Tuesday, March 3, 2020
11:00 a.m. – 11:20 a.m.
Why Just-in-Time (JIT) Privileged Access is the Next Big Step in Risk Reduction

Christopher Hills
Deputy Chief Technology Officer & Senior Solutions Architect
BeyondTrust

Abstract:
A true least-privilege security model requires users, processes, applications, and systems to have just enough rights and access—and for no longer than required—to perform a necessary action or task. While agencies are increasingly effective at applying the "just enough" piece using privileged access management (PAM) solutions, they have largely neglected the time-limited and persistent risk part of the equation.

Today, powerful accounts with always-on (24x7) privileged access proliferate across the DoD. The privileges of these accounts are always in an active mode—for both legitimate use and misuse. Just in Time (JIT) Administration is an approach in which agencies dynamically assign privileges to accounts and assets to ensure identities only have the appropriate privileges when necessary, and for the least time necessary. With JIT PAM, your admin privileges are no longer always ripe for abuse, so the threat window is drastically condensed.

For example, a typical always-on privileged account may be "privilege-active" 168 hours a week, versus just a couple dozen minutes using a JIT approach. Multiplying this effect across all your privileged accounts will have a truly massive impact on risk-reduction. Adopting JIT as part of your PAM approach means you can implement a true least-privilege model across your environment.

Attend this session to gain a firm understanding of how to:

- Significantly condense your agency's threat surface by shifting from an always-on privileged access model to a JIT approach

- Identify use cases where JIT PAM is an absolute necessity

- Choose and implement JIT PAM triggers, methodologies, and workflows that will immediately help you to drive down risk