How to Find Your Very Attacked People and *Protect* Them

graylog

When you think of your most at-risk people, your mind probably jumps to the usual suspects: your CEO, CFO, or the head of IT. But here's the thing: attackers don't care about your org chart. They care about access. And they're getting more creative in finding the right people to target.

Enter the concept of VAPs: Very Attacked People or Very Attacked Persons. It's not about titles; it's about who's actually being attacked. Sure, your executives are likely targets. But what about that marketing director signing vendor contracts? Or the HR manager handling sensitive employee data? Or the facilities coordinator with building access control privileges? These people might not have "CISO" in their title, but they hold the keys to your kingdom, and attackers know it.

The 2025 Verizon Data Breach Investigations Report (DBIR) tells us that 74% of breaches involve the human element, including social engineering, phishing, and errors. The days of indiscriminate phishing blasts are over. Attackers are narrowing their sights on specific individuals. They're tailoring their tactics. And they're succeeding.

Why VAPs Matter More Than You Think

Let's be blunt: If you don't know who your VAPs are, you're already behind. Identifying and monitoring them isn't just helpful—it's critical. Here's why:

1. Attackers Are Getting More Precise

Spear-phishing attacks, where the attacker crafts a message for a specific person, are 60% more effective than generic phishing attempts. It's like a burglar knowing which window you leave unlocked.

2. Low-Level Alerts Can Hide High-Risk Threats

Not all alerts are created equal. A "low" alert tied to a VAP isn't low—it's a ticking time bomb. If an attacker targets your CFO, even a single phishing email deserves immediate attention. Without the context of who is being attacked, you're stuck reacting to alerts in a vacuum.

3. Your Risk Model Is Incomplete Without the Human Factor

Most risk scoring models are focused on endpoints, not people. They tell you if a device is vulnerable or if a system is outdated. But they don't tell you if the same person has been phished three times in a month or if their credentials have been leaked on the dark web.

And that's a problem because attackers aren't looking for your "crown jewels." They're looking for the people who can give them access.

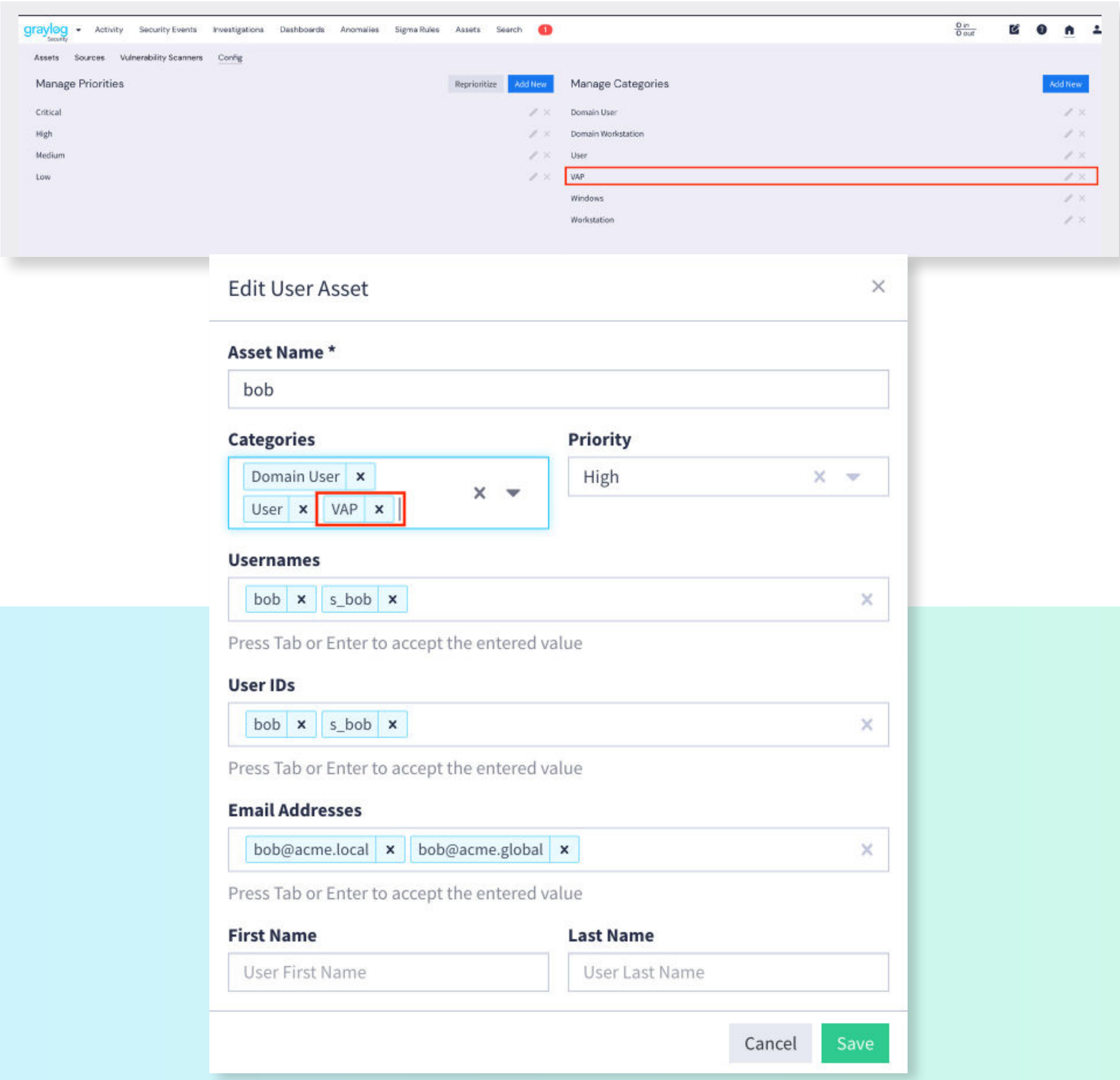
According to a recent Gartner report, 88% of boards see cybersecurity as a business risk, not just an IT issue. If cybersecurity is a business risk, then your people (the ones who can open doors to your business) need to be front and center in your security strategy.

How to Spot Your VAPs Without Guesswork

Let's get real: you can't protect what you can't see. Spotting your VAPs isn't about guesswork or gut feelings. It's about using your data—yes, the logs, the alerts, the threat intel and connecting the dots.

Here's what high-performing security teams are doing:

- **Correlate Attack Data Across Sources:** Don't rely on titles. Look at real attack patterns. Who's getting the phishing emails, the malware, the credential stuffing attempts? Are they clicking on those links? Are they getting flagged by your endpoint tools? You can configure a new category under the assets section and add the category "VAP". You can then manually assign the "VAP" category to any of the users listed in the assets section.



Manage Priorities

Critical
High
Medium
Low

Manage Categories

Domain User
Domain Workstation
User
VAP
Windows
Workstation

Edit User Asset

Asset Name *: bob

Categories: Domain User, User, VAP

Priority: High

Usernames: bob, s_bob

Press Tab or Enter to accept the entered value

User IDs: bob, s_bob

Press Tab or Enter to accept the entered value

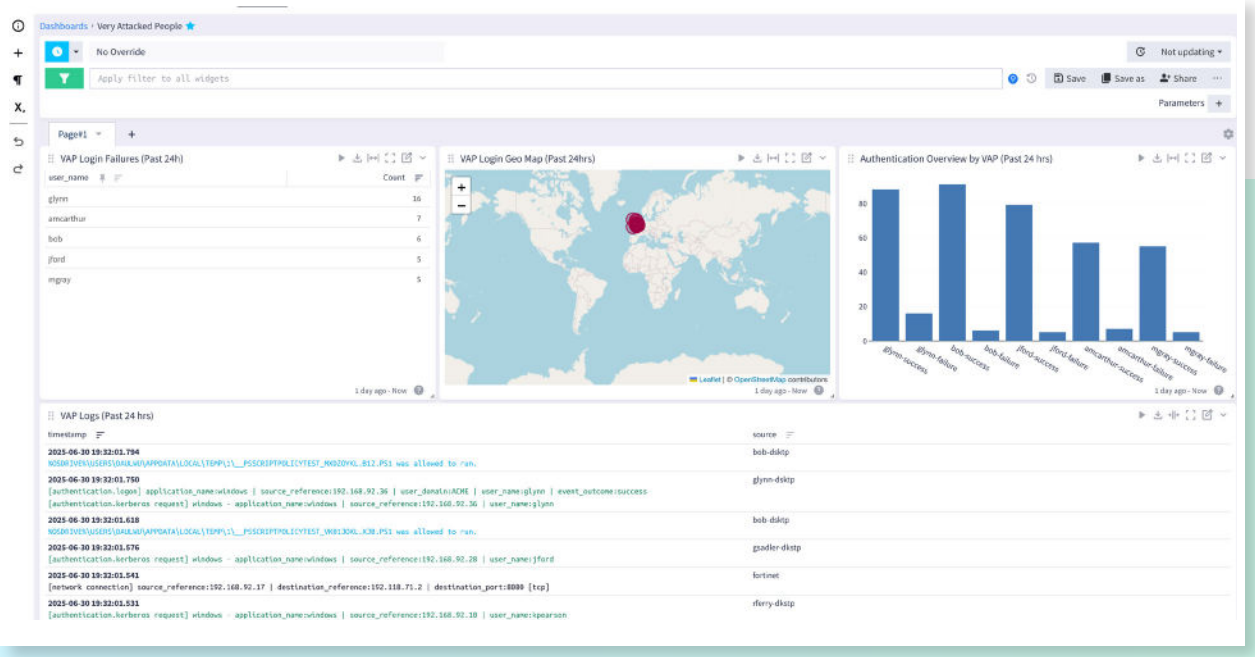
Email Addresses: bob@acme.local, bob@acme.global

Press Tab or Enter to accept the entered value

First Name: User First Name

Last Name: User Last Name

- **Build Dashboards That Focus on People, Not Just Endpoints:** Most dashboards show you endpoints, not humans. That's a gap. Build a view that shows attack activity by individuals, over time. Who's getting targeted? How often? What kinds of attacks? This visibility is essential to understanding your true risk.



VAP Login Failures (Past 24h)

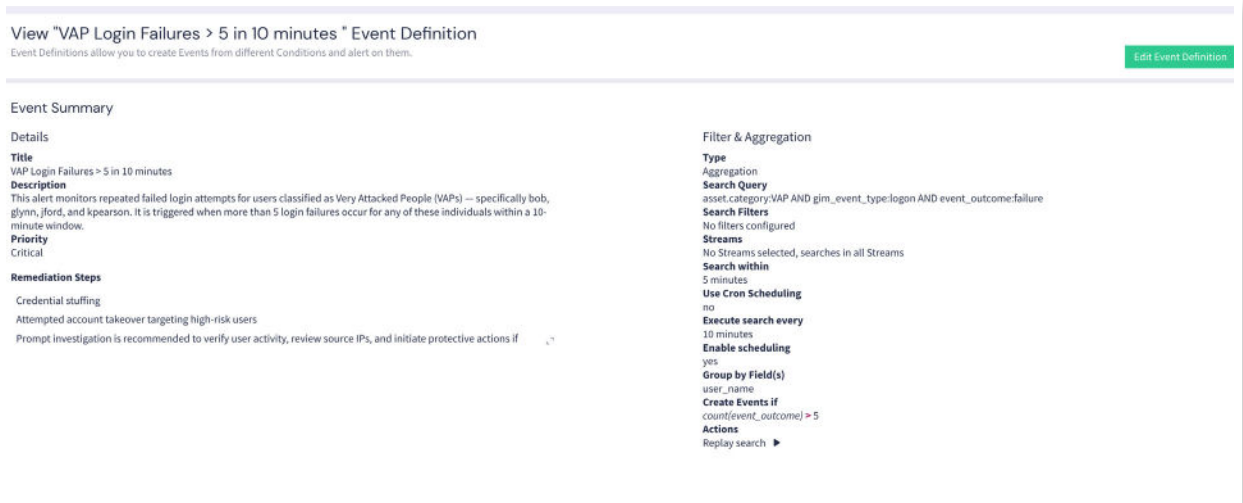
user_name	Count
glynn	16
amcarthur	7
bob	6
jford	5
mgray	5

1 day ago - Now

VAP Logs (Past 24 hrs)

```
timestamp                                                                                                   source
2025-06-30 19:32:01.794                                                                                     bob-dsktp
NOSDRIVES\USERS\DAULWU\APPDATA\LOCAL\TEMP\1\__PSSCRIPTPOLICYTEST_MXDZOYKL.B12.PS1 was allowed to run.
2025-06-30 19:32:01.750                                                                                     glynn-dsktp
[authentication.logon] application_name:windows | source_reference:192.168.92.36 | user_domain:ACME | user_name:glynn | event_outcome:success
[authentication.kerberos request] windows - application_name:windows | source_reference:192.168.92.36 | user_name:glynn
2025-06-30 19:32:01.618                                                                                     bob-dsktp
NOSDRIVES\USERS\DAULWU\APPDATA\LOCAL\TEMP\1\__PSSCRIPTPOLICYTEST_VK813OKL.X38.PS1 was allowed to run.
2025-06-30 19:32:01.576                                                                                     gsadler-dkstp
[authentication.kerberos request] windows - application_name:windows | source_reference:192.168.92.28 | user_name:jford
2025-06-30 19:32:01.541                                                                                     fortinet
[network connection] source_reference:192.168.92.17 | destination_reference:192.118.71.2 | destination_port:8080 [tcp]
2025-06-30 19:32:01.531                                                                                     rferry-dkstp
[authentication.kerberos request] windows - application_name:windows | source_reference:192.168.92.10 | user_name:kpearson
```

- **Tie Alert Priority to User Risk:** A login attempt from an unusual location might not matter for some employees, but for your CFO or your HR manager, that's a different story. Elevate alert priority based on the person's role and risk profile.



View "VAP Login Failures > 5 in 10 minutes " Event Definition

Event Definitions allow you to create Events from different Conditions and alert on them.

Event Summary

Details

Title
VAP Login Failures > 5 in 10 minutes
Description
This alert monitors repeated failed login attempts for users classified as Very Attacked People (VAPs) — specifically bob, glynn, jford, and kpearson. It is triggered when more than 5 login failures occur for any of these individuals within a 10-minute window.
Priority
Critical

Remediation Steps

Credential stuffing
Attempted account takeover targeting high-risk users
Prompt investigation is recommended to verify user activity, review source IPs, and initiate protective actions if

Filter & Aggregation

Type
Aggregation
Search Query
asset.category:VAP AND gim_event_type:logon AND event_outcome:failure
Search Filters
No filters configured
Streams
No Streams selected, searches in all Streams
Search within
5 minutes
Use Cron Scheduling
no
Execute search every
10 minutes
Enable scheduling
yes
Group by Field(s)
user_name
Create Events if
count(event_outcome) > 5
Actions
Replay search

Turning Data Into Action

At Graylog, we believe protecting your VAPs - your Very Attacked People and Very Attacked Persons - shouldn't be a manual, once-in-a-while checklist. It should be baked into your daily detection and response workflow. That's why we designed our platform to help you operationalize the concept of VAPs.

Here's how it works in practice:

- A phishing email targeting your CEO doesn't get lost in the noise. It's immediately flagged as a high-priority threat, whether it's one email or 100.
- Repeated login attempts on an HR admin's account? That's a red flag for a potential account takeover. Graylog helps you see that pattern before sensitive payroll data gets exposed.
- A VAP dashboard built into your SIEM gives you a people-first view of attacks. You're not just staring at logs; you're seeing risk in human terms.

Graylog ties together threat intelligence, anomaly detection, and asset data enrichment to give you a real-time, contextual view of your VAPs. No noise. No guesswork.

This isn't about adding more dashboards for the sake of it. It's about making your existing data work smarter so your team can respond faster and more effectively. It's about reducing alert fatigue by focusing on what matters most: the people who hold your business together.

Ready to Identify Your VAPs?

If you don't know who your VAPs are, you're flying blind. And in today's attack environment, that's not a risk you can afford to take.

The good news? It's not too late to get started.

Graylog can help you build a VAP-focused detection and response strategy that connects the dots between your data, your alerts, and your people. Let's talk about how to turn your attack data into a real defense plan, one that puts your people at the center.

Want to learn more? **Let's connect and make your data work smarter.**

©2025 Graylog, Inc. All rights reserved.