version:2025.08.08/01

Victor Shulist **CEH CISSP**

vtshulist@gmail.com
(613) 227-1600

3934 Bouvier Rd
Bourget
Ontario, K0A 1E0
https://www.linkedin.com/in/victorshulist

Profile

Mr. Victor Shulist is a consultant with over 25 years of experience in the areas of information solution architecture, software engineering, automation, information security with experience in both public and private sectors.   He is proficient in software development to the support and integration of various security technologies for the Security Operations Center (SOC) at CGI which included auditing, compliance reporting, and the development of incident tracking software and the development of a customer facing service level web reporting portal.

Areas of expertise:

- Splunk Platform(Certified User, Certified Power User, and Certified Administrator)
- Splunk SIEM (Enterprise Security)
- ServiceNow & ServiceNow Security Operations
- Nexpose Vulnerability Scanner
- ArcSight custom flexagent development.
- HP ArcSight ESM/Logger/connector appliance, Transformation Hub
- Web Application Firewalls/Database Activity Monitoring (Imperva)
- Compliance, including PCI, SOX, MITS
- IT Security (Antivirus, RSA, Entrust PKI, ITIL management)
- Software Development (C, C++, C#, Java, Python, Perl, PHP, XML, SOAP, REST.XSLT/XPath)
- Automation (deployment, monitoring, reporting)
- Source control tools such as Git
- Networking protocols such as IP, TCP, UDP, SNMP, SMTP, POP and LDAP
- RDMS (mySQL, MS SQL, Oracle)
- Health Monitoring (SNMP)
- Windows & Linux/Unix System Administration, including Active Directory/Group Policy.
- Application Security
- Trellix (formerly McAfee) ePolicy Orchestrator.
- ELK (Elastic/Logstash/Kabana) stack.
- QRadar SIEM

Professional Experience

Shared Services Canada
05/2022 - present

My second contract with Shared Services Canada (SSC). The main focus of my role in this contract was to assist in the deployment and refresh of the cyber-security monitoring solutions for GCSI-NG. Main duties and goals included:

- Review Detailed Design documents from the various solos (network security, application security, etc) and provide feedback on approach and design.
- Assisted in the development of cyber-security lab environment testing, including installation and configuration of Trellix (formerly 'McAfee') ePolicy orchestrator.
- Assisted in rollout and documentation for Change Management for Splunk infrastructure (configuration changes to Splunk forwards, indexers and Search heads) for new SSC clients.
- Configuration of Splunk forwards for custom parsing of newly deployed applications.
- Designed Active Directory Group Policies for the automated deployment and configuration of Splunk monitoring agents.
- Designed, developed and deployed the security monitoring solutions using SolarWinds SCM agents using a variety of protocols including SNMP, WMI and Custom Power shell scripts).
- Proof of concept of deployment of MDE (Microsoft Defender for Endpoint) using MECM and documented the efficacy of solution in air gapped networks.
- Development of custom network packet capture solution/netflow generation and integration with Splunk SIEM (Enterprise Security app)
- Deployment of security control tools (Nexpose vulnerability scanner, ClamAV (Linux Antivirus), Health Monitoring (using Zabbix), Configuration management solution (Ansible) and integration of these into central monitoring and alerting with Splunk Enterprise and Elastic Search (ELK stack).
- Deployment of Spunk SIEM app (Enterprise Security) and configuration of log injection, detection rules, reporting and dashboards.
- Translation of security monitoring use cases into Splunk Enterprise rules/configuration, testing and documentation.

Department National Defence (DND)
11/2021 - 05/2022

I was brought on to assist with the deployment of a lab testing environment using VMWare products as well as assess the current cyber-security tools and processes and develop a set of requirements for the CD-DAR (Cyber Defence - Decision Analysis/Response). solution. Specific goals of this engagement were:

- Assist in developing a lab environment to test future cyber-security solutions
- Review design documents for implementation of monitoring solutions
- Install and manage virtual machines and software and tools (for sandbox testing)
- Develop system functional requirements for the CD-DAR solution, this involved assessing different vendor solutions for firewall, antivirus, intrusion detection and SIEM.
- Investigate options for using machine learning technologies and data analytics tools and processes to determine how they may be part of future cyber-security solutions and testing them in the sandbox (testing) environment.

General Dynamics
06/2021 - 12/2021

I was brought on this contract to assess the general health of the Splunk deployment as well as develop use cases, ensure configuration and monitoring were up to best practices.

- Evaluate the existing Splunk deployment and its suitability to the requirements of GD security monitoring.
- Installation, evaluation and configuration of Splunk apps.
- Setup of health monitoring for forwarder management, distributed search, and app deployment.
- Training staff and providing documentation and work instructions.
- Use Case development
- Backup configuration and monitoring of Splunk environment.

Note: There was overlap between General Dynamics and DND. For November and December 2021 I was only 'on-call' or 'as needed' for consultations, while DND ramped up.

Bank of Canada - Automation and Integration Specialist
03/2020 - 07/2021

In this contract my role was to provide advanced development, implementation and support services for the automation and scripting of Security Operations Centre (SOC) tasks related to the Bank's SIEM and ITSM solutions. Also to work with Bank stakeholders to research, develop, test, deploy, monitor, tune, report and maintain SOC automation tasks/scripts, including solution dashboards. I was the subject matter expert in SIEM/ITSM automation, providing advice to all stakeholders and participating and contributing to the planning and prioritization of SOC automation tasks.

- Development of new and modification of existing Splunk applications to facilitate integrations with various security event devices
- Assisted in the development of ServiceNow workflows.
- Rollout of revision control system for Splunk configuration files using Git Hub Enterprise including documentation and SOC personnel training on the solution
- REST API Integration of Splunk to ServiceNow Security Operations module for automated incident creation between the two cloud-based technologies (Splunk Enterprise Security notable events to ServiceNow incidents and workflow integration). This involved creation of a custom Splunk app written in Python with XML based Splunk dashboards.
- Installation, configuration and customizations to ServiceNow Security Incident Response (SIR) module.
- ArcSight decommissioning: assisted in the translation of ArcSight content (rules, reports, etc) from ArcSight to Syslog-NG & Splunk rules.

Shared Services Canada - SIEM Engineer
09/2019 - 03/2020

I was hired for this role to integrate QRadar SIEM with existing security devices, align the security program centered around IBM QRadar, Splunk and ArcSight. The business goal was to develop a SIEM to detect insider cyber threats and enable the SOC to react quickly to restore operations. Development of the threat detection capabilities, rules development, event and flow anomaly detection. Life cycle management, licensing, and capacity management. During my time at SSC I also worked with ArcSight products, ESM, logger, ArcMC, Splunk Universal Forwarders and resolved flow, ingestion and parsing issues with ArcSight smart connectors and developed a proof of concept to implement Micro Focus Transformation Hub.

- Linux system administration, including upgrading and patching applications and RPM file updates, user management, file system permissions, disk partitioning.
- Designed and deployed QRadar SIEM architecture.
- Troubleshooting and integration of Windows event feeds from Splunk Universal Forwarders into QRadar.
- Worked with various teams, application, networking, etc, to integrate event feeds.
- Designed and deployed QRadar SIEM content, rules, reports.
- Integrated security device events, resolved parsing issues.

- Developed threat detection content for QRadar to support SOC's ability to detect and respond to cyber threats.

Bank of Canada - Developer & Security Consultant
04/2018 - 10/2018

I was brought on as a SIEM engineer to do a review of their attack detection modeling in ArcSight. This included review of the rules, reports, dashboards and active channels as well as an update of the network model. I reviewed the relevancy of existing content and aligned it to the current environment and threat landscape. I was also responsible for the integration of several types of data feeds including ePO, CyberArk, and Tanium among others as well as developing threat detection content around these data sources. I also developed, installed, tested and documented an end to end threat intelligence feed (including known suspicious IP addresses, domains, email addresses, etc), to integrate into ArcSight threat modeling content. Sources include CCTX among others. The goal of the network model realignment and threat intelligence feed was to help automate the prioritization of events so as to reduce the volume that SOC personnel need to wade through and reduce "analyst fatigue". Another objective was to evaluate the need for specific event types and reduce licensing requirements (and thus associated costs) on the SIEM (while off-loading, non-security events to loggers and retain security events to the threat detection rule engine). I also gained further experience in automation with Python scripting where I used the TAXII API with python libraries for importing IOC information into ArcSight SIEM. I developed the automated IOC (indicators of compromise) import solution from various providers into ArcSight SIEM. This solution required the development and integration of Python libraries and corresponding APIs.

- Participated in SCRUM meeting for development of data pipeline development for SIEM security event processing, dashboards and reports (log management and threat modeling).
- Threat modelling and content development for Security Information & Event Management(SIEM)
- Rollout of Arcsight Active Framework SIEM content
- Life Cycle management of all security auditing, threat modeling and cyber threat intel systems.
- ArcSight, ESM. Logger, Smart Connector (SC) upgrades, custom flex connector development
- Integration of TAXII/STIX automated threat intel feed into SIEM from CCIRC, FS-ISAC, and SWIFT

Bell Canada - Developer & Security Consultant
09/2015 – 04/2018

I was hired to manage the life cycle of various ArcSight threat detection and log management solutions. My day to day tasks included operational support and assisting the SOC in developing and customizing SEIM content (specific to each client need) as well as troubleshooting event flow issues and SEIM performance issues. I worked closely with end clients to maintain and update threat modeling content to reflect their specific risks, concerns and compliance/regulatory requirements. While at Bell I also was utilized in the development and coding effort of a customer web portal where I used my skills and knowledge in development (Java and C#) as well as database integration. I also developed custom scripting/coding solutions over and above that which was provided by the security tool vendor to provide the end client with the business-specific needs (compliance or automation to reduce SOC personnel manual work to increase margins).

- Development of custom reporting solutions to support specific customer use cases which utilized various APIs such as JDBC using Java.
- Developed data pipeline for Security event processing
- Administration, installation, configuration of ArcSight SEIM/loggers/connectors
- Custom flex connector development to link internal software systems

- Custom content development for SIEM for automated threat detection
- Software development for internal portal (C# / Java)
- Deployment of ArcSight SIEM and ArcSight loggers
- Web application development (C#, Java, Javascript), securing web application dealing with issues such as Cross Site Request Forgery, Cross domain access, cross site scripting (XSS)

CGI - SQL Developer & Security Consultant

07/2001 – 04/2015

Architect/Administrator/Developer/IT Security Specialist

I was initially hired on with CGI as a software tester. Later I was placed in the software coding teams for many large government clients for their web application development. In early 2004 I was shifted to MSS (managed security solutions) department where I initially applied my coding skills to develop automation solutions. Where the particular cyber-security solution fell short, I was able to add custom functionality to the tools to satisfy end-client business needs. As an example, I developed a solution for the automated signature updates of several types of IDS vendor solutions to sensors in different security zones (which required multiple hops/proxies). The vendor (at the time) did not offer that functionality. Where SOC personnel was previously doing this (very time consuming) operation manually, the automated solution both performed the updates and logged any exceptions to a central display for further manual remediation. Another example is automated scanning and reporting of Linux targeted malware (a functionality not provided by the AV vendor at the time). I also authored a cyber-security incident management solution application (coded in C#) for the use by the SOC. Also at CGI I was the author of the external facing client web application portal, which gave the clients a "one stop shop" for both an overview of the status of their service from availability reports of services provided to them to records of communication from CGI MSS regarding suspicious traffic on their network/hosts. I leveraged again both my software development background and my knowledge of cyber security to provide both effective, meaningful reporting to end clients including mandatory regulatory and compliance reporting (PCIDSS as one example). I integrated the events from many types of cyber-security solutions (too many to mention!) into ArcSight SIEM where I developed threat detection modeling content which helped automate the priority assignment for events viewed by SOC members which reduced manual work and increased margins.

- Developed and supported in-house incident management software for SOC, worked with SOC manager and staff to align SOC operations with process and technology, providing new software features to align with SOC operational requirements.,
- Development web application with T-SQL backend databases
- Security Operations Center (SOC) support for ArcSight Security Event Information Management (SEIM), including maintenance of correlation rule sets, filters, active channels
- Development of ArcSight FlexConnectors (custom parsers)
- Configuring and maintaining WAF (web application firewall), specific use cases involving network protocol anomalies (at HTTP protocol, TCP, IP)
- Development of automation scripts for backup, system health monitoring, compliance reporting, antivirus signature updating and monitoring
- Development of SNMP extension tool (ipMonitor) – using APIs such as Simple Object Access Protocol application in C# which provided a higher level view of availability/down/up time reports across services, across data centers.
- Development of in-house incident tracking tool using C# and mySQL backend to support SOC
- Customer development of Antivirus signature update tool for Linux Servers
- Development of LDAP to RSA integration software and RSA PIN reset application written in C/C++. This solution required the utilization of C#.net LDAP APIs.

- Development of custom parsers for their in-house applications for connectivity to ArcSight Logger and automation tools for auto-sync SEIM content between primary and secondary systems
- Deployment and support of ArcSight Logger appliances
- Developed service level reporting portal which provided key risk indicators and compliance dashboards.
- Development of custom scripting solutions, for example, automated IDS signature distribution and error reporting.
- Custom ArcSight SEIM rules development and parsers.
- Developed and supported PHP web application for RSA token management.

Bright House (formerly Road Runner) contracted through Convergys
06/2000 – 07/2001
Senior Technical Advisor

I was hired to help assist end users with their internet connection issues to the service as well as educate the end users on usage of the ISP's self service web application. I also tracked incidents and coordinated with local network troubleshooting teams.

- Provided 2nd level troubleshooting support for telephone support agents
- Directly worked with Network Operations Center (NOC) to resolve connection problems, email issues, etc
- Development of real time issue tracking system for call center

Education

Algonquin College, 1999-2000 (graduated with honours).
eCommerce, Web development, software design and relational database.

Training and Certifications

- Certified Python Developer, 2020-04-02
- CISSP with ISC^2 (2019 - 2022)
- Certified Ethical Hacker (CEH), EC-Council (2018 - 2021)
- (Registration Number:285906209, Validation Number:870238996 - https://www6.pearsonvue.com/testtaker/authenticate/AuthenticateScoreReport.htm)
- 2019 Certified Splunk Administrator
- 2018 Certified Splunk Power User [Dec 2018 - Dec 2020]
- 2018 Certified Splunk User (2018, LICENSE #: Cert-261189)
- ArcSight Certified Security Analyst (ACSA)
- 2016 ArcSight Certified Integrator/Administrator (ACIA) & ArcSight Certified Security Analyst (ACSA)
- 2011 Web Application Firewall and Database Activity Monitoring
- 2010 Entrust PKI
- 2005 ITIL Foundations Certification
- Algonquin College, E-Commerce/Web Development (honours) 2000
- SEM, ITIL, Entrust PKI, Web Application Firewall
- Database Activity Monitoring certifications

Professional Memberships

- International Information System Security Certification Consortium - (ISC)²
- Controlled Goods Program Industry Engagement Committee (IEC)
- EC-Council

Certifications

CISSP

- https://www.youracclaim.com/badges/7e83cd18-623f-48ff-acfc-b1efc42d7db0

CEH

- https://aspen.eccouncil.org