Artamis Karrys

Phoenix, AZ | artamiskarrys@gmail.com | artamiskarrys.com | github.com/akarrys

CORE SKILLS

Incident Response, Threat Hunting, IOC Development, Root Cause Analysis, MITRE ATT&CK Mapping

Microsoft Sentinel, Microsoft Defender XDR, Defender for Endpoint, Entra ID, Exchange Admin Center

PowerShell Analysis, LOLBins, WMI Persistence, Lateral Movement, Credential Abuse

Wireshark, DNS, DHCP, TCP/IP, Network Traffic Analysis

Windows, Linux, macOS, Active Directory, Group Policy

PowerShell, Java, SQL, JavaScript, C#, REST APIs, Git, Postman

ServiceNow, Jira, Datto RMM, Mimecast, Proofpoint, Meraki, UniFi

PROFESSIONAL EXPERIENCE

Phoenix Children's Hospital — IT Clinical Optimization Analyst I | Sep 2024 – Present

Support clinical and administrative staff in a regulated healthcare environment.

Partner with clinical teams to optimize EHR workflows and technical processes.

Create technical documentation and coordinate escalation of complex issues.

AccountabilIT — SOC Analyst I | May 2023 – Sep 2024

Investigated Microsoft Sentinel and Defender security alerts, including phishing, malware, and account compromise activity.

Analyzed PowerShell-based threats, WMI persistence, credential abuse, and lateral movement techniques.

Correlated endpoint, identity, email, and network telemetry to identify indicators of compromise.

Supported containment, remediation, threat hunting, and post-incident validation activities.

Mapped adversary behavior to MITRE ATT&CK techniques and documented investigative findings.

Troon Golf — IT Systems Technician | Jun 2022 – Mar 2023

Provided enterprise IT support for hardware, software, VOIP, and POS systems.

Managed Active Directory accounts, permissions, and access controls.

Supported network infrastructure utilizing UniFi and Meraki platforms.

PROJECTS

Cloudflare Security Hardening Project – Implemented CSP, HSTS, TLS 1.3, Cloudflare security controls, and improved Mozilla Observatory score from B+ (80) to A+ (110).

Malware Analysis Laboratory – Built isolated malware analysis environments and investigated persistence, process execution, and network activity.

EDUCATION

Arizona State University — Bachelor of Science, Applied Computing (Cybersecurity)