Benjamin Feld

Security+,
CISSP,
OSCP,
CEH

resume@benjaminfeld.com
www.benjaminfeld.com
linkedin.benjaminfeld.com

SUMMARY

I am an experienced Security Engineer with over 15 years 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

NOTABLE EXPERIENCE & PROJECTS

- Securing devices, applications, networks, authentication, processes, and more across on-prem and cloud environments. Including crafting and implementing security and hardening standards.
- Helping to build and scale security operations teams, including hiring, training and mentoring.
- Responded to innumerable real-world security incidents as a security and incident response subject matter expert (some high-profile incidents).
- Held both internal and product/customer-facing security roles.
- Breadth across Security Engineering, Security Analysis, Security Operations, and Security Automation / Development.
- Implemented Security Information and Event Management (SIEM) systems multiple times (ELK / OpenSearch, Splunk, Panther, LogRhythm, FortiSIEM, ArcSight, custom SQL / data warehouse).
- Implemented vulnerability detection / management automation multiple times.
- Created a large-scale ZTA device trust and authentication system (Go).
- Created massively scalable malware scanner API application (Go).
- Created enterprise-grade osquery back-end server application (Python).
- Created a custom enterprise device management system (based on Puppet).
- Built PCI & HIPAA-compliant cloud as a service product.

WORK EXPERIENCE

Staff Security Engineer, Aurora Innovation

Remote — August 2022 - Present

At Aurora, we believe that the benefits of self-driving technology will increase efficiency and mobility, while bringing a reliable driver supply and heightened safety to America's roads. As a Staff Security Engineer on the Enterprise Security Team, I contribute to securing our enterprise IT environment, which includes client endpoints (employee devices and systems), corporate SaaS products, internal infrastructure and networks, and identity and access management (IAM). The team is also responsible for company-wide security detection and incident response, including cloud and product-related issues.

Responsibilities

- Technical lead for enterprise client device security (employee laptops, development instances, mobile devices, etc.)
- Improving security detection and response capabilities.
- Develop and implement security tooling and practices.

Benjamin Feld

Security+,
CISSP,
OSCP,
CEH

resume@benjaminfeld.com
www.benjaminfeld.com
linkedin.benjaminfeld.com

- Participate in Security Operations and Security Incident Response on-call rotations.
- Mentor security and IT peers within my team and org.

Accomplishments

- I architected the client platform engineering (CPE) and enterprise client device security programs, including tooling selection, creation, and deployment; creation and automation of device provisioning and hardening standards; and detection and response capabilities and procedures.
    - Custom deployment of Puppet on EKS (kubernetes) with custom written ENC and node terminus.
- I architected and lead the development, deployment, and ongoing operations of a device trust system based on the zero trust model.
- Helped to scale the team from the ground up, through program and process creation, interviewing and hiring, and training and mentoring.

Senior Security Engineer, Slack

Denver, CO — January 2019 - August 2022

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 contributed 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 was 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

- 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 included 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 balanced building our own tools with the deployment of existing tools (COTS and OSS) based on analysis of where effort is best expended.
- Investigated potential security events and performing incident response for actual security events.
- Collaborated with the wider security organization in addition to partner teams throughout the company to achieve a wholistic approach to security.

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

Benjamin Feld

Security+,
CISSP,
OSCP,
CEH

resume@benjaminfeld.com
www.benjaminfeld.com
linkedin.benjaminfeld.com

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 supported 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.

Senior Security Engineer, ViaWest, Inc. (Flexential / Peak 10)

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.

Benjamin Feld

Security+,
CISSP,
OSCP,
CEH

resume@benjaminfeld.com
www.benjaminfeld.com
linkedin.benjaminfeld.com

- 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. (Flexential / Peak 10)

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.
- 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 (Nuspire)

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

Benjamin Feld

Security+,
CISSP,
OSCP,
CEH

resume@benjaminfeld.com
www.benjaminfeld.com
linkedin.benjaminfeld.com

- 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

Security+,
CISSP,
OSCP,
CEH

resume@benjaminfeld.com
www.benjaminfeld.com
linkedin.benjaminfeld.com

APPENDIX - SKILLS (TECHNOLOGIES, TOOLS, PROTOCOLS)

- **Software Development, Programming, and Scripting**
  - Python, Go (Golang), Bash Scripting
  - REST, gRPC, Protocol Buffers (Protobuf), JSON, YAML
  - Familiarity with C, PHP, Ruby, JavaScript, and other languages
- **Network and Systems Security**
  - Firewalls and Web Application Firewalls (WAF)
    - Hardware & Software (Cisco, Juniper, Fortigate, Checkpoint, Palo Alto, iptables, pf / pfSense, Imperva, Akamai Kona, AlertLogic)
  - SSL / TLS / mTLS, PKI, Certificates, and Encryption
  - IDS/IPS (Intrusion Detection / Prevention Systems)
  - Anti-Malware (AV) & Endpoint Detection and Response (EDR)
    - CrowdStrike Falcon, Carbon Black, osquery, FleetDM, Kolide, OSSEC, Yara, Cuckoo, MISP, The Hive, Cortext, VirusTotal
  - Mobile Device Management (MDM) and Configuration Management (CM)
    - Puppet, Chef, Ansible, Kandji, WorkspaceOne, Meraki, Foreman
  - SIEM (Security Incident and Event Management) & Log Management
    - Splunk, Panther, Elasticsearch, Logstash, and Kibana (ELK), OpenSearch, LogRhythm, ArcSight, SQL-based
  - SOAR (Security Orchestration, Automation, and Response)
  - FIM (File Integrity Monitoring)
  - Vulnerability Management (identification, remediation, automation)
  - Risk Assessment & Threat Modeling
  - OS Hardening and Patching
  - Policy and Procedure Creation, Modification, and Training
  - Secrets Management (Hashicorp Vault, AWS Secrets Manager)
  - Identity and Access Management (IAM) (Okta, AWS IAM, Duo, 1Password, LastPassword)
  - Threat Intelligence & Threat Hunting
  - Security Automation and Tool Development
- **DevOps / DevSecOps / Automation / Monitoring & Visibility**
  - Amazon Web Services (AWS)
  - Continuous Integration / Continuous Deployment (CI/CD)
  - Puppet, Chef, Ansible, Terraform, Spacelift, Troposphere, Packer
  - GitHub / Git, Docker, Kubernetes, Helm, Kustomize, Spinnaker, ArgoCD, Jenkins, Bazel, BuildKite, Harbor, Istio, Open Policy Agent, SPIFFE / SPIRE
  - Nagios, Check_MK, Nimbus, Prometheus, Grafana, Loki, Chronosphere, Thanos, Honeycomb, Jager, OpenTelemetry, OpenTracing
- **Operating Systems and Platforms**
  - Linux (Server and Desktop)
    - Administration and Hardening
    - Debian, Ubuntu, Amazon Linux, Arch, RHEL, CentOS
    - 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
  - Mac OS X / macOS
  - Virtualization
    - VMware vSphere (ESXi, vCenter, vCloud, vCM, etc.)
    - Proxmox Virtual Environment
- **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, Tailscale, Nebula
  - Content Delivery Network (CDN) (Akamai, CloudFlare)
- **Compliance and Auditing**
  - HIPAA / HITECH, PCI / PCI-DSS, SOC2, ISO 27000 series