



Strengthening Security at TeamViewer to Mitigate Advanced Threats

Agenda



Introduction



Recommendation



Implementation



Financials



Risks and Mitigation

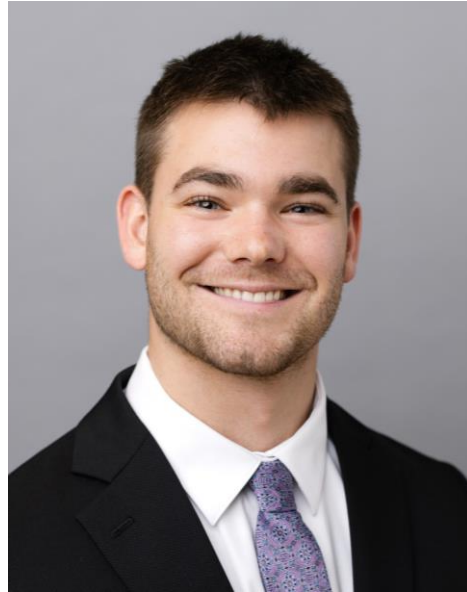


Conclusion

Meet the Team



Shane Rodriguez



Garrett Williams



Jong Won Choi



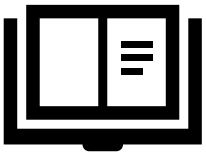
Anirban Das

Identifying and Solving Key Security Challenges from the TeamViewer Breach



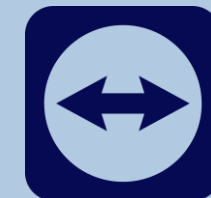
In June 2024, TeamViewer's monitoring system detected unauthorized access within its corporate IT environment, attributed to the state-sponsored hacking group APT29. The breach was contained before impacting customer data, but it exposed vulnerabilities in current credential management and detection measures

APT29's sophisticated tactics exploited gaps in TeamViewer's security protocols. The incident underscores the limitations of traditional security measures and highlights a pressing need for more robust defenses to safeguard sensitive systems and data



How can TeamViewer strengthen its security framework to prevent, detect, and respond to advanced cyber threats, ensuring future resilience against sophisticated actors like APT29?

Who Is APT29 and How Did They Affect TeamViewer?



Advanced Persistent Threat (APT) 29



Hacker groups believed to be linked to the **Russian Foreign Intelligence Service (SVR)**

Spear-Phishing at TeamViewer

Limited Scope of Compromise

- The breach affected only TeamViewer's internal corporate environment and a single employee account
- A broader compromise was avoided, suggesting a targeted phishing attack rather than a brute-force or exploit-based approach

Targeted Credentials Compromise

- Only one employee account was compromised, pointing to legitimate credential theft
- The attack's precision is consistent with phishing, targeting specific users to steal credentials

APT 29's Tactics and Techniques

- APT 29's recent campaign involved phishing emails exploiting RDP access
- The subtle, targeted attack suggests a well-orchestrated phishing campaign aimed at exploiting human weaknesses

Identifying the Root Cause Behind APT29's Spear Phishing Attack



Lack of Employee Training

- Employees were insufficiently trained to recognize sophisticated phishing attacks
- Phishing emails and attachments from external sources were not adequately flagged or avoided



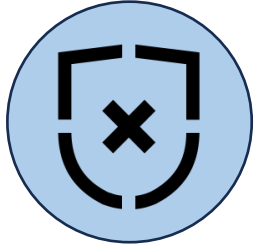
Deficiencies in MFA and Preventive Measures

- Multi-Factor Authentication (MFA) was not sufficiently implemented across all access points
- Preventive measures were inadequate to prevent unauthorized access



Failure to Adhere to Least Privilege Principles

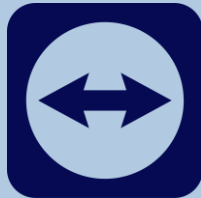
- A single employee account compromise led to broader access to internal credentials
- The absence of a strict privilege policy allowed unnecessarily broader access



Lack of Detective Behavior Monitoring

- No comprehensive analysis of user behavior or daily patterns to identify and flag anomalies
- Absence of proactive monitoring limited the detection of suspicious activities

Implement Training and Security Layers to Address Root Causes



Employee Training

- Employee training using SANS Security Awareness should consist of 1-2 hours of modular training on key topics like phishing, secure browsing, and incident reporting
- This training should be reinforced with quarterly refreshers, post-incident sessions, and regular simulated phishing exercises to assess and improve employee vigilance

Increased Email Monitoring

- For blocking suspicious emails, advanced email security tools (like Zscaler) should be deployed to scan for and block suspicious attachments, links, and emails from known malicious domains
- Emails that are flagged but not blocked should be marked with warning banners to prompt employees to exercise caution with potentially harmful content

Web Filtering

- Web filtering and DNS security can be implemented by using DNS filtering to block known malicious domains, thereby protecting users even if they click on a phishing link
- Real-time link analysis tools can further enhance security by verifying URLs upon click, dynamically preventing access to unsafe sites

Training Programs + Frameworks

[SANS Security Awareness Training and MITRE ATT&CK: Masquerading and Domain Authentication](#)

Advanced Authentication Technology Can Reinforce the Current MFA Process



Current Challenges with Existing MFA

Interception of One-Time Codes (OTP)

- Current MFA methods rely on OTP sent via out-of-band communications. These codes are vulnerable to interception if an adversary gains access to the communication channel or compromises the service provider

Push Notification Attacks and MFA Fatigue

- Push-based MFA can be exploited through repetitive login attempts, bombarding users with notifications which lead to “MFA fatigue” where users mistakenly approve unauthorized requests due to excessive prompts

Keylogger Vulnerability

- Current MFA require users to enter a static PIN along with their smart card and if keylogger is present on the device, and attacker can capture the password entered by the user

Advanced Cryptographic Authentication

Phishing-Resistant Authentication

- Requiring a registered, physical security device eliminate the reliance on OTP
- Attacks on service providers are ineffective

No Push Notification Vulnerabilities

- Users will not receive unsolicited prompts
- Users can avoid the risks of mistakenly approving unauthorized access attempts

Challenge-Response Protocols

- There is no need for static PIN or password
- Keylogger can't capture reusable credentials

Implementing Least Privileges and Role Based Access Controls for an Additional Layer of Protection



Role-Based Access Control (RBAC)

- Establish specific access levels based on job functions, ensuring each role only has permissions necessary for its responsibilities
- Conduct regular audits of access roles to align with evolving job requirements, reducing permission creep over time

Reduce Attack Surface

T1078 (Valid Accounts)

High-Risk Data Segmentation

- Isolate high-risk data from general access by implementing network segmentation, limiting access to sensitive information
- Limit access to critical data strictly to personnel who need it, minimizing potential exposure in case of a breach

Mitigate Insider Threats

T1021 (Remote Services)

Multi-Approval for Privileged Access

- For accessing high-risk resources, mandate dual approval to add an additional layer of security and oversight
- Deploy PAWs for administrative functions to separate privileged actions from routine tasks, reducing phishing-related risks

Reduce Attack Surface

T1055 (Process Injection)

Enhancing Detective Behavior Monitoring through a Multi-Layered Security Strategy



Implement NIST Cybersecurity Framework

- **Identify:** Track and manage all assets, including endpoints
- **Protect:** Enforce secure access and configurations
- **Detect:** Continuously monitor for unusual activity across environments
- **Respond:** Correlate events and address vulnerabilities swiftly
- **Recover:** Test recovery plans to quickly restore systems and data

Incident Alerting and Reporting for Real-Time Threat Response

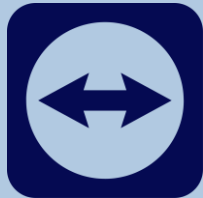
- **Behavioral Baselines for Anomaly Detection:** Use User and Entity Behavior Analytics (UEBA) to establish baselines of normal user behavior and detect deviations
- **Dashboard for Incident Visibility:** Implement a central dashboard to visualize incident trends and provide actionable insights to both security teams and organizational leadership

Utilize Advanced Detection & Centralized Event Management

- **Centralized SIEM Platform:** Use a centralized SIEM platform to aggregate and analyze logs from all environments in a centralized SIEM
- **Threat Intelligence Integration:** Incorporate threat intelligence feeds into the SIEM, enhancing detection capabilities by identifying known malicious indicators such as IPs or file hashes linked to threat actors

This security strategy builds a layered defense, beginning with NIST foundational controls, enhancing proactive alerting and reporting, and culminating in advanced detection and centralized event management to create a multi-tiered barrier against sophisticated threats

Project Completion will be in 8 Months with Training and Continuous Monitoring Following



	Months											
Steps	1	2	3	4	5	6	7	8	9	10	11	12
Stakeholder Buy-In												
Risk Assessment												
Vendor Selection & Procurement												
Deploy SIEM and Threat Intelligence Feeds												
Setup RBAC, PAWs, and MFA												
Launch Employee Training Program												
Simulated Phishing Campaigns												
Continuous Monitoring												
Performance and Security Audit												

Strengthening Security Measures with Strategic Investment



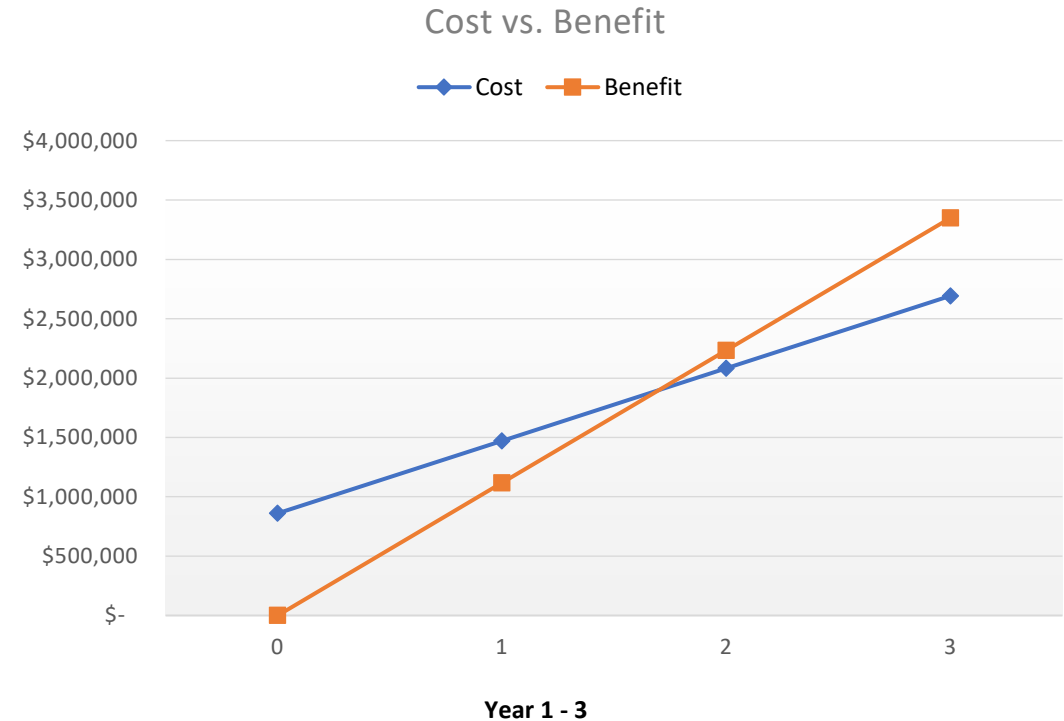
Cost and Benefit Breakdown

Total one-time costs: \$860,000
Total recurring costs: \$1,800,000
Total costs: \$2,660,000

Year 1 benefits: \$1,111,000
Year 2 benefits: \$1,111,000
Year 3 benefits: \$1,111,000
Total benefits: \$3,333,000

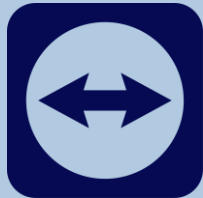
Key Assumptions

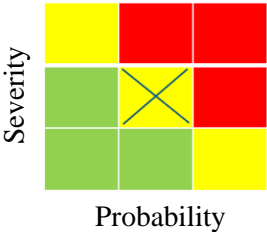
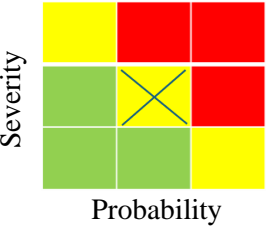
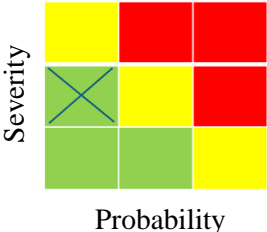
- 20% lower chance of security breach
- Security breach avoidance accounted for every year
- 3 Year projection to show break-even
- WACC is 9.49% (Software industry Std.)



NPV= \$407,576 ROI = 24% B/E: Year 2

Possible Risks will be Mitigated with a Solid Defense Strategy



Risk	Degree	Mitigation Strategy
Over-Reliance on Employee Training		<ul style="list-style-type: none">Ensure Phishing Simulations are promoted along with employee training. Safeguard layers will be used to detect security attacks that pass-through employee training initiatives
Privileged Access Abuse or Misuse		<ul style="list-style-type: none">Streamline the approval process for accessing sensitive resources by automating role-based access control (RBAC) workflows, ensuring quick and efficient access for approved users while enforcing compliance
Insufficient Monitoring Capabilities with SIEM		<ul style="list-style-type: none">Integrate threat intelligence feeds from reputable sources into the SIEM for enhanced detection capabilities. Additionally, implement regular tuning of SIEM rules and thresholds based on new threat intelligence to ensure effective anomaly detection

Implementing a Comprehensive Security Framework for Long-Term Resilience



Address Root Causes



Equip employees with targeted security training and regular phishing simulations to build awareness and make them a proactive part of your defense



Add Layered Protection



Strengthen entry points with strong MFA and advanced email filtering, creating multiple security layers. This approach not only blocks unauthorized access but also safeguards your system in case one layer is compromised



Enforce Least Privilege



Limit access to sensitive information based on roles, ensuring that only essential personnel have access. This minimizes internal risks and ensures critical data is protected from unnecessary exposure



Proactive Monitoring



Implement real-time monitoring to detect and respond to unusual activities quickly. Early detection enables rapid action, containing threats and reducing potential damage

Appendices



Case Assumptions

SANS Security and MITRE

Financial Assumptions

Financial Calculations

Extended Risks

Issue Tree

Sources

TeamViewer Case Assumptions



Assumption: APT29 used a Spear Phishing attack through email to compromise an employee account. We are assuming this because most related incidents involving this group have been through this method.

Source: [APT29 Spearphishing Campaign Targets Thousands with RDP Files - Infosecurity Magazine](#)

Assumption: TeamViewer currently has multifactor authentication with push notification abilities but not password confirmation to authenticate. We are assuming that this needs to be hardened for effective use.

Assumption: The employee account that was hacked was a standard analyst or senior analyst and not an executive employee. This connects with our recommendation for least privileges.

Assumption: There is least privileges currently set up, but it is not standardized or followed completely as shown in the case.

SANS Security Awareness Training and MITRE ATT&CK: Masquerading and Domain Authentication

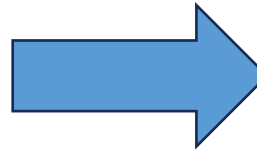


MITRE ATT&CK Domain Authentication

“Train users to recognize and handle suspicious email attachments. Emphasize the importance of caution when opening attachments from unknown or unexpected sources, even if they appear legitimate. Implement email warning banners to alert users about emails originating from outside the organization or containing attachments, reinforcing awareness and helping users identify potential spear phishing attempts.”

MITRE ATT&CK Masquerading

“Train users not to open email attachments or click unknown links (URLs). Such training fosters more secure habits within your organization and will limit many of the risks.”



SANS Security Awareness Training

“SANS is the most trusted and largest source for information security awareness training and security certification in the world. Leverage our best-in-class Security Awareness solutions to transform your organization’s ability to measure and manage human risk.”

Financial Assumptions



- A 2024 analysis by CanIPhish estimates SANS security awareness training at about \$2 per employee per month. For 1,500 employees, this would total roughly \$36,000 annually
- A 2024 estimate from ITQlick suggests Zscaler pricing at around \$2.40 per user per month, totaling roughly \$43,200 annually for 1,500 employees. (itqlick.com)
- **Potential Savings:** Implementing security awareness training and advanced security measures can reduce the likelihood and impact of breaches. Even a 10% reduction equates to approximately \$488,000 in savings.
- **Potential Savings:** By preventing incidents, employees remain productive. If a breach causes a 1% productivity loss across 1,000 employees with an average salary of \$70,000, the annual savings from prevention would be around \$700,000.
- Provide YubiKey 5C NFC to 1200 employees who are not managers and do not require access to sensitive information. Other 300 managers or those who need higher level of access will receive YubiKey C Bio [Buy YubiKeys at Yubico.com](https://www.yubico.com) | [Shop hardware authentication security keys](#)
- Deploying a secure cryptographic authentication infrastructure requires investment in compatible servers and potentially upgrading existing legacy systems [What Is FIDO2 & How Does FIDO Authentication Work?](#)
- Annual costs for support contracts, maintenance of servers, and software updates related to the cryptographic infrastructure; 10–15% of the initial setup cost [Cost of Multi-Factor Authentication: Is It Worth the Price? - 1Kosmos](#)
- Replacing lost or damaged tokens and managing inventory (e.g., for employees leaving or joining); 5–10% of the initial token purchase annually [Cost of Multi-Factor Authentication: Is It Worth the Price? - 1Kosmos](#)
- FIDO2 compatibility upgrade would cost \$250,000
- SIEM software's initial cost would be \$200,000
- TeamViewer handle maximum 300GB of logs per day
- [Salary: Cyber Security Auditor \(Nov, 2024\) United States](#)

Financial Calculations



Net Cash Flows (NCF)	\$	(860,703)	\$	505,421	\$	505,421	\$	505,421
NPV (Annual)	\$	(860,703)	\$	461,614	\$	421,604	\$	385,061
ROI (Running Total)		-100%		-24%		7%		24%
Break Even								

Costs

One-Time (Non-recurring)

Advanced Cryptographic Authentication (YubiKey Bio)	\$	28,500						
Advanced Cryptographic Authentication (YubiKey 5C NFC)	\$	66,000						
FIDO2 compatibility upgrade	\$	250,000						
SIEM software	\$	200,000						
SIEM implementation	\$	50,000						
SIEM MISC	\$	100,000						
Performance and Security Audit (5 auditors)	\$	166,203						
One-Time Costs per Period	\$	860,703						\$ 860,703

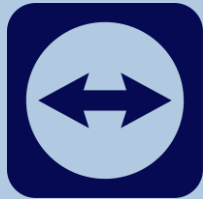
Recurring

Employee Training (CanIPhish)	\$	36,000	\$	36,000	\$	36,000		
Email filtering (Zscaler)	\$	43,200	\$	43,200	\$	43,200		
Annual MFA maintenance cost (10%)	\$	34,450	\$	34,450	\$	34,450		
Replacement of damaged tokens/inventory management (10%)	\$	9,450	\$	9,450	\$	9,450		
Microsoft Sentinel (300GB per day)	\$	337,479	\$	337,479	\$	337,479		
Employee Training for RBAC and Multi-Approval process	\$	150,000	\$	150,000	\$	150,000		
Recurring Costs per Period	\$	-	\$	610,579	\$	610,579	\$	1,831,737

Total One-Time and Recurring Costs per PeriodCosts

Cumulative Costs	\$	860,703	\$	610,579	\$	610,579	\$	2,692,440
	\$	860,703	\$	1,471,282	\$	2,081,861	\$	2,692,440
							\$	7,106,284

Financial Calculations



Benefits

Cost avoidance

Potential Saving from security awareness training and advanced security measure

Avoiding decrease in employee productivity

Total Benefits per Period

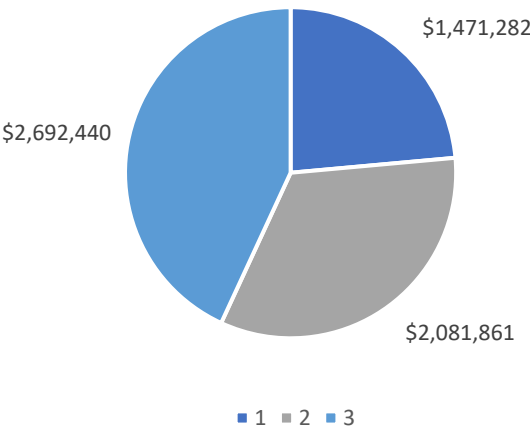
Cumulative Benefits

ROI	24%
NPV	\$ 407,576
IRR	35%

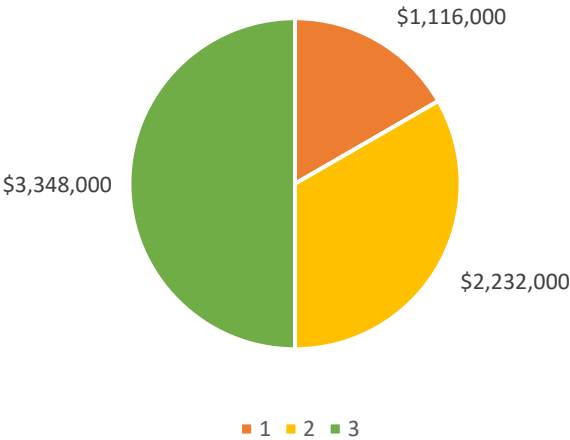
NPV	\$407,576
-----	-----------

	\$	976,000	\$	976,000	\$	976,000	
	\$	140,000	\$	140,000	\$	140,000	
Total Benefits per Period	\$	-	\$	1,116,000	\$	1,116,000	\$ 3,348,000
Cumulative Benefits	\$	-	\$	1,116,000	\$	2,232,000	\$ 3,348,000

Cumulative Costs by Year



Cumulative Benefits by Year



Microsoft Sentinel Pricing



Tier	Microsoft Sentinel Price	Effective Per GB Price ¹	Savings Over Pay-As-You-Go
Pay-As-You-Go	\$5.22 per GB	\$5.22 per GB	N/A
100 GB per day	\$342.52 per day	\$3.43 per GB	34%
200 GB per day	\$633.56 per day	\$3.17 per GB	39%
300 GB per day	\$924.60 per day	\$3.09 per GB	41%
400 GB per day	\$1,198.48 per day	\$3.00 per GB	43%
500 GB per day	\$1,460.80 per day	\$2.93 per GB	44%
1,000 GB per day	\$2,863.40 per day	\$2.87 per GB	45%
2,000 GB per day	\$5,538.80 per day	\$2.77 per GB	47%
5,000 GB per day	\$13,321 per day	\$2.67 per GB	49%
10,000 GB per day	\$25,576 per day	\$2.56 per GB	51%
25,000 GB per day	\$61,467.50 per day	\$2.46 per GB	53%
50,000 GB per day	\$117,990 per day	\$2.36 per GB	55%

5-10 people to manage and monitor the system

Source: <https://azure.microsoft.com/en-us/pricing/details/microsoft-sentinel/>

Centralized SIEM Platform and Pricing



SIEM Cost Summary

SIEM software	\$20,000 – \$1 million
Implementation	\$50,000
Training	\$0 – \$10,000
Resources	\$74,000 – \$500,000
Hardware	\$25,000 – \$75,000
Infrastructure	\$10,000

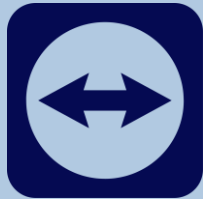
Source: <https://www.buchanan.com/managed-siem-pricing/>

Pricing Information

Threat intelligence pricing is often a subscription to multiple data feeds, with tiered pricing based on number of users. Data fees vary in cost from about \$1,500 and \$10,000 depending on the number of feeds.

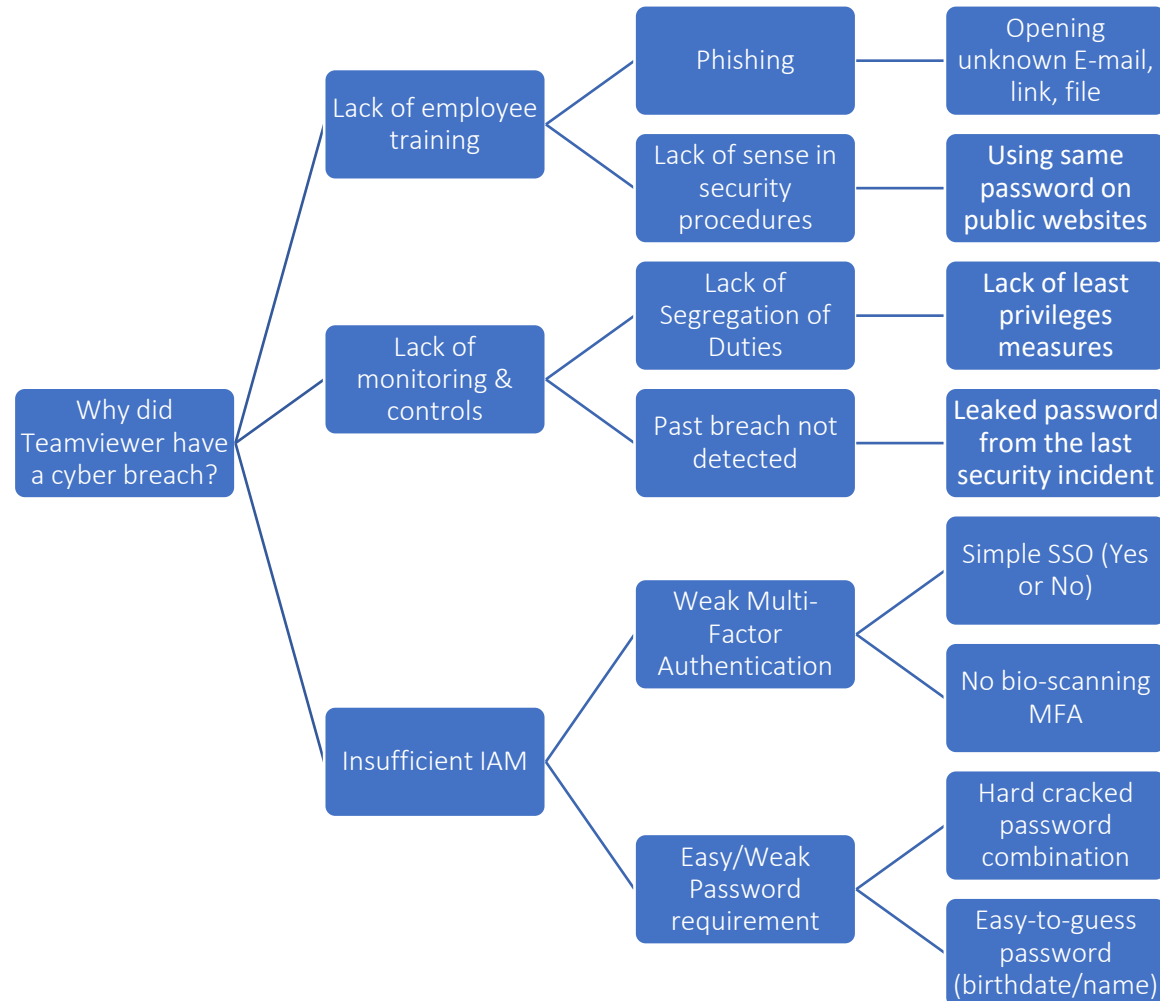
Source: <https://www.trustradius.com/threat-intelligence#:~:text=Threat%20intelligence%20pricing%20is%20often,o n%20the%20number%20of%20feeds.>

Extended Risks and Mitigations



Risk	Degree	Mitigation Strategy
High Costs and Resource Demands of Cryptographic Infrastructure		<ul style="list-style-type: none">Conduct a cost-benefit analysis to validate ongoing investment in MFA infrastructure. Prioritize high-risk accounts for cryptographic authentication, while utilizing lower-cost MFA options for less critical accounts
Increased System Complexity from Web Filtering and DNS Security		<ul style="list-style-type: none">Pilot the web filtering solution in a test environment to identify potential application conflicts. Implement a process for quickly whitelisting business-critical sites, and regularly review blocked content to ensure business needs are not hindered
False Positives in Behavioral Anomaly Detection		<ul style="list-style-type: none">Fine-tune UEBA thresholds and establish a feedback loop with security teams to refine detection criteria. Consider using machine learning algorithms that adapt and reduce false positives over time, increasing the accuracy of threat detection

Considerations and Issue Tree



Sources Used



- Midnight Blizzard. (2024). Midnight Blizzard escalates spear-phishing attacks. Link: [Midnight Blizzard Escalates Spear-Phishing Attacks](#)
- SolarWinds. (2024). What is Remote Desktop Protocol (RDP)? Austin, TX: SolarWinds. Link: [What Is Remote Desktop Protocol \(RDP\)? - IT Glossary | SolarWinds](#)
- SOCRadar® Cyber Intelligence Inc. (2023). APT profile: Cozy Bear / APT29. Ankara, Turkey: SOCRadar®. Link: [APT Profile: Cozy Bear / APT29 - SOCRadar® Cyber Intelligence Inc.](#)
- MITRE ATT&CK®. (2017). APT29, IRON RITUAL, IRON HEMLOCK, NobleBaron, Dark Halo, NOBELIUM, UNC2452, YTTRIUM, The Dukes, Cozy Bear, CozyDuke, SolarStorm, Blue Kitsune, UNC3524, Midnight Blizzard, Group G0016. McLean, VA: MITRE Corporation. Link: [APT29, IRON RITUAL, IRON HEMLOCK, NobleBaron, Dark Halo, NOBELIUM, UNC2452, YTTRIUM, The Dukes, Cozy Bear, CozyDuke, SolarStorm, Blue Kitsune, UNC3524, Midnight Blizzard, Group G0016 | MITRE ATT&CK®](#)
- FIDO Alliance. (2024). FIDO2. Mountain View, CA: FIDO Alliance. Link: [FIDO2 - FIDO Alliance](#)
- Microsoft. (2024). Microsoft Entra passwordless sign-in - Microsoft Entra ID. Redmond, WA: Microsoft Corporation. Link: [Microsoft Entra passwordless sign-in - Microsoft Entra ID | Microsoft Learn](#)

Sources Used (Extended)



- SANS Institute. (2024). *Security awareness training*. Bethesda, MD: SANS Institute. Link: [https://www.sans.org/security-awareness-training/SANS Institute](https://www.sans.org/security-awareness-training/SANS%20Institute)
- MITRE. (2019). *User training, mitigation M1017 - Enterprise*. Bedford, MA: MITRE Corporation. Link: <https://attack.mitre.org/mitigations/M1017/>
- MITRE. (2022). *Multi-factor authentication request generation, technique T1621 - Enterprise*. Bedford, MA: MITRE Corporation. Link: <https://attack.mitre.org/techniques/T1621/>
- MITRE. (2017). *Multi-factor authentication interception, technique T1111 - Enterprise*. Bedford, MA: MITRE Corporation. Link: <https://attack.mitre.org/techniques/T1111/>
- MITRE. (2020). *Phishing: Spearphishing attachment, sub-technique T1566.001 - Enterprise*. Bedford, MA: MITRE Corporation. Link: <https://attack.mitre.org/techniques/T1566/001/>
- *Cost of Capital*. (2024). Link: [https://pages.stern.nyu.edu/~adamodar/New Home Page/datafile/wacc.html](https://pages.stern.nyu.edu/~adamodar/New_Home_Page/datafile/wacc.html)