Proposal Options for External and Internal Network Penetration Test

Classification: CONFIDENTIAL & PROPRIETARY TO BHIS

Presented to:
Monterey County
Dan Kern

Proposal Number 2023-1193 Prepared by:
Black Hills Information Security, LLC
115 West Hudson St.
Spearfish, SD 57783

Date Issued: October 23, 2023

"Proposal" becomes "Statement of Work" upon signing.

Table of Contents

Black Hills Information Security Approach

Monterey County recognizes the need to identify vulnerabilities and associated risk within their organization to improve the security of their IT infrastructure.

Security should augment and strengthen your organization. Some penetration testing firms mistakenly believe that security is the sole business goal for a company or institution. At Black Hills Information Security (BHIS), we understand that your organization is looking for security solutions that drive business and institutional value, among many other considerations. We strive to provide our customers with the answer to one critical question: What actions can be taken to truly improve your organization and make its staff and security architecture better while allowing your organization to perform its other core business functions?

How does our company differentiate itself from others?
Below are several reasons why BHIS stands above and apart from other security consulting companies.

Community Involvement

Due to our commitment to strengthening the entire security community, BHIS strongly believes in giving back to that community. The members of BHIS are part of Paul's Security Weekly (formerly called "PaulDotCom" Security Weekly), the world's largest technical security podcast. We also believe in the power of open-source. We contribute to and are founders of many different open-source projects, such as Recon-ng, Pushpin, the Active Defense Harbinger Distribution, and the Penetration Testing Execution Standard. We have also presented at SANS, Defcon, Black Hat, DerbyCon, and HTCIA, as well as for the FBI, NSA, and DoD. BHIS believes that the landscape for security professionals today requires us to be more patient, persistent, and adaptable than attackers, and that education is the key to instilling these characteristics industry wide.

Non-Traditional Defensive Research

One situation is becoming increasingly evident: Attackers have an advantage on us. Why? Mainly because mainstream defensive tools and techniques are so transparent. Traditional AV vendors and Firewall/IDS vendors encompass 80% or more of most organizations' entire defensive strategy. Without question, a targeted attacker will go through the effort to acquire these same tools and bypass these technologies. This is why BHIS does not simply recommend the same easily bypassed technologies that other penetration testers often propose.

At BHIS, we are on the cutting edge of active defense technologies. In fact, we founded and maintain the only active defense security distribution framework on the internet. The Active Defense Harbinger Distribution is a DARPA-funded project created by BHIS which strives to be an incubator for new defensive ideas and technologies. The mindset of this project fuels everything we do at BHIS.

Meaningful Reports

Human Narratives, Not Just Tool Output

BHIS strives to provide reports to our customers that truly reveal the vulnerable attack surface of your organization, as well as detailing meaningful, real-world mitigations. BHIS does not copy and paste vulnerability scanning results into our reports. Rather, you will find a full narrative that navigates you through the assessment. Our findings write-ups are based on our security consulting experience across many industries and are tailored to your organization's specific situation. Our customers can run many of these tools on their own, yet there is little to no added value in a testing company charging exorbitant amounts of money for a report generated from a free or low-cost tool. Value from a test derives from what

is found beyond the scanning results via the experience of the tester. This experience and insight are integrated into every report that BHIS delivers.

Knowledge Transfer
BHIS was founded on world-class training. To date, we have trained over 20,000 information security professionals. Because of our teaching experience, we have a strong philosophical approach built on not just providing a report but detailing our tactics to ensure our customers understand how a given attack was executed and the impact on the customer environment. From web attacks, to AV bypass, to internal pivoting, BHIS works to ensure your employees can recreate what we have done in the penetration test. This focus is reflected in our reports, as our aim is to support strong security teams who can navigate your organization's defensive efforts confidently.

When we complete testing, we promise the following:

1. You will get a report that was generated by a real human being who was active in the testing of your organization. Actual thoughts about your organization and your needs will go into the report. We will never be satisfied by simply clicking "Generate Report" from a tool.
2. Your team will not only know what we found, but they will know how we found it. This approach is important because improving technology is relatively minor compared to improving the capabilities and understanding of your people. We strive to provide knowledge transfer so your team can approach the ever-changing threat landscape with a *methodology* and not just a checklist.
3. As part of this contract, all BHIS customers will gain access to an online Antisyphon Cyber Range for up to five (5) people from their team. This environment contains over 50 different challenges ranging from network, active directory and host-based threat hunting, web application attacks and security, operating system security, and forensics. This proposal item is available upon request for up to one year after contract start.

Scope Offered by Black Hills Information Security

External and Internal Network Penetration Test

Description

When performing scanning activities over the past years, we have noticed that automated tools are often finding fewer and fewer critical vulnerabilities. While this trend is a good thing, we are also discovering many organizations are vulnerable due to Low or even Informational findings. This is one of the major differentiators for Black Hills Information Security (BHIS). We look at scanning and exploitation as more of an endeavor of learning about your environment, the same way a targeted attacker would. We do not simply run a scanner, look for criticals, and then search tools like Core Impact and Metasploit for an exploit. We use our scanning information to try to understand your network and the individual roles of the computers that comprise it. We want to understand how these points of technology support the overall organizational objectives. With this approach, we find far more vulnerabilities than what is reported by a simple scan.

During the assessment and penetration testing phases, we will perform port scans, vulnerability scans, and testing for all computers, devices, databases, and networking equipment on in-scope networks. We will validate the scans to weed out false positives by manually verifying a subset of results within particular vulnerability classes. However, the true value of a penetration tester over a scanner is going the extra mile of looking at vulnerabilities (including the Low and Informational findings) as well as manually probing the in-scope networks and looking for additional methods of entry or compromise not flagged by a scanner.

Testing is typically performed remotely from BHIS systems connected to the Monterey County network. Several options are available from which BHIS can perform remote, internal network testing – minimizing setup time for your team and eliminating the travel costs of on-site testing.

Black Hills Information Security will use specialized techniques (if applicable) such as document metadata analysis, custom password dictionaries, and other proprietary methods. Remediation guidance will be provided for each vulnerability documented in the report, as well as strategic recommendations for improving the security of the organization as a whole.

Targets

- Up to
    - External (Public) Live Systems:
        - < 175 Live IPs
    - Internal (Private) Live Systems:
        - < 6000 Workstations < 350 Servers <10,000 Network Devices

This scope item will be completed remotely.

Objectives

- Provide a profile of the organization and threat modeling available to potential attackers
- Identify systems and key assets exposed to attackers
- Enumeration of vulnerabilities present on systems
- Provide recommendations for protecting key company assets
- Identify areas where sensitive information is exposed
- Provide evidence of the effectiveness of current defensive mechanisms and attack detection methodologies
- Provide an in-depth understanding of discovered vulnerabilities and repercussions, via exploit attempts, where applicable

- Provide recommendations for remediation of the identified practices and/or exposures based on the above testing

For web applications, please note that in-depth testing is best serviced by a dedicated BHIS Web Application Penetration Test that follows an industry-standard methodology, such as the one compiled by the Open Web Application Security Project (OWASP). However, as part of a network level assessment, a limited scan with the following high-level goals may be performed from a network perspective:

- Provide recommendations for mitigating select exposures in web applications
- Provide limited inventory of select vulnerabilities in the organization's web applications that may expose users to malicious exploits
- Provide high-level understanding and verification, via exploit attempts, of select vulnerabilities in the organization's web applications

Methodology

Assessment and testing focus on identifying key assets and targeting them to harvest information, just as an attacker would on the inside of the network. These tests will include:

- **In-Depth Company Profiling and Threat Modeling** – One of the values provided by testing is an understanding of what information can be gathered about your organization from open sources and, more importantly, what attackers can do with it. We will use various tools and resources to collect public information about your organization and couple it with custom threat modeling to perform targeted attacks and report on them.

- **Host Discovery and Service Identification** – BHIS identifies hosts using several network scanning techniques. By employing different techniques, we can quickly obtain a list of assets, and enumerate the services on them.

- **Vulnerability Discovery** - To further identify risk, a vulnerability scan is specifically tuned for the environment and then executed. This scan can be run across the network and is used as a baseline for exploitation. Internal testing also provides for the opportunity to run authenticated scans, which means the scanner will need user-level authentication to the targeted systems, which allows the scanner to compare the host's configuration to compliance and various industry standards.

BHIS Background with Network Assessments and Penetration Tests

The staff at BHIS hold multiple certifications in the area of network assessment and network penetration testing. However, certifications often don't tell the whole story.

We also teach network penetration testing for the SANS Institute and offer multiple free webcasts on the topic.

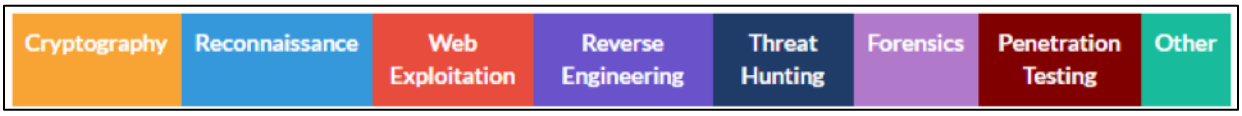
The link below highlights just a few webcasts we have offered in the area of vulnerability assessments and network penetration testing:
http://www.blackhillsinfosec.com/?page_id=4424

Antisyphon Cyber Range

As part of this contract, all Black Hills Information Security (BHIS) customers will gain access to an online cyber range for up to five (5) people from their team. This environment contains over 100 different challenges ranging from network, active directory and host-based threat hunting, web application attacks and security, operating system security, and forensics. This proposal item is available upon request for up to one year after contract start.

Challenges

After registration is complete and you've successfully logged into the Antisyphon Cyber Range Scoreboard, you will gain access to the Antisyphon Cyber Range challenges.



Antisyphon Cyber Range Challenge Types

There are seven (7) different challenge types:

1. Cryptography
2. Reconnaissance
3. Web Exploitation
4. Reverse Engineering
5. Forensics
6. Penetration Testing
7. Other

Many of these challenges have hints to help people through them.

The goal of any contract with BHIS is to help wholly strengthen our customers' teams. We fundamentally believe that training should be part of any contract we sign. Because of this, we make this cyber range available to all our customers.

ACE-T™ stands for "Antisyphon Cyber Education Testing." Individuals can get ACE-T™ certified by completing challenges in the Antisyphon Cyber Range, which contains a variety of challenges related to cryptography, forensics, penetration testing, reconnaissance, reverse engineering, and web exploitation. The Cyber Range currently has ten levels of ACE- T™ certification for users to work through.

ACE-T™ certification allows users to demonstrate their infosec expertise to colleagues, management, and HR personnel alike. Users also have the ability to share their ACE-T™ certification level with others by having them look up their name at the following URL: https://lookup.hackhills.com/.

Deliverables

Black Hills Information Security to Monterey County

- Schedule and coordination
  - Establishment of test dates
  - Project plan
  - Selection of tester(s)
- Rules of Engagement call
  - Review of scope
  - Communication Protocol
  - Confirmation of penetration testing start dates and times
- Report detailed testing results, as described in the Report Format section below:
  - First copy will be considered "draft pending customer comments/input"
  - The first copy will be issued no later than 10 business days from the completion of work. Monterey County then has 10 business days to review the report, add comments, and request changes. BHIS then has 5 business days to issue a response and deliver the final report.
  - If no comments/input are received, the "Draft" will be considered "Final"
  - BHIS will invoice upon report delivery.
- General recommendations for improvement of organizational security
  - Monterey County's questions will be answered for 90 days following completion of work. BHIS cannot guarantee tester's continued availability after this point.

Black Hills Information Security (BHIS) will compile each phase of the security assessment into a report containing the following:

- **Executive Summary** – A highlight of the major problems found and high-level recommendations that address the specific issues, tailored for an executive-level audience. An overall risk analysis rating relative to the discovered findings will also be assigned and described in this section.
- **Methodology** – A complete description of all testing performed, including instructions for recreating the test scenarios so that the organization can re-test after mitigating controls have been implemented (as available).
- **Findings** – A complete description of each major vulnerability found, including details on how it was exploited and what information or level of access was obtained as a result. This section will also contain:
  - ***Discussion*** – A description of how the documented vulnerability could affect the organization if an attacker exploited it
  - ***Recommendations*** – A detailed description of how to fix the vulnerability (as available), including command and configuration examples. Also included are any organizational improvements to policy and/or processes that will help remediate the vulnerability
  - ***Resources*** – Links to information about the vulnerabilities that were found and remediation guides (as available)
- **Supporting Data Archive** – An archive of all tool output and vulnerability scan reports. The archive will also include:
  - Listing of all open ports and likely services based upon fingerprinting and analysis techniques
- **Results of Any Specific Testing (as applicable)**
  - For example, password cracking, wireless assessments, social engineering, and port scanning will be included. Each vulnerability or exposure will be documented in the format described above.

Monterey County to Black Hills Information Security

- Signed agreement (see separate MSA)
- BHIS strongly suggests testing occur on non-production systems and databases (for web application penetration testing). When needed, we can accommodate two phase engagements, where testing occurs on non-production assets with some issues validated later on production.
- Authentication credentials for the web application(s) to be tested
- Remote access via VPN or other compatible remote access method
- Scoping document with scope authorization. Generated with project management team following award of proposal.
- BHIS will need access to customers testing environment for the 2 weeks of the reporting period
- Primary Project Contact and Primary Technical Contact information:

Primary Project	Primary Technical (if different)
Name: Dan Kern	Name:
Title:	Title:
Email:	Email:

Please note, the project management team will generate a scoping checklist in conjunction with the BHIS customer during meetings, following the signing of the statement of work. Below is a breakdown of some of the items typically covered in the scope checklist.

- Targets or technical points of focus
- Primary and backup points of contact
- Notification procedures for critical findings
- Authorized testing timeframes
- Notification procedures and protocols for customer points of contact
- Meetings, notifications, and contact frequency and format
- Sensitive and/or prohibited ranges and systems
- Customer guidance to testers
- Etc.

Project Timing

Timing

Please note that the timing of this project will be determined following signature of proposal/statement of work. The schedule will be generated by the BHIS project team, following coordination with Monterey County regarding deadlines, tester availability, and customer enterprise environmental factors (e.g., remote access, test string availability, blackout dates, support personnel etc.). No guarantees on schedule can be made that are not identified in this section.

BHIS has not preplanned this work.

Work that has not been preplanned may take six to twelve (6-12) or more weeks to commence, starting from the date of a signed proposal/statement of work. This estimate is based on current workloads, resources, and projections.

Cancellation or rescheduling of work without 4 (four) weeks prior notice will incur an additional charge. The following schedule may be enforced if BHIS is not able to reschedule work to avoid idling a tester.

- Less than 4 weeks' notice incurs an additional 20% charge
- Less than 2 weeks' notice incurs an additional 50% charge
- Day of start or within testing time frame incurs an additional 100% charge

BHIS will make a reasonable effort to reschedule work for testers and avoid the additional charge. Additional charge shall be assessed only on the portion of a test that is delayed or cancelled.

The table below is listed for planning and estimation purposes. This reflects time on keyboard or on-site actively engaged in the testing methodology. It does not include planning, coordination, set up, reporting or debriefing the customer. As all BHIS engagements are timebound, proper guidance from Monterey County will result in optimal coverage within the time constraints.

Service Options	Estimated Active Tester Time for Planning Purposes
External Network Penetration Test <175 Live IPs	4 days
Internal Network Penetration Test <6000 Workstations <350 Servers < 10,000 Network Devices	7 days
Antisyphon Cyber Range	Within a Year

Fees

Quote

The following fixed fee(s) for service below is/are good for 45 days from issuance.

Fee(s) include(s) project setup, coordination, test preparation, standard report production, report review, report editing, and comment resolution. Any work beyond this description and the work described in each section above should be discussed with the BHIS team prior to signing of this proposal. All line items are timebound.

Remote Testing Options	Estimated Active Tester Time for Planning Purposes	USD
External Network Penetration Test <175 Live IPs	4 days	$14,080
Internal Network Penetration Test <6000 Workstations <350 Servers < 10,000 Network Devices	7 days	$23,680
Subtotal		**$37,760**
Onsite Testing		
NA	NA	NA
Subtotal		**NA**
Assessment Total (not including any applicable travel expenses)		**$37,760**

Included Services	USD
Antisyphon Cyber Range ($1,800 Value)	Included

There is no decrease in cost if customer chooses not to select the included service. The included service is available upon customer request.

NOTE: Daytime/business hours testing is assumed. Daytime/business hours are defined as 8am ET to 6pm PST, Monday through Friday. Automated scanning may be run off-hours but not penetration testing.

Remediation validation (remediation check of reported findings) can be added as an option as one day blocks of $2,500. Remediation validation must be completed within 30-60 days from the Initial Report. Ongoing remediation validations are limited to one validation. Remediation validations cannot be performed on Pivot, Red Team, Physical, and Wireless tests.

Client is invoiced per the MSA or monthly for work completed over an extended period of time.

The above statement of work is hereby accepted and will be executed in accordance with the signed Master Service Agreement on file. In consideration of the mutual promises herein contained and other good and valuable consideration (the receipt of which is hereby acknowledged), authorized representatives of the parties have signed this Agreement as of the Effective Date.

Monterey County	**BHIS**
Signature:	Signature: DocuSigned by: Nora Fletcher CD99DA2F5E8C407...
Name:	Name: Nora Fletcher
Title	Title Project Management Professional
Date:	Date: 11/29/2023 | 4:34 AM MST

Invoice Name(s)/POC(s):
Invoice Address:
Invoice Email:
Invoice Phone:
Invoice Mailing address of company is different than physical address:
Special Instructions, if required:

Appendix A: About Black Hills Information Security

Black Hills Information Security is a leader in the information security industry. We are part of the most popular weekly security podcast on the topic, provide monthly webcasts on late-breaking computer attack vectors, and frequently speak at internationally recognized conferences in addition to teaching for the SANS Institute.

John Strand, GCIH, GCFW, CISSP
John is the Owner of Black Hills Information Security (BHIS) and has both consulted and taught hundreds of organizations in the areas of security, regulatory compliance, and penetration testing. John is also an instructor and course author of BlackHat's "Active Defense, Offensive Countermeasures, and Hacking Back" and the SANS Institute's "Hacker Tools, Techniques, Exploits and Incident Handling" classes. John is co-author of the" Offensive Countermeasures: The Art of Active Defense" book and is a contributor to the industry shaping Penetration Testing Execution Standard and CIS Critical Security Controls frameworks. He leads the Hunt Teaming, Command & Control (C2)/Data Exfiltration and Pivot testing development at BHIS. He is a dynamic speaker at IANS symposiums and other conferences worldwide. In his spare time, he co-hosts the Hack Naked TV and Security Weekly podcasts.

Ethan Robish, GCIH, GREM
Before becoming the second full-time employee at BHIS, Ethan interned with BHIS for 4 years while he obtained a B.Sc. in Computer Science and a minor in Mathematics at South Dakota School of Mines & Technology. During that time Ethan implemented defensive security solutions for the Exchange Online security team as an intern at Microsoft and obtained his GIAC Certified Incident Handler certification from the SANS Institute. Ethan is the project lead of the Active Defense Harbinger Distribution.

Joff Thyer, GXPN, GWAPT, GPEN
Joff has over 25 years of experience in the IT industry in roles such as enterprise network architect, network security defender, penetration tester, and malware researcher. He has experience with intrusion detection and prevention systems, penetration testing, engineering network infrastructure defense, and software development in multiple programming languages.

Joff has taught "Automating Information Security with Python" at the SANS institute and developed/taught information security classes "Enterprise Attack Emulation/C2 Channels", "Regular Expressions", and a beginner "Introduction to Python" course for AntiSyphon training. Joff is also a faculty member with the IANS research group in Boston, MA.

Joff holds a B.Sc. in Mathematics, an M.Sc. in Computer Science, and holds the GIAC certifications GPEN, GPYC, GWAPT, and GXPN. He helps lead technology development, assumed compromise testing, and malware research techniques at BHIS. In his free time, Joff enjoys woodworking and being a musician.

Beau Bullock, OSCP, OSWP, GCIH, GCFA, GSEC, GPEN, GXPN
Prior to joining BHIS, Beau's primary role has been implementing security controls to protect information and network assets. He has held information security positions in the financial and health industries. Beau has experience with all aspects of enterprise network security including penetration testing, vulnerability analysis, data loss prevention, wireless security, firewall management, and employee security training. In his spare time, he hosts the Hack Naked TV information security webcast and presents at conferences. Beau holds a B.S. in Information Technology.

Brian Fehrman GXPN, OSCP
Brian Fehrman has been with Black Hills Information Security as a penetration tester and security analyst since 2015, but he has been interested in security since his family got their very first computer. Brian has a passion for learning; he spent eight and a half years as a full-time student prior to his career. In this time, he obtained a BS in Computer Science, an MS in Mechanical Engineering, and an MS in Computational Sciences and Robotics. Beyond that, he is a GIAC certified Exploit Researcher and Advanced Penetration Tester (GXPN), an Offensive Security Certified Professional (OSCP), and he will

begin working towards a PhD in Cyber Operations in the Fall of 2019. Brian's love of learning is evident in his work too, as one of his favorite aspects of his job is the continuous new challenges that push him to improve his skills. He enjoys being able to protect his customers from "the real bad guys" and his favorite aspects of security include internal-network pivot tests, red teaming, and hardware hacking.

David Fletcher, GSE, GSEC, GCIA, GCIH, GCFA, GAWN, GISP, GLEG, GCPM, GWAPT, GPEN, GXPN
David Fletcher has been working for Black Hills Information Security as a penetration tester and security analyst since 2015. He has spent most of his career working for the US Air Force and engaged in a variety of disciplines within the IT industry including boundary defense, web and application development, system administration, and offensive cyber research. David approaches penetration testing with a creative mind, treating each test as a puzzle and always exploring new methods of exploitation. He holds a BS in Electrical Engineering and an MS in Information Security Engineering from the SANS Technology Institute. Outside of work, David enjoys playing the guitar, hunting, and fishing.

Brian "BB" King, GXPN, CEPT, CISSP, GCIH, GCIA
BB has been a Security Consultant at BHIS since 2015 and a penetration tester since 2008. In previous corporate security roles, he developed application security testing and reporting standards, worked with development teams to improve coding practices, and with new penetration testers to help them gain proficiency and understanding. At BHIS, he specializes in web applications and web APIs, and sees developers and QA engineers as partners in the never-ending quest to make security part of the development lifecycle instead of just a checkpoint near the end. He teaches penetration testing and reporting classes with Antisyphon Training and at local security conferences whenever he can.

Derek Banks, CISSP, GCFA, GNFA, GCIA, GCIH, GMOB, GPEN, GSEC Gold (Ret.)
Derek has been a Security Analyst for Black Hills Information Security since 2014 and has been in the IT industry for his entire career. He has experience in forensics, incident response, creating custom host and network-based monitoring solutions, penetration testing, vulnerability analysis, and threat modeling. Derek has a BS in Computer Information Systems and a MS in Data Science. Derek enjoys spending time with his family, staying physically fit, outdoor activities, and playing the guitar.

Sally Vandeven, GIAC (GSE, GCIH, GPEN, GWAPT, GCIA, GNFA, GCFE, GCFA, GREM, GSEC, GCPM, GCWP), CISSP, CCE, GAWN
Sally Vandeven has been a security analyst and penetration tester for Black Hills Information Security since 2015. She also currently works as a faculty research advisor for the SANS Technology Institute graduate program. Prior to joining the team at BHIS, Sally worked as an application developer, Linux system administrator, and a mom, which she describes as the best job in the world. Sally has a talent for physical security tests, but she also enjoys internal pivot tests, cracking passwords, and finding new and unique ways to approach her work. Sally has many hobbies outside of work, her top three are hiking, biking and juggling.

Rick Wisser, GCIH
Rick has over 15 years of experience in networking, system infrastructure, and deployment. His past experience includes working in an information systems capacity, engineering, and engineer management. Rick served in the Air Force and his career has involved medical systems, aerospace/defense, telephone, storage devises, radio frequency, wireless communications and other specific proprietary computing systems.

C. J. Cox, CISSP, QSA, GSNA
C. J. has over 25 years of experience in information technology and security in both government and industry. He has worked in in roles to include help desk, system administration, classroom teaching, network operations Information System, Security Officer, Information System Security Manager, Information System Security Engineer, and technology management.

Jordan Drysdale, GCIH, GPYC, CCNP, VCP, HP MASE, FCNSP

Jordan Drysdale has been with the Black Hills Information Security family since 2016. He is a security analyst, penetration tester, and member of the systems administration team. Jordan came to BHIS with a very strong background, including many years of work in networking tech support and systems engineering. Throughout the years with BHIS, Jordan has fostered growth initiatives, developed training courses, and shared knowledge with anyone willing. Jordan now serves as part of the quality control team and serves as one of BHIS's external and internal network testing leads.

Craig Vincent, OSCP (retired), OSWP (retired), GWAPT
Craig Vincent is a security analyst and penetration tester and has been with Black Hills Information Security since early 2018. He has a background in software development, red teaming, and systems engineering with a B.S. in Computer Science and a B.S. in Computer Security from Fairmont State University. He has the OSCP, OSWP, CEH, and Security+ certifications. When on an engagement, Craig has the keen ability to find a couple of seemingly minor vulnerabilities that he can exploit together for a more interesting result...the "popping of boxes.

Kent Ickler, GCIH, MCSE, MM
Kent Ickler has nearly 20 years of experience working in the Information Technology fields. He has a Masters in Management with undergraduate studies in Network Design and Management. He has extensive background in telecommunications, Financial Services, Higher Education Management and SMB industries. His background in Business Management provides a thorough understanding of how Business Operations are supported by Information Technology and how the complex and critical nature of Information Security can make or break business in today's environment.

Bryan Strand, GHIC, GCCC
While Bryan's focus at Black Hills Information Security is currently the Manger of Business Capture, he has a growing passion for strengthening defenses through the CIS 20 Critical Controls. He has earned his GIAC Certified Incident Handling Certification and GIAC Critical Security Controls Certification.

Justin Angel, OSCP, OSCE
Justin is a technical resource with a passion for network-based offensive security. He developed a foundation for InfoSec while pursuing his Bachelors Degree in Information Security and Assurance at Kennesaw State University, where he graduated Magna Cum Laude in December of 2013. Certification programs, such as the Offensive Security Certified Professional (OSCP) and Offensive Security Certified Expert (OSCE), later allowed him to obtain a practical skill set that now enables him to creatively identify and exploit vulnerabilities pursuant to achieving threat objectives during engagements.

Michael Allen, OSCE, MLSE, CISSP, OSCP, SEPP
Michael Allen is a Senior Security Analyst and Red Team Practice Lead who joined the team at Black Hills Information Security (BHIS) in 2019. Having started hacking and picking locks at an early age, Michael has since turned "doing things he's not supposed to do and going places where he's not supposed to be" into an impactful career. He has a multitude of infosec certifications and his “think like a criminal” mindset on security assessments brings incredible value to the clients he serves. Pentesting isn't just a job for Michael; it's a way of life, in which he brings fun, creativity, and passion to every hack, breach, and bypass he attempts.

Dale Hobbs, GSEC, GCIA, GCIH, GPEN, GCCC, GDAT, CRTP
Dale has over 22 years of experience in networking, system administration, and security operations and engineering. His past experience includes heading up the infosec team for a large North American Retail company where he built their security program from the ground up. Dale holds the GSEC, GCIA, GCIH, GPEN, GCCC, GDAT certifications and is an active member of the SANS Advisory board.

Mike Felch
Mike is a red team lead and security researcher at Black Hills Information Security along with being an active instructor and course creator for offensive security training curriculum. Prior to joining BHIS, he was Vice President of Security Research for an infosec startup leading technical teams and exploiting

hardware. Throughout his career, he's held roles as a software engineer, pentester, and system administrator. Mike is a divergent thinker who enjoys cognitive challenges and understands the power of collaboration. He's actively involved in the infosec community as a public speaker and regularly open sources red team tools and security research.

Corey Ham, OSCP
Corey is a security analyst at BHIS, specializing in penetration testing and red teaming. He has over 8 years of experience in offensive security consulting focused around adversary simulation engagements and TTP development. Corey has been a speaker at various conferences, including defcon red team village and source zero con. He has published and contributes to open source projects focused primarily around OSINT. Outside of security, his technical interests include infrastructure and development, and his personal hobbies include the outdoors and cars. Corey graduated with a BS in computer networking from Baldwin Wallace University in Berea, OH.

Tim Fowler, OSCE, OSCP, OSWP, CISSP
Tim Fowler has been working for Black Hills Information Security as a penetration tester since 2021. Prior working for BHIS, he worked in the financial sector as a cyber security research scientist and red teamer, as well as managed all cyber range operation for a financial institution. Prior to that he worked as a security consultant, performing penetration testing, policy review, and incident response. Tim is active in the information security industry and as contributed by giving talks at various conference's, developed a wireless penetration testing training course and served as a mentor for a collegiate cybersecurity program. Outside of work, Tim enjoys spending time with his family, working in his woodshop, tinkering with his CNC machines, and training for long course triathlon's.

Ben Burkhart, OSCP, ESCP. ESCPPT, Sec+
Ben Burkhart is a security analyst and penetration tester at Black Hills Information Security with experience focusing on enterprise Windows Active Directory networks and internal penetration assessments. Ben has also worked to help organizations bolster their security incident detection and response capabilities by performing adversarial threat emulation activities. Ben has led and delivered internal, external and application penetration assessments as well as incident response, assumed breach and cloud security audits for organizations of varying size and industry, including Fortune 25 companies. Ben has a non-traditional background, including a lifetime of tinkering with technology and a storied career bartending in Chicago. When he's not working, Ben enjoys running, video games, and caring for a retired racing greyhound named Louise.

Ralph May, OSCP
Ralph May is a penetration tester and security analyst for Black Hills Information Security. Ralph joined the BHIS team in 2020. Before joining BHIS, Ralph works for a competing firm as a penetration tester for the last five years. Ralph has delivered on a diverse set of engagements to included advanced adversary simulations, physical engagements, and advanced hybrid cloud penetration tests. Ralph is extremely active in the security community, speaking at multiple conferences and contributing to numerous open-source security tools. Ralph is a US Army veteran, having worked directly under the United States Special Operations Command as a soldier and civilian on many different information security challenges and treat actor simulations.

Kevin Klingbile, GIAC (GSE, GMOB, GCCC, GMON, GCLD, GDAT, GCDA, GPEN, GBFA, GWAPT, GCFE, GNFA, GSEC, GCIH, GCWN, GCIA, GNSA), CISSP P
Kevin has over 18 years experience working in the Information Technology field. Prior to joining the team at BHIS, Kevin worked in energy utilities, telecommunications, and healthcare industries. He has held positions from helpdesk to network engineer, systems admin, and security analyst. Kevin is a contributor to the IT security community as an advisor on the CIS top 20 controls panel. He also teaches security courses at Western Dakota Tech as an adjunct professor. He holds an MBA in Information Technology Management and a BS in Information Technology.

Ashley Knowles

Ashley has over a decade of experience in Cyber Security. She has spent her career working as a penetration tester providing internal and external network penetration tests, web application, social engineering, WiFi and physical assessments. Ashley also spent three years leading an internal red team and developing custom red team tooling. Ashley holds a B.S. in Information Science and Technology and is currently studying for a M.S in Cybersecurity at DePaul University.

Luke Baggett, GSEC, GPEN, GCIH, GCIA, GCFE, GXPN
Luke Baggett is a security analyst for Black Hills Information Security. Before joining BHIS, he worked in roles involving network security monitoring and systems administration. Luke holds a BS in Computer Science from the Georgia Institute of Technology and multiple certifications from the SANS Institute.

Sean Verity, GXPN, GPEN, GAWN, CISSP
Sean Verity began working for Black Hills Information Security (BHIS) in March of 2022 as a security analyst and penetration tester. Prior to working at BHIS, Sean built a comprehensive ethical hacking program for one of the largest federal credit unions in the United States (US). Sean is also a US Marine Corps (USMC) veteran. During his time in the USMC, Sean discovered his calling when he learned that there was a profession that would allow him to hack (legally, of course). Sean is excited to be on a team with like-minded individuals and to participate in passing on knowledge. Outside of work, Sean enjoys laughing at his wife's jokes, hunting, gardening, and working out.

Joseph Kingstone, OSCP, OSWP, CISSP, CRTO, CRTP, MCSA, eCPTX, eCPPT, eWAPT, PNPT
Joseph has been in I.T. since 2014 and in Cyber Security since 2015. Joseph has held roles from Tier 1 Help Desk/System Administrator to Senior Operator on Red Team engagements. His favorite part of working at BHIS is collaboration among a large group of talented testers and helping customers understand, plan, and fix vulnerabilities. Outside of work Joseph enjoys tinkering with cars, exploring the planets with a telescope, and helping fellow veterans break into CyberSecurity.

Gabriel Prud'homme, OSEP, OSCP, PACES, CRTE, CRTP, CRTO, CARTP
Gabriel Prud'homme joined Black Hills Information Security (BHIS) in 2022 as a full-time Penetration Tester / Security Analyst. Gabriel previously worked in the IT field for 15 years before transitioning to security as a pentester for a large telecommunication company where he delivered internal, external, social engineering, and wifi security assessments for various industries. His curiosity and passion have driven him to acquire several certifications over the years. He is honored to be part of the BHIS team for their "doing the right thing and doing it right" philosophy. During his free time, he enjoys "taking the time" with his family, backpacking, and scuba diving.

Melissa Bruno
Melissa Bruno began working for BHIS as a Security Analyst in March of 2017. Her focus is on penetration tests for web applications, external networks, and internal networks. Melissa has a bachelor of science degree in computer information systems with a concentration in information security, and prior to joining BHIS she worked on securing systems and programming security tools as a Security Engineer. She describes testing at BHIS as being akin to "going on a treasure hunt every day." Outside of work she is an avid reader of sci-fi and fantasy novels, as well as technical books that help hone her skills.

Daniel Pizarro, PNPT, eCPPT, eWPTX, eWPT, eJPT, OSWP, OSCP, PenTest+, CySA+, Security+
Daniel Pizarro is a Security Analyst and Penetration Tester at Black Hills Information Security (BHIS). Before joining the BHIS team, Daniel developed open-source security tools, worked as a penetration tester, participated in bug bounty programs, and worked as a cyber security instructor. His responsibilities at BHIS include web application and external penetration testing, as well as internal infrastructure testing.

Alyssa Snow
Alyssa Snow joined Black Hills Information Security as a security analyst in the Spring of 2022. Alyssa holds a BS in Computer Science. She began her career building automated security solutions as an application security intern. Previously, Alyssa worked on an internal offensive security team at a software company. Alyssa chose to work at BHIS because of the team full of inspiring people who are passionate

about security and educating the community. Outside of work Alyssa enjoys spending time outdoors with her loved ones.

John Malone, eJPT
John Malone has a background in management consulting and physical security, and recently began working with Black Hills Information Security. He holds an Associates of Science degree in Computer Networking and a graduate-level education in Organizational Psychology. John's experience ranges from contracting as a security officer up to holding a leadership position as an account manager for a Fortune 500 client, where he had full ownership of the organization's Midwest physical security operation. He has experience in physical penetration tests, along with some webapp, internal, and wireless network tests. Outside of work, John enjoys competing in CTF events, creative writing, and spending time with his family.

Steve Borosh, OSCP
Steve Borosh is a proud U.S. Army Infantry veteran and security consultant at Black Hills Information Security. Steve has extensive experience as a penetration tester, red team operator, and instructor since 2014. Steve has instructed courses on penetration testing and red teaming for the public, private, and federal law enforcement sectors. Steve also has experience teaching and speaking at conferences such as Blackhat, various BSides events, Gartner, and others. Steve maintains a blog and GitHub repository to share knowledge and open-source offensive tools with the community. Steve earned a B.S. in Computer and Information Science from ECPI University.

Jack Hyland
Jack Hyland started interning with Black Hills Information Security in 2021 while finishing up his bachelor's and master's in cyber-security. Throughout his college career, he worked for a research lab dedicated to studying deep-learning attacks and defenses against popular privacy technologies such as Tor. While working for the lab, his peer-reviewed research was published and presented at an international conference. Jack enjoys participating in CTFs and cyber-security competitions to stay active in the community and was a finalist at the 2022 Collegiate Penetration Testing Competition. He now works as a full-time tester for Black Hills Information Security and specializes in web-application penetration tests. Outside of work, he enjoys rock climbing, snowboarding, and homebrewing IPAs.

Troy Wojewoda, GSE, GRID, GNFA, GCFA, GCIH, GCIA, GREM, GAWN, GSEC, GSEC Gold, CISSP
Troy is a security analyst and penetration tester at Black Hills Information Security. Prior to joining BHIS, Troy has held roles in application and system administration, host and network intrusion detection, wireless security, penetration testing, digital forensics, malware analysis, threat hunting and incident response. In addition to earning several professional certifications, Troy has a BS in Computer Engineering and Computer Science. Troy enjoys writing custom tools and developing novel techniques for testing the security posture of an organization. Away from work, Troy enjoys spending time with his family, camping/hiking in the mountains, homebrewing, woodworking and coaching children in STEM programs.

Hal Denton, Network+, Security+, CEH, GREM, GPEN, GCFA, GNFA, CISSP
Hal Denton joined the Black Hills Information Security (BHIS) team in December 2021. In his role as a Security Analyst, he works DFIR engagements/development, as well as hunting and threat detection creation. Hal started his career over 20 years ago, moving through different roles such as help desk, system admin, security engineer, incident response, digital forensics, malware analysis, threat hunting, threat intel, research, and SOC lead. Hal says, “I love the fact BHIS is trying to provide an easier on-ramp for the next generation of security professionals… to be a part of the family was a no-brainer.” Outside of work, Hal enjoys spending quality time with his family, disconnecting from technology by going backpacking through the woods, and a variety of hobbies such as 3D printing, home improvement, and gardening.

Bradley Konsela
Bradley is a Linux enthusiast, hacker, and musician. He has an academic background in computer science and a professional background in IT and supercomputing cluster system administration. He

joined the BHIS team in 2019. When he isn't testing, he can often be found tinkering with Linux, building and playing synthesizers, and rock climbing with friends.

Chris Traynor, GSEC, GCIH, GWAPT, GPEN
Chris joined Black Hills Information Security (BHIS) in July 2022 as a Penetration Tester, where he is responsible for Pen Testing web apps, APIs, and networks. Chris has over 15 years of experience in Web/Mobile App development, QA Automation, and Penetration Testing. He is also a TA for SEC504, SEC542, SEC560, & SEC580 with the SANS Institute where he is working on becoming an instructor. Chris is an active member of the GIAC Advisory Board, InfraGard, and The Open Organization Of Lockpickers (TOOOL).

Jason Mehlenbacher
Jason Mehlenbacher joined the Black Hills Information Security (BHIS) team in January 2022. As a Penetration Tester, he performs security testing for customers and provides detailed reports of the findings. Previously, Jason worked at Comerica Bank as technical lead for a networking/security team, and before that, he was an IT specialist for the Air Force. Jason was drawn to work at BHIS because of the people and environment; he values the knowledge-sharing community. When he's not working, Jason can be found spending time outdoors, riding his motorcycle, and gaming.

Isaac Burton
Isaac is a penetration tester at Black Hills with 7 years of work experience in various fields including infrastructure, supercomputing, cybersecurity course development, tool creation and ethical hacking. He is proficient in JavaScript, Python and C programming, and specializes in web application and API testing. Isaac enjoys a challenge and is constantly searching for new learning opportunities. Outside of work, he enjoys hardware hacking, video games, going to the gym, and working on his Jeep.

Fernando Panizza, OSCP, OSWE, CRTO
Fernando has been a Penetration Tester at BHIS since March 2022, he has over 8 years of experience in information technology and over 5 in information security working with government and financial organizations. Prior to joining BHIS, Fernando was a security consultant performing penetration testing and incident response. Outside of work he enjoys security challenges, music, video games and martial arts.

Terry Reece, GCFA
Terry is a penetration tester at Black Hills Information Security with 25 years of experience in a broad range of fields within information security. His past experiences include providing incident response and penetration testing services across a wide variety of industries including healthcare, government, retail, non-profit, and financial. Outside of work, Terry enjoys fishing, playing guitar, and spending time with his family.

Phil Miller, OSCP
Phil Miller joined the team at Black Hills Information Security (BHIS) in the spring of 2022 as a Penetration Tester working on web application, external, and internal network testing. Prior to this role, he was an information security associate for an e-commerce B2B company. Phil chose BHIS because of the "the amazing content and fantastic quality of work that they deliver, and it's an awesome group of talented individuals." He loves being on a team with folks who are also passionate about their work. Outside of work, he enjoys the arts (drumming & music, drawing & painting), as well as sports (golfing, bowling, and basketball).

Serena DiPenti
Serena DiPenti joined Black Hills Information Security (BHIS) in April 2022, after previously working as a network engineer at Cisco. As a Security Analyst and Content Creator, she communicates pentester concepts through content. Serena chose to join BHIS because she wanted to be a part of a company that fosters community. She values the flexibility to create what she wants and the opportunity to collaborate with incredibly intelligent people. Outside of work, she can be found biking, creating on TikTok, and trying new hobbies.

Cameron Cartier
Cameron Cartier joined Black Hills Information Security in 2023 as a Penetration Tester. In this role, she hacks things, teaches things, and researches things of all sorts. Cameron loves the friendly collaborative environment; she gets to do cool things with cool people and get paid for it. She is a graduate student researching privacy enhancing technologies. Outside of work, Cameron enjoys jiu-jitsu, gardening, hanging with friends, and adventuring in the mountains.

Kaitlyn Wimberley
Kaitlyn Wimberley joined BHIS in March of 2022 as a SOC Security Analyst. Kaitlyn obtained her Master of Science in Cyber Security from New York University in 2021 with high honors. While at NYU, she worked as a teaching assistant in NYU's Offensive Security course, and served as president of the OSIRIS security lab. Kaitlyn has also earned the Pentest+ and BTL1 certifications. In her spare time, Kaitlyn enjoys the usual things (games, music, and reading), attempting to keep plants alive, and going on adventures with her family.

Kiersten Gross
Kiersten is a security analyst and SOC member. Prior to joining BHIS, he worked as a shop-hand. Kiersten has a BS in Software Development and an MS in Cybersecurity. Away from work, Kiersten enjoys spending time in the mountains with his family.

Dave Hoff
Dave is a Cloud Architect and Systems Administrator at Black Hills Information Security. Prior to joining BHIS, Dave worked in the higher education industry and has worked in incident response, detection engineering, SIEM design and maintenance, threat intelligence, and network security monitoring. Dave earned a BS in Information Systems and enjoys automating his work and sharing his knowledge with others. When he's not working, Dave enjoys building specialized vehicles, playing music, and camping.

Michael Getman
Michael is a SOC analyst at Black Hills Information Security. Prior to joining BHIS, Michael held roles as an enterprise technician and systems administrator. Michael ha a AAS in Network and Systems Administration.

Hayden Covington
Hayden is a security analyst at Black Hills Information Security. Prior to joining BHIS, Hayden worked in the SOC of a naval contractor as a tier 2 analyst, SOAR/SIEM engineer, and the enterprise insider threat lead. In addition, Hayden has also worked in a forensics, administrative, and project management capacity in the past. Hayden has a BS in Cybersecurity from Regent University where he served for multiple years as vice president of the university’s student activities board. With a passion for process improvement and automation, Hayden is always on the lookout for ways to optimize processes, freeing up time for more valuable tasks. Outside of work, Hayden enjoys triathlons, motorsports, and tinkering in various other hobbies.