JOSEPH CARSON (CISSP)  
Chief Security Scientist | Thycotic

- 25+ Years Experience in Enterprise Security
- (ISC)² Information Security Leadership Award (ISLA®) Winner 2018
- Security Professional of the Year 2020 and Blogger Finalist
- Frequent speaker at Cyber Security events globally
- Adviser to several governments, critical infrastructure, finance and maritime industries
- Author of 4 books including Cybersecurity for dummies and Least Privilege for dummies
Data Applications Privileges
Traditional Perimeter

Build a fence around the data. This approach has fundamental flaws

• You can’t be 100% sure the fence is working
• Cloud and Mobile computing blurs the perimeter
• Over 60% of breaches fraud is conducted by stolen credentials
Add Layers and Layers?

1. Perimeter control
2. Trusted Insiders
3. Data in Secure vaults
4. Firewalls and Network
5. IDS and IPS
6. SIEM
Zero trust assumes any user or system that accesses the network, services, applications, data, or systems starts with zero trust. To gain authorized access, trust must be earned by the prospective user through verification.
Classifying Trust Dynamically

Adaptive Security
1. Secure Digital Identity
2. Multi-fA (Trust Level)
3. Secure Privileged Access
4. Secure Data Vaults
5. Check Reputation
6. Check Behavior
7. Check Risks
## Privileged Access Management Matrix

### Why, Who, Where, and How

<table>
<thead>
<tr>
<th>Why Are They Needed</th>
<th>Types of Privileged Accounts?</th>
<th>Who Uses Them?</th>
<th>How Are They Used?</th>
<th>How Are They Secured?</th>
<th>Risks If Compromised?</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Config changes</td>
<td>• Domain</td>
<td>• IT Admins</td>
<td>• Interactive Logons</td>
<td>• Passwords</td>
<td>• Malware</td>
</tr>
<tr>
<td>• Administrative Tasks</td>
<td>• Local Accounts</td>
<td>• Security Teams</td>
<td>• API’s</td>
<td>• 2FA</td>
<td>• Financial Fraud</td>
</tr>
<tr>
<td>• Create/Modify/delete users</td>
<td>• Root</td>
<td>• Helpdesk</td>
<td>• Services</td>
<td>• MFA</td>
<td>• Ransomware</td>
</tr>
<tr>
<td>• Install Software</td>
<td>• Privileged Users</td>
<td>• 3RD Party Contractors</td>
<td>• Applications</td>
<td>• Keys</td>
<td>• Compliance Failure</td>
</tr>
<tr>
<td>• Access Data</td>
<td>• Emergency Accounts</td>
<td>• Application Owners</td>
<td>• Automation</td>
<td>Access Workflows</td>
<td>Data Breach</td>
</tr>
<tr>
<td>• Backup Data</td>
<td>• System Admin</td>
<td>• DBA’s</td>
<td>• DevOps</td>
<td>Session Recording</td>
<td>Data Poisoning</td>
</tr>
<tr>
<td>• Update Patches</td>
<td>• Service Accounts</td>
<td>• Applications</td>
<td>• SSH</td>
<td>Launching</td>
<td>Insider Threat</td>
</tr>
<tr>
<td>• Interactively</td>
<td>• Applications</td>
<td>• O.S</td>
<td>• RDP</td>
<td>Behavior</td>
<td>Service/Application Downtime</td>
</tr>
<tr>
<td></td>
<td>• Batch Jobs</td>
<td>• Developers</td>
<td>• VPN</td>
<td></td>
<td>Revenue/Brand Loss</td>
</tr>
<tr>
<td></td>
<td>• Human/Non-Human</td>
<td></td>
<td>• Browsers</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Standard Accounts Access to Privileged Data</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### 1. Identity & Access Management
- **Privileged Access Management (PAM)** - Secure Usage of Privileged Accounts and Privileged Data
  - Privileged Accounts (Objects) - Secure Vaulting of Privileged Credentials
  - Privileged Data (Target) - Secure Access to Privileged Data
The PAM Lifecycle – 7 STEPS TO SUCCESS

1. Define Privileged Access
2. Automate Discovery of Privileges
3. Manage and Secure Privileged Access
4. Monitor Usage and Access
5. Alert on privilege abuse
6. Enable PAM for Incident Response
7. Continuous Review, Audit & Update
Privileged Access Security

- Privileged Account Discovery, Provisioning & Protection
- Endpoint Privilege Elevation & Application Control
- High Velocity Secrets Management for Applications & DevOps
TAKE THE PAM RISK ASSESSMENT – IN 5 MINS

MORE RESOURCES AT THYCOTIC.COM

• FREE EBOOKS
• Whitepapers & Case Studies
• Webinars and Blogs
• FREE TOOLS