414.217.1615
Milwaukee, WI
binary0010@gmail.com

William Racsek

Director, Threat Detection & Response

GitHub: C0den
LinkedIn: william-racsek

Key Security Competencies

- Strategic Leadership and Vision
- Security Operations Center Management
- Incident Detection, Management, and Response
- Security Architecture/Design
- Malware Analysis
- Vulnerability Management
- Digital Forensics
- Security System Administration

Education

Associates Degree Programming, *ITT Technical Institute* 2004
Candidate for Software Applications and Programming Completed 22 month of study before transferring to B.S. program
Bachelors Degree Computer Science, *ITT Technical Institute* 2006
Information Systems Security Honors: Alpha Beta Kappa, National Honors Society GPA: 3.8

Technical Experience

DIRECTOR / SECURITY OPERATIONS CENTER **MAY 2020 — Present**
Fannie Mae *Reston, VA*

- Provides leadership and coordination in the planning, development, implementation and operation of company-wide, integrated security systems, to include detective and preventative controls, network and endpoint based security tools and configurations.
- Responsible for maintaining and advancing all areas of the Security Operations Center (SOC); including Detection, Incident Response, Cyber Intelligence, Insider Threat and Cyber Incident Management; staff of 32.
- Ensure the SOC can deliver on core objectives while the company transitions away from physical data centers and moves services into the cloud; including Amazon Web Services (AWS), Google Cloud Platform (GCP), and various Software as a Service (SaaS) providers.
- Participates in Security and Privacy Emergency Response Leadership Team; provides input and subject matter expertise regarding internal and external organizational incidents/legal matters.
- Recommends, participates in the development of, and establishes company security policies and procedures; establishes and implements short- and long-range departmental goals, objectives, policies, and operating procedures; monitors and evaluates program effectiveness; effects changes required for improvements.
- Develops and manages annual budgets for the organization and performs periodic cost and productivity analyses; plans and develops strategies and programs for cost savings opportunities/increased capabilities.
- Serves as a principal point of collaboration, leadership, and expertise to both internal and external constituencies on professional and operational matters pertaining to the mission, goals, objectives, and scope of the program.
- Oversees all facets of the daily operations of the SOC, ensuring compliance with the Company, FHFA, state, and federal laws, policies, and regulations.

MANAGER / INCIDENT RESPONSE & THREAT HUNT **OCT 2016 — MAY 2020**
Fannie Mae *Reston, VA*

- Provides supervision of Incident Response and Threat Hunting personnel, which includes work allocation, training, promotion, enforcement of internal procedures and controls, and problem resolution; evaluates peak performance and makes recommendations for personnel actions; motivates employees to achieve peak productivity and performance; 8 direct reports.
- Responsible for the execution and delivery of the incident response services for internal business customers and coordination of response actions and plans as part of an integrated Cyber Team with Threat Intelligence, Detection, and Vulnerability Management partners.
- Served as technical lead on large and highly complex incident response engagements.
- Lead the malware analysis working group made up of key technical resources.
- Partner with peer cyber teams to modify existing capabilities based on changes to the threat landscape using both technical and non-technical measures.
- Acts as a technical lead for other team members; coaches, mentors, and trains junior employees.

SENIOR TEAM LEAD / INCIDENT RESPONSE — **MAR 2014 — SEP 2016**
Fannie Mae — *Reston, VA*

SENIOR TEAM LEAD / SECURITY OPERATIONS CENTER — **AUG 2013 — FEB 2014**
Rockwell Automation — *Milwaukee, WI*

SENIOR ANALYST / INCIDENT RESPONSE — **SEP 2012 — JUL 2013**
Rockwell Automation — *Milwaukee, WI*

- Integral part of the Computer Security Incident Response Team tasked with identifying, analyzing and remediating known vulnerabilities and exploits from Advanced Persistent Threats.
- Coordinates the identification, containment, eradication, and recovery of high/critical incidents.
- Provides second level monitoring and investigation of information security events generated by complex network, endpoint, and log analysis platforms.
- Detects and analyzes malware using static and dynamic analysis techniques with tools such as IDA, Ollydbg, Capturebat, LordPE, ChimpREC, Process Monitor, and Process Hacker.
- Performs forensic analysis of suspected or known compromised systems and servers using EnCase Enterprise, Volatility and custom Live Response tools.
- Managed workflow and updating of incident management and trouble ticket systems.
- Gives recommendations for better tuning and creation of signatures, rules, alerts, data parsers, and custom scripts.
- Monitors external information sources for situational awareness of the threat landscape.
- Utilized ticket tracking and wiki systems to document, log, and assist in the remediation of daily network security issues.
- Developed custom security tools to reduce incident response times and track tools, tactics and techniques of attackers.
- Acts as a technical lead for other team members; coaches, mentors, and trains junior employees.

DATA SECURITY ANALYST INCIDENT RESPONSE — **AUG 2010 — SEP 2012**
Bucyrus International Caterpillar Global Mining — *South Milwaukee, WI*

- Act as lead technical responder for Global Mining Computer Incident Response Team. Maintained 100% reporting and incident closure SLA requirements.
- Planned, implemented and managed global vulnerability management solution utilizing Tenable Security Center. This program helped to identify internal and external risks to the company through our desktop, server and network infrastructures. This program has also been key in driving Global Mining to meet Caterpillar SRT patching requirements.
- Administrator of endpoint security products including Safend external device control, Wave Systems full disk encryption, Iron Mountain client backup.
- Responsible for conducting infrastructure security assessments and evaluating mitigating controls and usefulness to the business.
- Suggested and implemented project and process improvement ideas that resulted in time and money savings to the company.
- Facilitate the creation and maintenance of policies, standards and procedures promoting the overall security of the company by using experience and industry best practices.
- Give guidance for infrastructure projects to ensure security is maintained. This helped to strengthen the organizations overall security posture.
- Lead several internal investigations where digital evidence gathering and analysis was needed using EnCase Enterprise and open source solutions such as dd, The Skeuth Kit and Autopsy
- Assisted with 3rd party penetration testing.
- Act as mentor to assist other team members, with this help other team members were more confident in their abilities and able to take on larger and more complex tasks and projects.

MORE EXPERIENCE AVAILABLE UPON REQUEST

Skills

Tools and Languages

- Splunk, Arcsight, RSA Envision, Netwitness for Logs
- Expert level experience with Windows Desktop/Server and Linux
- Fluent in static and dynamic binary analysis using tools such as Volatility, PEid, Ollydbg, IDA Pro, Cuckoo Sandbox and FireEye MAS
- High level of knowledge relating to endpoint security including full disk encryption, external media encryption, external device control, data backup/recovery, antivirus, endpoint detection and response (Crowdstrike/Carbon Black),and data loss protection
- Expert level knowledge of security tools such as Nessus/Security Center, Tanium, FireEye Appliances, ThreatConnect, Netwitness, Metasploit, Wireshark, Snort/Sourcefire/Firepower
- Programming experience in several scripting languages including Python, Ruby, Shell Scripting, LaTeX, and Visual Basic; used GIT and Subversion to share, deploy and collaborate on projects

Communication/Soft

- Lead with empathy and compassion
- Strong ability to listen carefully and understand security needs and concerns
- Strong writtern and verbal skills
- Team player
- Ability to adapt to changing environments and learn quickly
- Encourage diverse perspectives and value psychological safety