Benjamin Feld,
CISSP,
OSCP,
CEH

Denver, CO

Email: benwfeld@gmail.com

LinkedIn:
profile.benjaminfeld.com

SUMMARY

I am an experienced Security Engineer with over a decade of experience. I have a strong and broad technical background that includes computer networking, systems administration, cloud computing, software development, and DevOps / DevSecOps. I am well versed in many aspects of information systems security, including offensive security (red team), network / system defense (blue team), security automation, security tool development, threat hunting, and incident response. I hold a B.S. degree in Information and Network Technologies with a major in Systems Security and have over a decade of hands-on industry experience. I am an active CISSP and OSCP. I have also earned many additional industry certifications. I have a passion for security and enjoy putting my skills to use to advance business objectives.

CERTIFICATIONS

- **(ISC)² CISSP (Certified Information Systems Security Professional)**
- **Offensive Security Certified Professional (OSCP)**
- **EC-Council CEH (Certified Ethical Hacker)**
- **CompTIA Security+ ce**
- **Various inactive certifications**

EXPERIENCE

Senior Security Engineer (Detection & Response), Slack

Denver, CO — January 2019 - Present

Slack is where work happens. It's where the people you need, the information you share, and the tools you use come together to get things done. Slack aims to make your working life simpler, more pleasant, and more productive. As a Senior Security Engineer on the Security Customer Protection Team, I contribute to security detection and incident response capabilities primarily focused on detecting security threats to Slack users as well as protecting Slack from being used with malicious intent. This is a hybrid role that is responsible for engineering, analysis, threat hunting, IR, and tool development. This team was previously the Enterprise Security Operations Team, where I provided similar contributions, but with a scope that also included corporate security, such as endpoint detection and response and corporate SaaS security.

Responsibilities

- In my current role, I am primarily responsible for building tooling and automation to surface security threats targeting Slack customers or misusing Slack with malicious intent.
- My team was previously responsible for the security posture of our global corporate networks, all corporate endpoints, all enterprise SaaS tools, and customer-facing security matters (including platform misuse and abuse).
- Creating and tuning security event alerting by analyzing the available data and finding the signal within the noise. This includes identifying data and security coverage gaps and proposing solutions to enhance security and visibility within our environments and of our devices.
- Sourcing, designing, building, implementing, maintaining, and tuning security tooling necessary to support automated security detection within our defined areas of responsibility. We balance building our own tools with the deployment of existing tools (COTS and OSS) based on analysis of where effort is best expended.
- Investigating potential security events and performing incident response for actual security events.
- Collaborating with the wider security organization in addition to partner teams throughout the company to achieve a wholistic approach to security.

Benjamin Feld,
CISSP, OSCP, CEH

Denver, CO

Email: benwfeld@gmail.com

LinkedIn: profile.benjaminfeld.com

Accomplishments

- Built a hyper-scalable malware scanning service that scans all customer file uploads for malware using Go, Yara, Docker, Kubernetes, and AWS.
- Built a highly-scalable backend for osquery using Python, Flask, and AWS infrastructure.
- Designed and built the AWS account for the Enterprise Security Operations Team, including implementing an infrastructure-as-code pipeline to deploy our AWS infrastructure and security tooling and applications. This included VPC design and account architecture and then implementing these designs within code.
- Designed and built the Jenkins deployment for the Enterprise Security Operations Team using an Infrastructure as Code approach.
- Contributed to the roll-out of Splunk. This included data ingestion and normalization as well as Splunk specific configurations (e.g. installation and configuration of Splunk applications).
- Created sharabale Jupyter Notebooks using Python to assist during investigations and incident response, replacing haphazard SQL queries.
- Global rollout of DNS filtering technology to all corporate endpoints.

Senior Security Operations Engineer, Sony Interactive Entertainment (Sony PlayStation)

San Diego, California — April 2017 - December 2018

Recognized as a global leader in interactive and digital entertainment, Sony Interactive Entertainment (SIE) is responsible for the PlayStation brand and family of products. As a Senior Security Operations Engineer, I helped to support the security framework that is integrated into the PlayStation platform, including the PlayStation Network (PSN). I helped to create, improve, and leverage DevSecOps practices, processes, and tools to secure a hybrid, highly scaled, environment. My team also supports SIE corporate security initiatives and tooling.

Responsibilities

- Review and improve Hybrid Data Center / Cloud (AWS) based DevSecOps processes and tools.
- Collaborate with operations teams to build infrastructure and servers on AWS.
- Work closely with product and platform teams to engineer and implement cloud security controls with a focus on DevSecOps.
- Implement a tools driven and highly automated approach to deliver key security management processes by maximizing use of existing toolsets.
- Develop procedures to automate security tasks which seamlessly integrate into code builds and deployments.
- Assist and train team members in the use of cloud security tools and the resolution of security issues.
- Lead AWS Cloud DevSecOps engineering integrations with platforms such as Splunk ES, Evident.io, and CloudPassage, and Vault.
- Build security utilities and tools for internal use that enable the Security Engineering team to operate at high speed and wide scale.
- Evaluate security technologies for cloud environments in order to implement controls in the most streamlined and integrated manner.
- Deploy automated security solutions for cloud delivery processes.
- Deploy compliance solutions for large-scale cloud environments using container and microservice technologies.

Benjamin Feld,
CISSP, OSCP, CEH

Denver, CO

Email: benwfeld@gmail.com

LinkedIn: profile.benjaminfeld.com

Senior Security Engineer, ViaWest, Inc.
Centennial, Colorado — January 2014 - April 2017

ViaWest is a super-regional provider of colocation, managed hosting, and cloud solutions. As a Senior Security Engineer, I was responsible for designing, implementing, managing, maintaining, and growing ViaWest's corporate and customer-facing information security practice and product. I directly supported multiple HIPAA and PCI compliant environments.

Responsibilities

- Design and implement internal security protections and customer-facing security products.
- Design and implement security tools and controls, including logical access controls.
- Conduct vulnerability scanning, penetration testing, forensic investigations, and incident response.
- Responsible for enterprise and customer vulnerability management and critical vulnerability response.
- Handle security escalations from internal operations support, partner teams, customers, and vendors.
- Participate in alert monitoring, advanced troubleshooting, and break-fix situations.
- Support PCI and HIPAA compliant environments, including administration and participation in internal and external (formal) audit processes.
- Ongoing training and research to stay informed about existing and emerging security threats.

Accomplishments

- Assisted in design and implementation of compliant cloud platform, including continued improvement.
- Created abuse report processing procedures and architected automation to support 100+ reports per day.
- Created enterprise vulnerability management framework, including critical vulnerability response program.
- Assisted in creation and roll-out of formal Security Operations Center (SOC), including defining procedures.

Solutions Engineer II, ViaWest, Inc.
Denver-Metro, Colorado — June 2011 - January 2014

ViaWest is a super-regional provider of colocation, managed hosting, and cloud solutions. As a Solutions Engineer II, I worked in ViaWest's VTAC providing, top tier, customer facing support for all of ViaWest's products.

Responsibilities and Accomplishments

- Provided support and troubleshooting for ViaWest's multi-region network.
- Supported and monitored customer environments and services.
    - Managed bandwidth, firewalls, load balancers, and backups
    - Systems administration (Windows and Linux)
    - Site-to-site and Client-to-site VPNs
    - Carrier circuits / bandwidth
    - Cloud solutions (VMware)
    - Managed DNS hosting
- Interacted with partner groups within ViaWest

Benjamin Feld,
CISSP, OSCP, CEH

Denver, CO

Email: benwfeld@gmail.com

LinkedIn: profile.benjaminfeld.com

- Rolled out ViaWest's new managed backup solution
- Selected in first round of the rollout of new VTAC (from existing NOC)
- Provided support to the internal security team, which I would later join and help to grow.

Security Operator, GBprotect
Englewood, Colorado — December 2010 - June 2011

GBprotect is a comprehensive Managed Security Services Provider. As a Security Operator, I worked in GBprotect's SOC monitoring customer environments for security threats and responding to active threats in real time. Technologies included: Snort / Sourcefire, ArcSight, Nessus, CheckPoint, and Cisco.

Responsibilities and Accomplishments

- Monitored customer environments for security threats, via IDS/IPS event monitoring and analysis as well as firewall and OS log monitoring and analysis.
- Responded to active security threats including customer-specific escalation procedures and blocking threat sources via firewall and IPS technology.
- Ensured the availability of customer environments by working with customer technical contacts and service providers to resolve any unavailability issues.
- Identified false-positives and modified IDS/IPS signatures to minimize the number of false positives
- Continued training and research to stay informed about existing and emerging security threats.

EDUCATION

Westwood College
BS in Information Technology (Major in Information Systems Security)
Denver, Colorado — January 2009 – December 2011

I graduated from Westwood College, Summa Cum Laude (with highest honors), with a Bachelors of Science in Information and Network Technologies with a Major in Systems Security. I graduated in three years (in 2011) with a cumulative GPA of 3.81, while working full time. My major focused on advanced information technology, computer networking, and systems security skills. Curriculum included the study of computer hardware and software, computer operating systems, computer networking (CISCO Networking Academy curriculum), and network and systems security.

Honors and Awards

- Honor: Graduated Summa Cum Laude (with highest honors)
- Award: Multiple President's List Awards (Term GPA 4.0 or above)
- Award: Multiple Dean's List Awards
- Award: Multiple Perfect Attendance Awards

Benjamin Feld,

CISSP, OSCP, CEH

Denver, CO

Email: benwfeld@gmail.com

LinkedIn: profile.benjaminfeld.com

APPENDIX - SKILLS (TECHNOLOGIES, TOOLS, PROTOCOLS)

- **Software Development, Programming, and Scripting**
  - Python, Go (Golang), Bash Scripting
  - REST, gRPC, Protocol Buffers (Protobuf)
  - Familiarity with C, PHP, JavaScript, and other languages
- **Network and Systems Security**
  - Firewalls
    - Hardware (Cisco, Juniper, Fortigate, Checkpoint, Palo Alto)
    - Software (iptables, pf / pfSense)
    - Web Application Firewall (WAF) (Imperva, Akamai Kona, AlertLogic)
  - SSL / TLS, PKI, Certificates, and Encryption
  - IDS/IPS (Intrusion Detection / Prevention Systems)
  - Malware Detection & Analysis
    - Yara, Cuckoo, MISP, The Hive, Cortext, VirusTotal
  - Enterprise Anti-Malware (AV) & Endpoint Detection and Response (EDR)
    - Carbon Black, osquery, Tripwire Enterprise, TrendMicro, ESET
  - SIEM (Security Incident and Event Management)
    - Splunk, Elasticsearch, Logstash, and Kibana (ELK), LogRhythm
  - SOAR (Security Orchestration, Automation and Response)
  - FIM (File Integrity Monitoring)
  - Log Management (Aggregation and Correlation)
  - Vulnerability Management (identification and remediation)
  - Risk Assessment
  - OS Hardening and Patching
  - Policy and Procedure Creation, Modification, and Training
  - Secrets Management
  - Identity and Access Management (IAM)
  - Cloud Security, Corporate Security, Platform Abuse
  - Threat Intelligence
  - Security Automation and Tool Development
- **DevOps / DevSecOps / Automation / Monitoring & Visibility**
  - Amazon Web Services (AWS)
  - Continuous Integration / Continuous Deployment (CI/CD)
  - Chef, Ansible, Terraform, Troposphere, Packer
  - GitHub / Git, Docker, Kubernetes, Jenkins
  - Nagios, Check_MK, Nimbus, Prometheus, Grafana, Thanos
  - Honeycomb, Jager, OpenTracing
- **Operating Systems and Platforms**
  - Linux (Server and Desktop)
    - Administration and Hardening
    - RHEL, CentOS, Amazon Linux, Debian, Ubuntu, Arch
    - LAMP stack (Linux, Apache, MySQL, PHP/Python)
    - Bind (DNS), Nginx, HAProxy, Squid
    - Mail (Sendmail, Postfix, Amavis, Spamassassin, Dovecot)
  - Microsoft Windows (Server and Desktop)
    - Administration and Hardening
    - Active Directory and Group Policy
    - Windows Server 2003, 2008, 2012, 2016; XP, 7, 8, 10, 11
  - Mac OS X / macOS
  - VMware vSphere (ESXi, vCenter, vCloud, vCM, etc.)
  - Amazon Web Services (AWS)
- **Computer Networking**
  - Routing, Switching, Load Balancing
  - LAN, WAN, and WLAN technologies
  - Cisco, Juniper, Fortinet, Palo Alto Networks
  - ACL, ARP, DNS, IPv4, NAT, OSPF, STP, VLAN, VLSM, VPN, WiFi, Ethernet
  - Content Delivery Network (CDN) (Akamai, CloudFlare)
- **Compliance and Auditing**
  - HIPAA, PCI / PCI-DSS, ISO 27000 series