

# Matthew Andreko

## Senior Security Consultant

Highly skilled and experienced cybersecurity professional with a decade of expertise in conducting red-team attack simulations, penetration testing, and custom development. Possesses a strong technical background combined with exceptional client management and communication skills. Proven ability to identify and exploit vulnerabilities, providing valuable insights to enhance organizational security posture. Excels in collaborating with cross-functional teams to deliver effective solutions that meet client needs. A trusted advisor known for consistently exceeding expectations and delivering results in complex and dynamic environments.

## Work History

### 2018-12 - **Senior Security Consultant**

**Current**

*TrustedSec*

Perform red-team attack against customer environments, simulating actual attacker tactics, techniques, and procedures. Create custom tools and frameworks to exploit new vulnerabilities or automate tasks for the team.

- Keep up to date on new techniques and attack methods, performing them on customer systems
- Collaborate and contribute to team software and utilities to increase productivity of team
- Manage customer expectations and communication
- Craft custom report deliverables to identify vulnerabilities and attack path

### 2015-06 - **Senior Red Team Consultant**

**2018-12**

*Accenture (Formerly FusionX)*

Perform red-team attack simulations against external customers networks

Maintain persistence on internal networks for goal-oriented results, providing value by identifying detailed attack chains that could be utilized by real attackers

- Complete in-depth research and development, establishing new approaches to ever-changing attack

## Contact

### Address

Lizton, IN 46149

### Phone

317-331-9089

### E-mail

matt@andreko.net

### LinkedIn

linkedin.com/in/mattandreko

### WWW

www.mattandreko.com

### WWW

github.com/mandreko

## Skills

Attack Simulation

Penetration Testing

Problem-Solving

Staff mentoring

Concise interpersonal communication

Custom Development

Vulnerability Assessment

IT Security

InfoSec

Self-Motivated

landscape

- Utilize new techniques to identify and exploit vulnerabilities in customer networks
- Develop custom command and control (C2) software and other tools to aid in team projects and prevent detection
- Create comprehensive and accurate reports and presentations for both technical and executive audiences.

**2012-09 -  
2015-06**

## **Security Consultant**

*Optiv (Formerly Accuvant LABS)*

Perform onsite and remote security consulting including penetration testing, vulnerability assessment, web application security assessment, internal and external security assessment, social engineering, and wireless assessment

- Generate and present technical and executive level reports on security vulnerabilities to external customers
- Develop custom tools for security testing and workflow management to aid and expedite projects and work of other consultants
- Provide tools and mediums to aid in communication between remote consultants.

**2011-07 -  
2012-09**

## **Senior Software Analyst**

*Leaf Software Solutions, Carmel, IN*

Develop web-based management software for automotive dealer services

- Refactor and clean large codebase to upgrade from .NET 2.0 to 4.0, utilizing LINQ, generating same functionality with fewer lines of code as well as being more easily readable
- Undertake research assignments for next generation of software
- Main topics include build/deployment, NoSQL database storage, and best-practice development patterns and standards
- Identify security weaknesses in current code-base
- Provide demonstration of how malicious actors could cause data loss or cause harm to company.

## **Languages**

---

C#, ASP.net

JavaScript (Node, jQuery, React, Angular, etc)

PowerShell

Python

C/C++

SQL (MySQL, Microsoft SQL Server, Postgresql, etc)

Go

PHP

## **Software**

---

Cobalt Strike

Metasploit

Burp Suite

Kali Linux

Git

Visual Studio

Microsoft Office

Ansible

2010-06 -  
2011-07

### **Software Developer III**

*Autobase/Dominion Dealer Solutions, Carmel, IN*

Develop web-based automotive CRM software to replace existing client-server software

- Participate in Agile SCRUM product lifecycle, utilizing extreme programming model, pairing developers to analyze business requirements given by analysts to implement solutions
- Established initiative to switch from SVN to Git, providing guidance and training to team
- Collaborate with outside vendors to understand and implement web-based solutions for scanning driver licenses and other cards from web-based interface, increasing speed of user experience

2007-04 -  
2010-05

### **Software Developer**

*Key Benefit Administrators, Indianapolis, IN*

Develop in-house applications based on specifications provided by team lead

- Work with several team members to provide stable and scalable services
- Provide custom reports on day-to-day basis
- Develop and maintain service that would distribute agent and vendor commissions based on complex set of rules, handling cash advances, and several other advanced features
- Responsible for running monthly, verifying data to finance department and creating custom reports from Microsoft SQL 2008 and Active Reports
- Manage SVN repositories, including advanced branching and merging scenarios to aid in development amongst multiple team members
- Train new team members and contractors to learn and use existing code-bases for various web applications.

1999-08 -  
2007-04

### **Software Developer / System Administrator**

*On-Ramp Indiana, Noblesville, IN*

Provide technical expertise for multitude of tasks, including developing custom software, customer support, and network engineering in team-oriented environment. Delivery of superior service to customers, fielding

diagnosing, troubleshooting, and resolving complex and/or unusual support calls.

- Instrumental in training new staff
- Configure and support Cisco network devices on complex network, providing segmentation from customer and company assets
- Established hardened Microsoft Windows server infrastructure in accord with baselines such as CIS benchmarks
- Develop several custom applications, integrating into various internal services such as Vircom Modusmail Server, WebTrends, Microsoft IIS, and Microsoft DNS Server to provide automation to previously manual tasks
- Reverse-engineered Vircom Modusmail to identify weakness in their webmail interface, allowing attacker to decode plain-text cookie values to hijack user sessions.

## Education

---

### **No Degree: Computer Technology; Minor Electrical Engineering**

*IUPUI - Indianapolis*

## Certifications

---

**2012-06**      Offensive Security Certified Professional (OSCP)

**2013-04**      Offensive Security Certified Expert (OSCE)