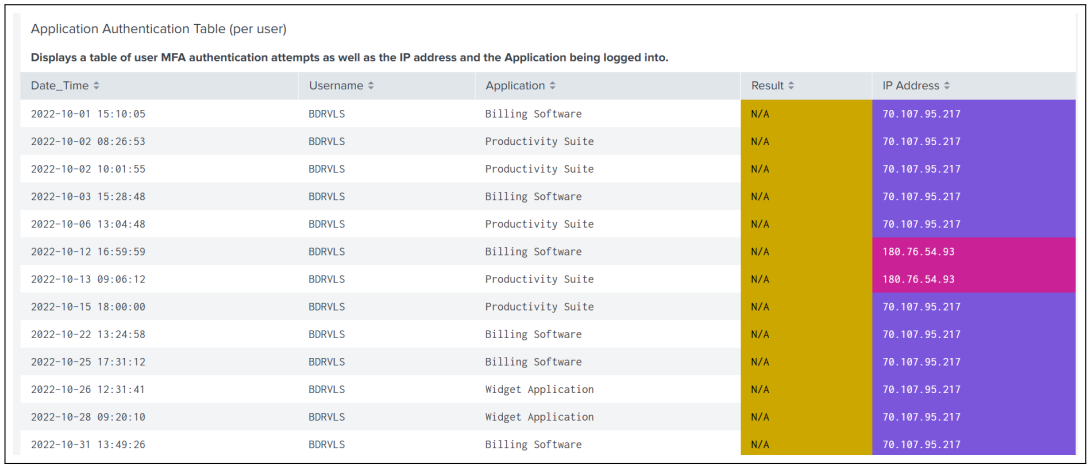


Figure B3: Dashboard 02 - MFA Login Results for User BDRVLS

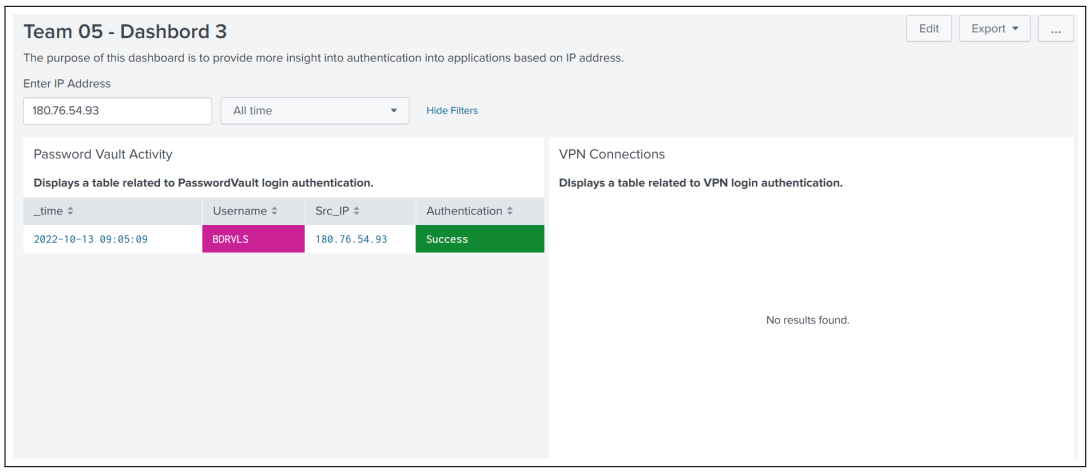


Application Authentication Table (per user)

Displays a table of user MFA authentication attempts as well as the IP address and the Application being logged into.

Date_Time	Username	Application	Result	IP Address
2022-10-01 15:10:05	BDRVLS	Billing Software	N/A	70.107.95.217
2022-10-02 08:26:53	BDRVLS	Productivity Suite	N/A	70.107.95.217
2022-10-02 10:01:55	BDRVLS	Productivity Suite	N/A	70.107.95.217
2022-10-03 15:28:48	BDRVLS	Billing Software	N/A	70.107.95.217
2022-10-06 13:04:48	BDRVLS	Productivity Suite	N/A	70.107.95.217
2022-10-12 16:59:59	BDRVLS	Billing Software	N/A	180.76.54.93
2022-10-13 09:06:12	BDRVLS	Productivity Suite	N/A	180.76.54.93
2022-10-15 18:00:00	BDRVLS	Productivity Suite	N/A	70.107.95.217
2022-10-22 13:24:58	BDRVLS	Billing Software	N/A	70.107.95.217
2022-10-25 17:31:12	BDRVLS	Billing Software	N/A	70.107.95.217
2022-10-26 12:31:41	BDRVLS	Widget Application	N/A	70.107.95.217
2022-10-28 09:20:10	BDRVLS	Widget Application	N/A	70.107.95.217
2022-10-31 13:49:26	BDRVLS	Billing Software	N/A	70.107.95.217

Figure B4: Dashboard 02 - Authentication Activity for User BDRVLS



Team 05 - Dashbord 3

Edit Export ...

The purpose of this dashboard is to provide more insight into authentication into applications based on IP address.

Enter IP Address

180.76.54.93 All time Hide Filters

Password Vault Activity

Displays a table related to PasswordVault login authentication.

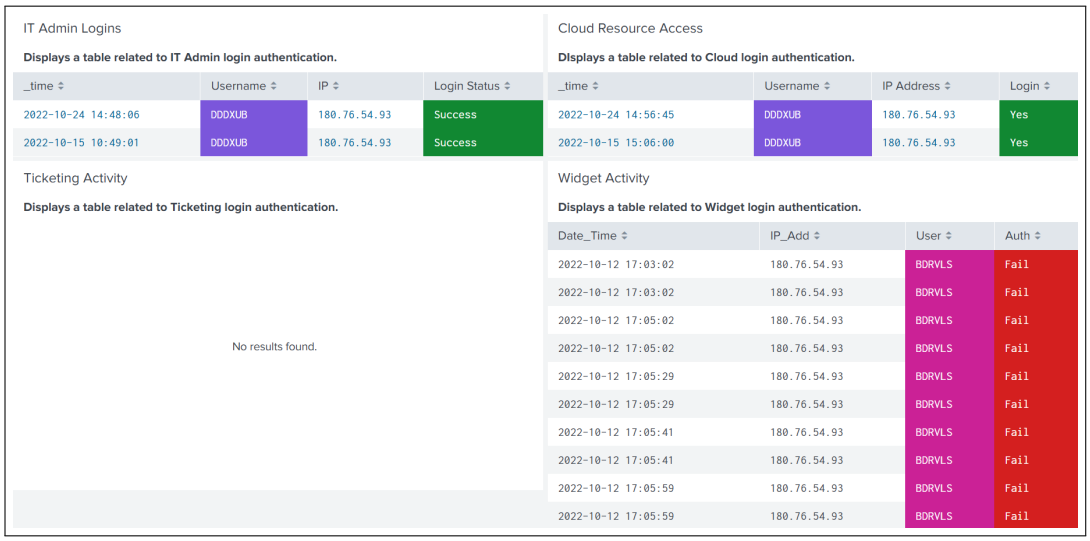
_time	Username	Src_IP	Authentication
2022-10-13 09:05:09	BDRVLS	180.76.54.93	Success

VPN Connections

Displays a table related to VPN login authentication.

No results found.

Figure B5: Dashboard 03 - Password Vault Login from IOC-Tagged IP



IT Admin Logins

Displays a table related to IT Admin login authentication.

_time	Username	IP	Login Status
2022-10-24 14:48:06	DDDXUB	180.76.54.93	Success
2022-10-15 10:49:01	DDDXUB	180.76.54.93	Success

Cloud Resource Access

Displays a table related to Cloud login authentication.

_time	Username	IP Address	Login
2022-10-24 14:56:45	DDDXUB	180.76.54.93	Yes
2022-10-15 15:06:00	DDDXUB	180.76.54.93	Yes

Ticketing Activity

Displays a table related to Ticketing login authentication.

No results found.

Widget Activity

Displays a table related to Widget login authentication.

Date_Time	IP_Add	User	Auth
2022-10-12 17:03:02	180.76.54.93	BDRVLS	Fail
2022-10-12 17:03:02	180.76.54.93	BDRVLS	Fail
2022-10-12 17:05:02	180.76.54.93	BDRVLS	Fail
2022-10-12 17:05:02	180.76.54.93	BDRVLS	Fail
2022-10-12 17:05:29	180.76.54.93	BDRVLS	Fail
2022-10-12 17:05:29	180.76.54.93	BDRVLS	Fail
2022-10-12 17:05:41	180.76.54.93	BDRVLS	Fail
2022-10-12 17:05:41	180.76.54.93	BDRVLS	Fail
2022-10-12 17:05:59	180.76.54.93	BDRVLS	Fail
2022-10-12 17:05:59	180.76.54.93	BDRVLS	Fail

Figure B6: Dashboard 03 - Correlation of IOC-Tagged IP Across Multiple Services