



CYBER FUSION CENTER PRAGUE

VIDEO TRANSCRIPT

Opening

Hello and Welcome to the Accenture Cyber Fusion Centre Prague. Based in Prague, the capital of the Czech Republic, we have a custom built a secure facility to house the largest cybersecurity team in the region. The team is made up of a unique group of professionals, specializing in a range of fields to provide holistic expertise to our Clients. We use the latest techniques and knowledge, utilizing our multi-disciplinary team, to help our Clients transform to the Digital Age with confidence and resilience. We aim to be a real trusted partner to our global Clients with a strong base of industry experience and the expertise which is critical when facing the complex and fast paced changes of today's cybersecurity challenges. Our team is a diverse pool of security talent from all over the world, working together as one to be the delivery specialists of today and the security leaders of tomorrow. Come with me to learn more about what we do every day....

Embedded Lab/Security Assessments

Our Security Assessments team helps our Client's to protect their most valuable assets by performing hundreds of vulnerability assessments, penetration tests, source code and configuration reviews every year. Ethical hacking is a science and an art using the latest tools and creative techniques to outsmart the hackers. Vulnerabilities discovered during assessments along with our remediation advice helps our clients to harden their environment against attacks and directly increases their business resilience.

Alongside our assessments team, we have a dedicated, highly specialized team who focus on embedded systems. This unique team works in our custom-built lab and automotive space where our engineers enable our clients to confidently take their products to market. Specializing in automotive testing, we also have a broad range of experience across diverse industries from homeware to telecom networks.

Privileged Access Management

Helping our clients to protect their assets allows us to safeguard their business operations and resilience. Our Privileged Access Management team takes care of the implementation, operations and service improvements such as advanced automation and integration. This enables our clients to transform the way they allow their assets to be accessed and used contributing to sustainable, risk aware operations

Strategy and Risk

Our strategy and risk experts help clients to define their security programs, identify their risks and map their threat landscapes. Building a culture of strong planning and robust controls is essential for organisations to have confidence in the resilience of their operations and know that even if the worst happens, the plan is there to remediate and get back to business.



Application Security

Our Application Security team focuses on putting security at the center of the software development lifecycle. We enable our clients to deploy their application assets safely and at speed while managing any business risks. We cover a wide portfolio of services spanning the whole software development life cycle from design and threat modelling up to the protection of the application in production.

Security Operations Center

Our Center provides 24x7 support for our client's Security Operations with a range of shared and dedicated analysts. We carry out dynamic monitoring across our client's networks, not just protecting IT but also the OT which enables businesses. Our aim is to enable our clients to detect, prevent and respond to the threats from the world around us. This allows them to focus on their core business with strength and purpose.

Threat Hunting and Incident Response

The Threat Hunting and Incident Response team provide an effective and timely response to efficiently counter any threats and lock out the adversary. Whilst Threat Hunting, the objective is to actively identify existing compromises and threats unknown to the client's security team, assist with remediation and harden the environment against future attacks. Incident Response capabilities are designed to establish the cause and full effect of any cybersecurity attacks, identifying the techniques used and minimizing the chance of repetition. In both approaches the outcomes are used to support our client's cyber response capabilities, improving their detection and response to threats against their business.

Closing shot

Thank you for joining us at the CFC Prague, hope to see you soon. Bye.

Copyright © 2021 Accenture
All rights reserved.
Accenture and its logo
are registered trademarks
of Accenture.