

**UC Tech Awards 2023 Candidate**

**Category:** IT SECURITY
**Name:** UCDH Privileged Access Management Project Team (53)
**Number of people:** (53)
**Location:** UC Davis Health

1. **Person submitting the application/nomination**
	1. Janet Vocaire-Tramposch, UCDH Staff
	2. **Email address: jtramposch@ucdavis.edu**
	3. **The name of your organization:** UCDH
2. **Award category** IT Security
3. **Name of person, name of the team, or name of the project to receive the award** UCDH Privileged Access Management Project Team
4. **All project team members - if applicable** (Name, title, department, location/organization, and please indicate if they are faculty or staff, along with their email address(s).

UCDH Staff (except those notes as consultants or contractors).

PAM Charter Stakeholders

Table Caption: This table shows the Stakeholder names, their title, their email, and their project responsibility.

|  |  |  |  |
| --- | --- | --- | --- |
| Member  | Role  | Email | Responsibility  |
| Scott Harrison | CTO UCD Health  | seharris@ucdavis.edu | Senior Advisor  |
| Nic Borton | CISO UCD Health  | nborton@ucdavis.edu | Senior Advisor  |
| Angelica Lewis  | Director Enterprise Applications  | aolewis@ucdavis.edy | Approval/Stakeholder  |
| Michael Perdue  | Director IT Customer Service  | meperdue@ucdavis.edu | Approval/Stakeholder  |
| Derek Lee | Director IT Infrastructure | nborton@ucdavis.edu | Stakeholder |
| Lee Smith   | UCDH IT Security Operations Manager  | lesmith@ucdavis.edu | Approval/Stakeholder  |
| Dawn Roarty  | Program Manager, Identity Management  | dmroaty@ucdavis.edu | IAM Leadership |
| Ilvana Mesic  | Campus IAM Director  | imesic@ucdavis.edu | Campus IAM Leadership (she has retired) |

PAM Working Group / Extended Project Team – diverse team that assists with decision making, option development, and change management. Also participates in the project work of adding their area of technology to the various solutions, as appropriate.

Table Caption: This table shows the working group supervisor, their title, the direct report who participated, their email, their project role, and project responsibility.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Supervisor | Title | Direct Report | Email | Project Role / Representing | Responsibility |
| Dawn Roarty dmroarty@ucdavis.edu | Program Manager, Identity Management  | Ezequiel Cothran  | ercothran@ucdavis.edu | IAM Team | SME  |
|  | Program Manager, Identity Management  | Patrick Garvey | pdgarvey@ucdavis.edu | IAM Supervisor | SME  |
| David Simmonsdmsimmons@ucdavis.edu | Manager Network Services | Praveen Kumar | prakumar@ucdavis.edu | Net Services Analyst | Network SME |
| Tejinder Singhtsingh@ucdavis.edu | DSG Supervisor | Kelly Nair | kenair@ucdavis.edu | Apps Ops Analyst | DSG SME |
| Marie Houstonkenair@ucdavis.edu | Supervisor, EMR Environment Management | Sal Cruz | scruzjr@ucdavis.edu | System Admin, Epic Environment | EMR SME |
| Greg Falcigfalce@ucdavis.edu | Manager, Voice Services | Antonio Guzman | tgguzman@ucdavis.edu | Voice Engineer | Voice SME |
| Dan Cottondgcotton@ucdavis.edu | Manager, Academic Info Systems | Hai Vu Nguyen | hvunguyen@ucdavis.edu | Supervisor, Academic Info Systems | AIS SME |
| John Harrisonjrharrison@ucdavis.edu | Supervisory, IOT Enterprise Imaging &PACS | Eloy Navarro | efnavarro@ucdavis.edu | IT Applications Ops | Apps SME |
| Mangesh Kamblemdkamble@ucdavis.edu | IT Architect | no delegate |  |   |   |
| Monica Moldovanmmoldovan@ucdavis.edu | Director, Revenue Integrity & HIM Enterprise Services | Joshua Simon | jasimon@ucdavis.edu | Info Systems Manager | HIM SME |
| Kent Andersonkander@ucdavis.edu | Research | Jeff Trunelle | jbtrunnelle@ucdavis.edu | Developer, Research Infrastructure | Research SME |

PAM Team – ongoing project work team

Table Caption: This table shows the project team supervisor/email, their title, the direct report who participated, their email, their project role, and project responsibility

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Supervisor | Title | Direct Report | Email | Responsibility |
| Dawn Roarty dmroarty@ucdavis.edu | Program Manager, Identity Management  | Ezequiel Cothran  | ercothran@ucdavis.edu | IAM Team |
| Lee Smithlesmith@udavis.edu | Supervisor, IT Security | Jesse Barber  | jpbarber@ucdavis.edy | PAM Lead Administrator; tech lead for the project |
|  |  | Leigh Broadfoot (contractor)  | lbroadfoot@ucdavis.edu | IT Security, Business Analyst |
|  |  | Kit Chung  | khchung@ucdavis.edu | IT Security Analyst |
|  |  | Jan TramposchLisa Deyo (IT Program)Mike Patel (contractor)Curtis Rodocker | jtramposch@ucdavis.edulcdeyo@ucdavis.edumpatel@ucdavis.educmrodocker@ucdavis.edu | IT Security PM |
| Kevin Talbotkctalbot@ucdavis.edu | Enterprise Architecture | Kevin Bickerton  | kbickerton@ucdavis.edu | Enterprise Architect |
| Sang Hoongschoong@ucdavis.edu | Supervisor, Enterprise Compute | Manish Mehta  | mamehta@ucdavis.edu | Unified Compute Analyst, AD |
|  |  | Bracia Hall | bhall@ucdavis.edu | Unified Compute Sys Admin, Unix/Linux |
|  |  | Akinola Adedoyin | aadedoyin@ucdavis.edu | Unified Compute Sys Admin, Unix/Linus |
|   |   | David Fidel | dkfidel@ucdavis.edu  | Unified Compute, Sys Admin Windows Server |
| David Simmonsdmsimmons@ucdavis.edu | Manager Network Services | Praveen Kumar | prakumar@ucdavis.edu | UCDH Enterprise Network Analyst |
| Farshad Maserratfmaserrat@ucdavis.edu | Database Systems Manager | Manuel Ventura | mventura@ucdavis.edu | SQL Database Administrator |
| Shesh Ananthulaskananthula@ucdavis.edu | Director, Client Services | Mark Devine | skananthula@ucdavis.edu | Client Engineering Supervisor |
|  |  | Johnny Lee Prayer | jpreyer@ucdavis.edu | InfoSys Manager, Field Services |
|  |  | Clayton Martin | clmartin@ucdavis.edu | Lead Analyst, Windows Desktop |
|  |  | Shawn Mayhew | sdmayhew@ucdavis.edu | Lead Analyst, Windows Desktop |
| Mike Perduemeperdue@ucdavis.edu | Director, IT Customer Svc and Access | Jeremy Chadwick | jkchadwick@ucdavis.edu | Manager, Access |
|  |  | Tim Lammi | tflammi@ucdavis.edu | InfoSys Manager, Service Des |
|  |  | Joseph Love | jalove@ucdavis.edu | InfoSys Manager, Service Desk |
|  |  | Justin Parker | juparker@ucdavis.edu | InfoSys Manager, Service Desk |
|  |  | Service Desk Personnel |  | Answering TOC calls and helping to get customer issues solved quickly |

Vendor and Consultants

Table Caption: This table shows the consultant name and title, the Firm they work for, and their email.

|  |  |  |
| --- | --- | --- |
| ***Consultant*** | ***Firm*** | ***Email*** |
|  Gabe Underwood , Architect and Training | BeyondTrust | gunderwood@beyondtrust.com |
|  Chris Boudreau, Client Manager | BeyondTrust | cboudreau@beyondtrust.com |
|  Tasha Clowater, TAM | BeyondTrust | tclowater@beyondtrust.com |
|  David Hartman, Sr Architect | Integral Partners | dhartman@ipllc.co |
|  Ahmad Alkurdy, Architect | Integral Partners | aalkurdy@ipllc.co |
|  Justin Glasscock, Senior Admin | Integral Partners | aalkurdy@ipllc.co |
|  Jens Hansen, Architect PMW | Integral Partners | aalkurdy@ipllc.co |
|  Brent Andrewsen, Manager | Integral Partners | bandrewsen@ipllc.co |
| Jason Ellis, Manager, Advisory | Integral Partners | bandrewsen@ipllc.co |
|  David Morimanno, Sr Architect, Advisory | Integral Partners | dmorimanno@ipllc.co |

1. **Which location was affected by the work?** (The name(s) of the organization affected)

All UCDH computing environments with these tools installed are better protected from cyber criminals (external or internal) when this work is done.

1. **Summary** The UCDH Privileged Access Management initiative selected and is installing BeyondTrust Privileged Access Management tools at UCDH over a 3-year time horizon. These tools help UCDH to manage, control, and audit privileged access credential use and provide for privilege elevation and de-elevation within UCDH computing assets, and by our key vendors. By improving our ability not only to protect privileged accounts but also manage, rotate, and centrally control, and limit the use of “admin privileges” to those who truly need them we protect the overall mission of UCDH by helping to ensure Confidentiality, Integrity, and Accessibility of UCDH technical assets.
2. **Narrative**

**A. Description of the initiative(s) or portfolio of work that support the nomination based on the award description.**

The UCDH Privileged Access Management initiative selected and is installing BeyondTrust Privileged Access Management tools at UCDH over a 3-year time horizon. Initial current state and gap analysis occurred in 2020. The work began in earnest in March 2021 and has continued steadily since that time. The team has remained on track, with only minor delays. Here is an overview of the roadmap that shows the three years of the project plan and the work to be done, and the status of that work.



Slide Caption: Here is an FAQ about PAM that explains what PAM is, why it is needed, how does it work, and who are privileged users.



Slide Caption: The below slide shows BeyondTrust products we selected and installed/are installing. The information included is why we selected BeyondTrust, what BeyondTrust modules did we buy, key functions of a PAM System, and other supporting functions of PAM systems.



***B. Impact and Mission Alignment:*** Privileged Access credentials are the sought-after credential for cyber criminals. A criminal who has gained control of a privileged access credential can potentially perform nefarious actions without detection, potentially bypassing our traditional security controls. By improving our ability not only to limit the use of and protect privileged accounts but also manage, rotate, and centrally control them we protect the overall mission of UCDH by helping to ensure Confidentiality, Integrity, and Accessibility of UCDH technical assets.

***B. Complexity:*** the scope of these BeyondTrust products touches every UCDH IT managed server and every UCDH managed PC.

For example…

B1. *Password Safe*: The product provides secure storage, daily rotation, monitoring and auditing of privileged credentials and their use. Implementing Password Safe required defining all the use cases, implementing them in Password Safe, and then onboarding each IT server (about 2200) and IT administration group one-by-one, using a “white glove” approach to ensure no business interruption. The servers onboarded included the AIX servers that support EPIC. The team developed a “repeatable” onboarding process, refined it over time, and used it to onboard all IT Administrators to Password Safe.

B2. *AD Bridge:* This product connects the Unix environment (about two hundred servers) to Active Directory, and therefore all the Unix Admin accounts consolidated and moved into AD and added to Password Safe. Unix admin accounts are “local” accounts, usually with the same name and password on each of several hundred servers. These passwords were rarely updated due to the time it would take – log into each server, update password. With AD Bridge, Password Safe can rotate those “local” admin accounts each night, and there is greater visibility into the admin activity on our critical Unix servers.

B3. *Endpoint Privilege Management:* Also called “Privilege Management for Windows.” This product allows tool administrator to classify end users and their PCs/Laptops (about 20k) into “low, medium, and high” flexibility policies. Administrators deploy an agent to each end user PC/laptop to enforce the policy for that user. When a user wants to perform an action that requires elevated privileges (today, users may have local admin privileges to accomplish this) the installed EPM agent checks the policy and if allowed enables the action. If not, the end user can call the Help Desk to obtain permission via a “code” from the help desk that the end user enters via a prompt on their PC. Tool administrators tune the policies over time, as the centralized policy manager can “listen” to end user activity on each PC, and tool administrators can tune the appropriate policies to better support end user activity. The bottom line is that end users who did not have Local Administration rights on their PCs can do more than before, and end users who did have Local Administration rights on their PC no longer need those broad administration rights. This closes a giant security issue.

B4. *Privilege Manager for Unix and Linux.* A similar solution to Privilege Manager for Windows is begin implemented for Unix.

Other solutions pending: Privileged Remote Access – will create an environment to better manage vendor remote access. DevOps Secret Safe – will improve the management of secrets in our AIS teams applications.

***C. How their success is measured/quantified.***

Leadership and the project team has measure success based on completing the scope of work on the PAM Roadmap pretty much as it was planned, and on budget. The consultants who have been assisting us have said that UCDH has a “model PAM Program.” It is all due to people from UCDH Senior Leaders to PAM Team, to Administrators, to Consultants and BeyondTrust who have invested in bringing these solutions to life!

***D. Timing.*** Completion of this work started March 2021 – present and is planned to conclude at the end of FY24.