SECURELY YOURS LLC

5 REASONS WHY YOU NEED
ADVANCED M365 DETECTION & RESPONSE

1 BEST-in-CLASS DETECTION

The platform is built for Microsoft 365, Exchange, Entra, Teams, SharePoint, and six additional Microsoft sources. This focused approach allows our solution to run hundreds of Microsoft-only detections correlated across Microsoft apps. That depth allows you to block attacks when they happen, even before the attack is reported by Microsoft. Securely Yours uses the information from Petra to better monitor Microsoft solutions and block attacks.

2 INCREASED ATTACKS on MICROSOFT SOLUTIONS

The success rate on M365 attacks has jumped from 5% to 50% in the past year. What changed? Attackers have figured out a way around MFA and use fake Microsoft portals and malware in browsers to steal session token and gain access. These attacks are external and are not detected by the installed EDR tool. Securely Yours uses Petra to identify and block these attacks and at the same time reduce the number of False-Positives.

3 BEYOND IMPOSSIBLE TRAVEL

With Petra, Securely Yours can trace user activities across Entra ID, Outlook, SharePoint, Teams, and more. What Microsoft P2 misses, Petra will catch and report.
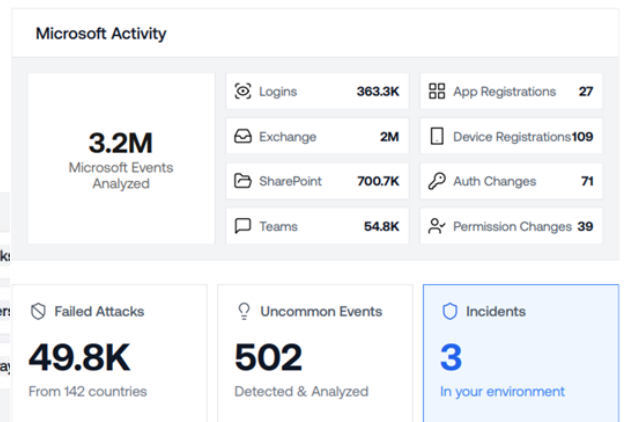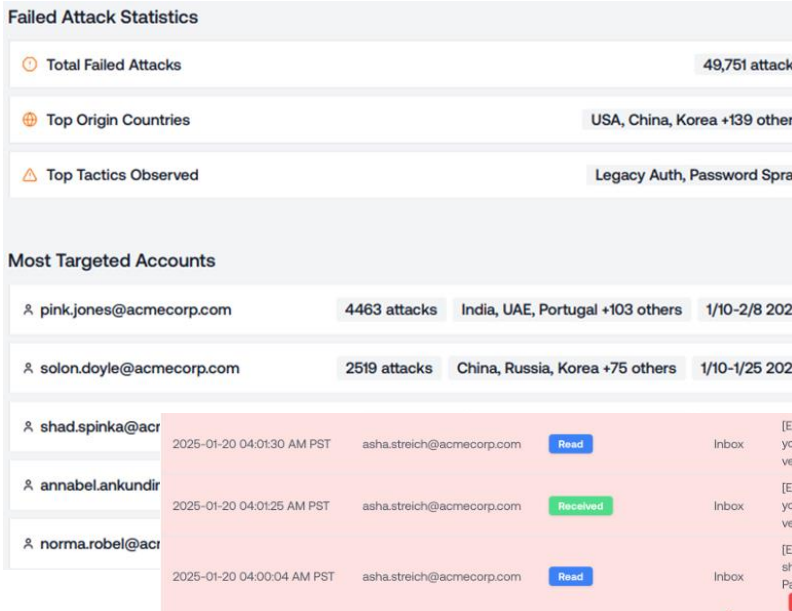
Our solution looks across logins and activities such as which email a user is reading/sending, which SharePoint docs are accessed, what Teams messages the user is reacting to, is the user using a VPN, etc. It provides details beyond the email header to easily facilitate forensic activities.

4 FAST DEPLOYMENT TO FASTER RESPONSE

Our process is a 1-click onboarding process and detection starts in less than 1 minute. Logs are processed in real-time. In no time, you are able to see ongoing attack campaigns in your environment: who's being targeted, what toolkits the attacker is using, and what city the attacker is coming from.

5 ADVANCED ANALYTICS

To provide fast and actionable results, our solution uses advanced fingerprinting to examine low information logs, columnar data store to manage data sets, and advanced machine learning models to sift through seemingly benign patterns, filter out noise, and find emerging threats.

Failed Attack Statistics

⏱ Total Failed Attacks		49,751 attacks
🌐 Top Origin Countries		USA, China, Korea +139 others
⚠ Top Tactics Observed		Legacy Auth, Password Spray

Most Targeted Accounts

👤 pink.jones@acmecorp.com	4463 attacks	India, UAE, Portugal +103 others	1/10-2/8 2025
👤 solon.doyle@acmecorp.com	2519 attacks	China, Russia, Korea +75 others	1/10-1/25 2025
👤 shad.spinka@ac			
👤 annabel.ankundir			
👤 norma.robel@acr			

2025-01-20 04:01:30 AM PST	asha.streich@acmecorp.com	Read	Inbox
2025-01-20 04:01:25 AM PST	asha.streich@acmecorp.com	Received	Inbox
2025-01-20 04:00:04 AM PST	asha.streich@acmecorp.com	Read	Inbox

[EXTERNAL] 12572822 is your Microsoft OneDrive verification code. **Phish**

[EXTERNAL] 12572822 is your Microsoft OneDrive verification code. **Phish**

[EXTERNAL] Brad Smith shared "ConEd LLC Due Pay Application" with you **Phish**

Microsoft Activity

3.2M Microsoft Events Analyzed			
◎ Logins	363.3K	🔲 App Registrations	27
✉ Exchange	2M	📱 Device Registrations	109
📁 SharePoint	700.7K	🔑 Auth Changes	71
💬 Teams	54.8K	👤 Permission Changes	39

🚫 Failed Attacks	💡 Uncommon Events	⭕ Incidents
49.8K From 142 countries	**502** Detected & Analyzed	**3** In your environment

ADVANCED M365 MONITORING
For
Microsoft 365, SharePoint, Exchange, Entra, and Teams

Powered By
Petra Security

SECURELY YOURS LLC