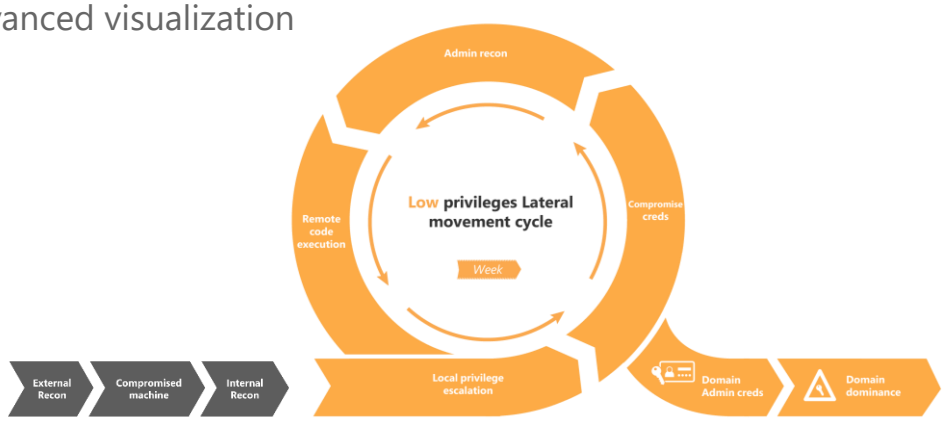
SIGNATURE CONSULTANCY

Cyber Resilience: Protect Identities

Reduce the impact of Identity Compromise and prevent Compromised Identity abuse.

Detect, prioritize and investigate advanced attacks and insider threats by combining behavioral and deterministic detection capabilities together with behavioral insights and advanced visualization



Detect Suspicious Activities

- Build organization behavioral profile
- Abnormal Resources Access
- Abnormal Authentication Requests
- Abnormal Modification of AD Sensitive Groups
- Abnormal Working Hours
- Pass the Hash

Basic Identity Protection (per User)

- **Define and Document** Administrative Privileges Policies, Processes, and Procedures
- **Define and Document** user Access Management Policies, Processes, and Procedures
- **Enforce** Identity protection across Organization(GPO)
- **Deploy and Configure** Microsoft Advanced Threat Analytics solution
- **Capture** & Analyze DC Network
- **Capture** & Analyze All Traffics related to DCs
- **Alerts** and thresholds setup and Configuration
- **Handover** and Operator Training

Premium Identity Protection (per User)

- **Basic Identity Protection**
- **Multi-Factor Authentication** solution design and implementation
- **Windows Hello** for Business solution design and deployment
- **Credential Guard** Solution design and deployment
- **Security** Compliance Toolkit

* Excluding Licenses. Minimum 500 Users Environment.

 | www.signatureconsultancy.com

Cyber Resilience: Protect Identities

How Does it work and What to Expect?

Planning & Design

- Design & Plan MFA Auth Provider
- Design & Plan MFA Federation
- Design & Plan Custom Apps Integration
- Design Hybrid Azure AD
- Design & Plan Windows Hello for Business
- Design & Plan Windows Credential Guard

Installation & Configuration

- Analyze Group Policy Against MS Security Baseline
- Edit and Apply Required Policy as per MS Security Baseline
- Create MFS Auth Provider
- Configure MFA Users & Device Settings
- Install & configure Hybrid Azure AD
- Configure Windows Hello for Business
- Configure Windows Credential Guard

Benefits

- 24/7 Monitoring
- Increased productivity with Next Actions Recommendation
- Continuous self adjusting and adapting
- Focus on what's important
- Comprehensive Alerts
- Detect Insider threats

Technologies Used in This Solution

- Windows Server 2016
- Windows Server 2016 Active Directory Services (AD)
- Azure Active Directory Services Premium
- Microsoft Advanced Threat Analytics
- Microsoft Security Compliance Toolkit

Enterprises successfully use UEBA to detect malicious and abusive behavior that otherwise went unnoticed by existing security monitoring systems, such as SIEM and DLP.

Gartner

 | www.signatureconsultancy.com

SIGNATURE CONSULTANCY

CRPI-int-v3