Booz | Allen | Hamilton®

ACALVIO

EMPLOYING A DECEPTION STRATEGY IN ZERO TRUST ENVIRONMENTS

THE ZERO TRUST IMPERATIVE

The federal government and critical infrastructure can no longer depend on conventional perimeter-based defenses to protect critical systems and data. Cyber threats are intensifying, and cloud, mobile, and remote-work capabilities are blurring traditional network boundaries. Organizations across government and industry must now embrace a new mindset: It's zero hour for "zero trust." This approach relentlessly questions the premise that users, devices, and network components deserve to be trusted just because they're in the network.

IMPLICATIONS FOR CYBER DEFENSE OPERATIONS

Zero trust is driven by core principles: assume a breach; never trust, always verify; and allow only least-privileged access based on contextual factors. A robust zero trust architecture (ZTA) can resist attacks, contain ransomware, and prevent data breaches. Zero trust also changes the security operations model. Zero trust enterprises incorporate historical security operations center (SOC) measures with identity and access management (IdAM), insider threat analytics, and application-specific data to surface new insights in cyber fusion centers.

DECEPTION TECHNOLOGIES' ROLE

To make the most of ZTA for cyber defense operations, you need a way to enable effective monitoring and proactive threat hunting in a zero trust environment. Deception technology can help by providing high-confidence alerting for malicious activity. That's why Booz Allen is partnering with Acalvio to deliver the only deception technology certified FEDRAMP Ready along with our trusted professional services. This technology is part of a sensor suite for cyber defense, and it's informed by offensive adversary tactics, techniques, and procedures (TTPs). What's more, this technology covertly detects threats that can't be found with traditional sensors like endpoint detection and response (EDR) and extended detection and response (XDR). For example, in a zero trust environment, identity stores are a primary attack surface where any compromise of identity can create significant risk. Acalvio's ShadowPlex, which includes identity-specific deceptions, can help detect attacks against identity stores, adding an additional layer of protective value to a zero trust deployment. Endpoints and any credentials they contain are also a persistent source of risk; when an adversary escalates privileges and/or modifies rules to move laterally into previously protected areas, Acalvio's ShadowPlex will trigger an alert. By seeding decoys, accounts, and tokens in a network, any enumeration to those machines or use of those accounts notifies an operations center that security has been compromised. Deception

technologies not only provide clear signals of activity that warrant investigation and action but also reduce data-processing costs and singular reliance on analytics for true/positive alerts.

DECEPTION & ZERO TRUST USE CASES

Zero trust environments are built on the principle of least privilege, reducing the available attack surface. This raises the bar for threat actors. As shown in the following use cases, combining zero trust principles with deception technologies brings to bear a powerful preventative architecture and proactive sensor strategy to secure your enterprise.

INSIDER THREATS

Insiders, and attackers with stolen credentials, can authenticate and gain access to sensitive data. Deception is ideally suited to target such insider threats. Deception uses breadcrumbs with fake credentials and baits with fake sensitive data to detect credential access, privilege escalation, data collection, and exfiltration tactics.

PROTECT IDENTITY STORES

Identity stores are a vital enabler of zero trust, and deception technologies can be a powerful component of a comprehensive defense strategy for protecting them. Specifically, the deployment of identity specific deceptions to detect identity store threats and the deployment of deceptive identity stores to divert/mislead attackers.

EARLY DETECTION OF WORKSTATION/ HOST COMPROMISE

Zero trust environments rely on the identification of users' identities to apply the principles of least privilege. It's common for attackers to target user workstations to gain access to identities through credential compromise. Securing workstations is critical, and deceptions deployed on user workstations provide early and acccurate detection.

LATERAL MOVEMENT

Zero trust limits lateral movement via micro segmentation. Breadcrumbs provide attackers with alternate deceptive paths within and across the micro-perimeters to attractive decoy data stores. Subsequent lateral movement, or simply enumeration, to the decoys is suspect and generates a high-fidelity alert.

DETECT, CONTAIN, & ENGAGE

Prebuilt decoys and decoys based on enterprise golden images loaded with fake data are instrumented to observe attacker actions. When deployed, the decoys collect detailed attacker TTPs, which can be used to improve analytics, patch targeted vulnerabilities, and block further attacks.

RAPID RESPONSE

Automation and orchestration is an essential pillar of zero trust, and one that deceptions are well suited to enable. After providing early and precise detection of a threat, they deliver automated response via mechanisms such as isolation/quarantine of a compromised host, blocking of IP addresses/URLs in network firewalls, and suspending malicious host processes.

THREAT HUNTING WITH PRECISION & SPEED

Threat hunting enables proactive identification, confirmation, and elimination of threats in zero trust environments. The right deceptions can enable threat hunting by equipping defenders with the ability to deploy targeted deceptions that support confirmation of latent/dormant threats during a threat hunting mission. Such deceptions should be complemented by analytic capabilities that enable confirmation of threat activity including threats leveraging advanced TTPs and in-memory exploits.

ABOUT BOOZ ALLEN & ACALVIO

Booz Allen leverages industry-leading ZTA assessments, strategy, and engineering support, advanced threat-hunting techniques, and operational monitoring services to protect federal and commercial enterprises. Acalvio's ShadowPlex product delivers a powerful set of deceptions—including decoys that represent hosts, applications, accounts—designed to uncover stealthy cyber threats. Contact us to learn more about how deploying deception technologies can improve your sensor strategy and enable operational monitoring in a zero trust environment.

FOR MORE INFORMATION

Garrettson Blight
National Cyber Solutions Director
Booz Allen Hamilton
Blight_Garrettson@bah.com

Chad Scrupps
SVP of Worldwide Sales & Channels
Acalvio
chad@acalvio.com