RANGEFORCE

Certificate of Continuing Education Completion

THIS CERTIFICATE IS AWARDED TO

Polina Sotnikova

For successfully completing 406 modules, equivalent to 304.5 hours study, provided by the RangeForce Platform

Extracting Strings From Running Processes,CVE-2019-3396 Confluence Unauthenticated RCE,CVE-2018-13382 FortiOS 6.0.4: SSL VPN Improper Authorization,CVE-2021-3156 Baron Samedit: Hands-on,Sublist3r,Nmap: Multiple Targets,Nmap: SSH Enumeration,Docker Dockerfile,Ensure the Security of IP Networks,Ensure the Security of IoT Edge Networks,Gobuster,CVE-2014-6271 Shellshock,CVE-2016-8655 Privilege Escalation: Kernel Exploit (Chocobo Root),Unrestricted File Upload: Find & Exploit (NodeJS),OWASP ZAP: Basics,Cookie Security: HttpOnly: Find & Exploit (PHP),Introduction to OSINT,Windows Event Logs: PowerShell Queries and Filters,TShark Basics,PowerShell Remoting,PowerShell Filtering and Formatting,AWS IAM: Intro,Wireshark Basics,PowerShell Objects and Data Piping,PowerShell Modules,Linux Advanced Logging,Ansible: Introduction to Playbooks,SAST: SonarQube Introduction,Introduction to Injection Attacks,Docker Introduction,Brute-force Defense,AWS Instance Metadata SSRF,AWS Instance Metadata SSRF,Antivirus Logging,NIST Cybersecurity Framework Overview,Web Hosting Basics (Apache),CVE-2014-0160 Heartbleed: Hands-on,Finding Common Web Vulnerabilities,Introduction to Hades Ransomware,Introduction to SSRF,Introduction to Ransomware Challenge,Introduction to Conti Ransomware,Netcat Introduction,Romance Scams,Regular Expressions in YARA,Elastic: Elastic Security Basics,Firewall Policies Rule Ordering: FortiOS,Introduction to BlackMatter Ransomware,Handover Procedures,Extortion Emails,Work Email Handling,Misinformation,CVE-2018-6789 Exim Buffer Overflow,CVE-2018-4939 Adobe ColdFusion RCE,CVE-2018-6789 Exim Buffer Overflow,CVE-2018-4939 Adobe ColdFusion RCE,Password Sharing,Protect Data at Rest,Manage Risks Related to IoT Device Operating Systems and Firmware,Ensuring Privacy,Microsoft Defender ATP,Identify the Need to Protect IoT Resources,Apply a Forensic Investigation (Part 2),Securely Collect and Analyze Electronic Evidence,Complying With State, Federal and National Legislation,Follow-up On the Results of an Investigation,The Importance of Risk Management,Integrating Documentation into Risk Management (Part 1),Request/Response Model,Map the IoT Attack Surface,Application Monitoring and Logging,Automated Testing,Static and Dynamic Code Analysis,Vulnerability Prevention Guidelines: Web,Vulnerability Prevention Guidelines: Mobile,Vulnerability Prevention Guidelines: IoT,Vulnerability Prevention Guidelines: Desktop,Identifying and Ranking Threats,Protect Data in Transit and at Rest,Secure Error Handling and Logging,Handle Vulnerabilities Due to Process Shortcomings,Azure Security Monitoring,Limiting Access,Common General Programming Errors,Ensure the Security of Mobile Networks,General Principles for Secure Design,Handle Vulnerabilities Due to Human Factors,Ensure the Security of Wireless Networks,Promoting Physical Security,Identify Security Requirements and Expectations,Managing Incident Response,Azure Security Management,Build in Security by Design,Identify Factors That Undermine Software Security,Cloud Security - Misconfigurations,Azure Security for the SOC,Application Maintenance,Security in SDLC,Information Security Governance,AWS Security Hub Overview,CVE-2017-6327 Symantec Messaging Gateway RCE: Overview,Microsoft 365 Security Overview,Web Attack Overview,CVE-2020-10189 Zoho ManageEngine RCE Overview,CVE-2020-10189 Zoho ManageEngine RCE Overview,CVE-2021-3156 Baron Samedit: Overview,Web Protocols Overview,Hybrid Cloud Overview,CVE-2020-5902 F5 BIG-IP Load Balancer Overview,CVE-2020-14882 Oracle WebLogic RCE: Overview,CVE-2014-0160 Heartbleed: Overview,CVE-2020-8515 DrayTek Pre-auth Root RCE Overview,Insecure Deserialization Overview,OWASP Zed Attack Proxy Overview,Office Macros Introduction,Introduction to Vulnerability Scanning,Scheduled Tasks Introduction,Rundll32 Introduction,Mshta Introduction,Access Token Manipulation Introduction,System Services: Service Execution Introduction,Process Injection (Process Hollowing) Introduction,Accessibility Features Introduction,Crisis Management: Introduction,Elastic: Introduction to Elastic Stack,Elastic: Introduction to Elastic Security,WMI Introduction,Introduction to PKI,Introduction to Vulnerability Management,DLL Search Order Hijacking Introduction,Introduction to Mobile Device Management,Elastic: Introduction to Fleet and Elastic Agent,Introduction to Log Management with the Systemd Journal,Introduction to Microsoft Defender,Cloud Access Security Broker Introduction,IAM - Creating Strong Passwords,Cloud Security - Access Control,IAM - Principle of Least Privilege,XML External Entities Overview,Broken Access Control Overview,Cisco SecureX Overview,Kubernetes Overview,Broken Access Control Overview,Phantom Overview,Java Secure Coding Overview,Cryptography Overview,QRadar Overview,Secure Coding Overview,SQL Injection: Overview,XSS Overview,Nmap: Overview,Cloud Security Overview,Security Testing,Cloud Security - Isolating Attacks,AWS Security Overview,Security Testing,Company Credit Cards,Cloud Security - Shared Responsibility,Anticipating Ransomcloud Attacks,Introduction to Cloud Ransomware,Introduction to DoppelPaymer Ransomware,Introduction to Egregor Ransomware,Cracking a Password Hash,Keys to Useful Threat Intelligence,Ransomware Kill Chain,Ransomware Prevention and Mitigation,Prepare for Forensic Investigation as a CSIRT,Contain and Mitigate Incidents (Part 2),Password Cracking 2,Contain and Mitigate Incidents (Part 1),Deploy an Incident Handling and Response Architecture (Part 3),Deploy an Incident Handling and Response Architecture (Part 2),Deploy an Incident Handling and Response Architecture (Part 1),Splunk: Basics,Hafnium TTP,Introduction to Fully Automated Analysis,RansomEXX Ransomware TTP

1/27/2023

Date

Taavi Must, CEO of RangeForce