www.Pueo.com 301 Lafayette Blvd, Fredericksburg, VA 22401 (P) 540.681.2122 (F) 202.869.3765

# PUEO

## Proactive Security Solutions to a Rapidly Evolving Landscape

*Pueo's approach to comprehensive security... "Reactionary security doesn't safeguard our nation, proactive solutions do."*

### Background and what we do…

Traditional physical security and cybersecurity vulnerability assessments can generate marginal improvements to a customer's overall security posture. However, as threats outpace resources, traditional solutions fall short. Pueo's approach integrates physical and cyber disciplines to capitalize upon the synergies and threat commonalities between the two, for cost effective risk assessments and vulnerability mitigations. Our analytic approach, grounded in deep research, applied to emerging cross-industry trends, renders defensible insight to supplement traditional assessment methodologies. Our techniques are designed and supported with both strategic and tactical experts to include numerous DoD-IC senior executives, senior NSA-certified Red Team leaders, and critical defense infrastructure and counterintelligence professionals. While the rapidly evolving security landscape invalidates traditional security methodologies, Pueo's integrated analytic approach delivers the vigilance our customers require.

**WHY PUEO?**

- Combined Physical and Cyber techniques for added value
- Renowned experts
- Defensible and insightful analytics
- Comprehensive and prescriptive mitigation plans

"In the new year, we expect to see more security and IT professionals joining together as the two functions continue to converge."
*Security Informed*

### Pueo's Integrated Approach

Pueo's combined physical and cyber approach accelerates and streamlines assessments, findings, and recommendations to quickly and efficiently bolster customer security postures.

Pueo provides the industry's most thorough vulnerability assessments through the utilization of both physical and cybersecurity assets, in tandem. Integrating the two further enables and facilitates each discipline in order to paint the most accurate overall security posture portrayal for our customers.

**Combined Physical + Cyber**

**Physical Security**

- Intrusion Detection Systems
- Access Control
- Surreptitious Entry
- Surveillance
- Human Exploitation
- Elicitation
- ID/Badge Replication
- CCTV
- TRASHINT
- RFID Signal Capture/Cloning
- Open Source Research

- Adversarial Based Penetration Testing
- Insider Threat
- Access Escalation
- Vulnerability Exploitation
- Cross-Discipline Facilitation
- System & Network Exploitation
- Critical Infrastructure
- Persistent Access
- Social Engineering
- Data and Information Fusion
- Comprehensive Security Solutions

**Cyber Security**

- Network Defense
- Ethical Hacking
- Phishing
- Data Analysis
- Access Control
- Network Compromise
- Data Exfiltration
- Create & Customize Network Exploitation Tools
- Escalation of Network Privileges

### Unrivaled Expertise

Pueo's strategic experts, including numerous DoD and IC senior executives, ensure each customer is subjected to only the most meaningful diagnostics and evaluation – without wasted efforts or frivolous noise. Our operational expertise is sustained by senior NSA-certified Red Team leaders and critical defense infrastructure and counterintelligence professionals, spanning numerous industries, domains, and functions with current Tactics, Techniques, and Procedures (TTP) proficiency for rapid evaluation and solution implementation. Pueo's statisticians, including a Johns Hopkins University professor, ensure both insight and appropriateness in our analytic forecasts.

Renowned expertise for strategic direction

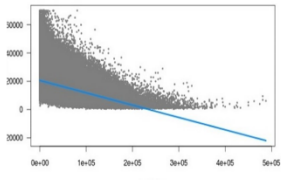
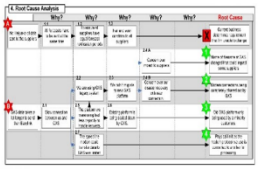
Operational proficiency across all domains and TTPs

Statisticians for unmatched analytical capacity

Pueo is a Service-Disabled Veteran-Owned Small Business and 8(a), HUBZone, and Indian Incentive Program Participant

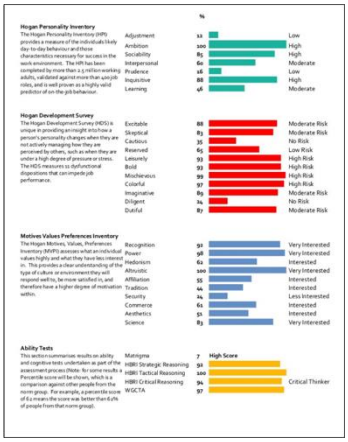
## Security Analytics

Using quantitative data related to successful and attempted penetrations, reviews of available and emerging technology, and historical and evolving adversary TTP, Pueo has developed multiple models to support our physical and cyber security assessments. Pueo uses its proprietary database and models to continually monitor changes in the cyber and physical security landscape to include new and emerging adversary TTPs, threats, and technologies to provide regular updates on your level of vulnerability, based on our last assessment.

| Statistical Forecasting | Analytic Solutioning | Threat Score |
|---|---|---|
|  |  |  |
| Pueo's forecasting models predict the adversary's likelihood of success. Advanced statistical techniques integrate both "known" and "observed" statistical characteristics for increased forecast confidence. | Analytic techniques (e.g. Root Cause) executed with customer collaboration, clearly describe and identify exploitable factors and associated parameters, that if addressed or remediated, will provide the highest level of protection. | Pueo translates qualitative and quantitative findings into a transferrable vulnerability score, utilizing its proprietary database and continuous monitoring models in both the cyber and physical security landscapes. |

## Prescriptive Solution Reporting

Through our proprietary report-generating solution, detailed findings documentation, emerging industry trends, and customer-specific remediations are summarized quickly and efficiently for users at all levels. Where traditional methodologies culminate in hypothesis-filled briefings, Pueo's proprietary methodology, ***PUEO SURE*** ™ (Security User Readiness Evaluation), is a groundbreaking approach that ensures customers possess the data and insight necessary for security transformation, mitigation, and preparedness throughout the organization. Pueo focuses on building customer expertise for vendor independence.

## Threat Scoring Matrices

Utilizing our unique multi-disciplined approach, thorough vulnerability exploitation, deep experience, and trends analysis, Pueo generates a FICO-like security health score providing defensible insight to customer security posture standing within their respective industry. Pueo accomplishes this while maintaining customer confidentiality at every level.

| Unhealthy | Healthy | Very Healthy | Industry Leader |
|---|---|---|---|
| • Inadequately prepared for most adversarial attacks<br>• Outdated physical and cyber security systems in place<br>• Security plans, policies & procedures need to be developed<br>• Security awareness training is needed throughout organization | • Somewhat prepared for adversarial attacks<br>• Physical & cyber security systems in place<br>• Security plans, policies & procedures are in place, but should be further developed<br>• Additional security awareness training throughout organization | • Adequately prepared for adversarial attacks<br>• Robust security systems in place<br>• Plans, policies & procedures developed & maintained by skilled professionals<br>• Security conscious employees<br>• Minor tweaks needed | • Very prepared for most adversarial attacks<br>• Robust physical & cyber security systems in place<br>• SME driven security policies & procedures<br>• Organizational leadership buy-in<br>• Overall security posture reflects proactive over reactionary measures |

### Prescriptive Mitigating Solutions

- Specifically tailored to customer threats and needs
- Industry leading research, data analysis & subject matter expertise driven
- Focused on improving your overall security posture
- Packaged solutions & enduring support to become an industry leader

### Open Source Research

- Tailored research of organizational threats
- Identify potential vulnerabilities
- Scan public facing Web pages & domains

### Recon & Surveillance

- Verify gaps & vulnerabilities for thorough exploitation
- Cover story & assessment road mapping

### Execution


- Social engineer specific applications & audiences
- Phishing attacks, file system exploitation
- Clone access badge RFID signals & access badge replication

### Privilege Escalation


- Proven adversarial-based TTPs
- Network access token & account manipulation
- Complex physical and network-based social engineering attacks
- Surreptitious Entry

### Persistence & Lateral Movement

- Repeatable & unfettered access to facilities & networks
- Exploit vulnerabilities in systems & personnel
- Further penetrate physical & cyber domains

### Facilitation & Enabling

- Implant controlled malicious devices
- Bypass multi-factor authentications
- Access to physical security systems
- Multi-discipline collaboration

### Exfiltration & Insider Threat


- Complex exfiltration of controlled data from physical & cyber domains
- Firmly established as trusted insider

### Access to Secure Areas

- Access to SCIFs, IT infrastructure & secured environments
- Obtain command level network privileges