

The background features a dark blue gradient with a subtle pattern of white dots. On the left side, there are several circular elements: a large scale with numerical markings from 140 to 260, and several smaller circles with dashed lines and arrows, suggesting a technical or data-related theme.

# CYBER SECURITY CONSULTANT – SPIDER LABS

JOAS ANTONIO

# DETAILS

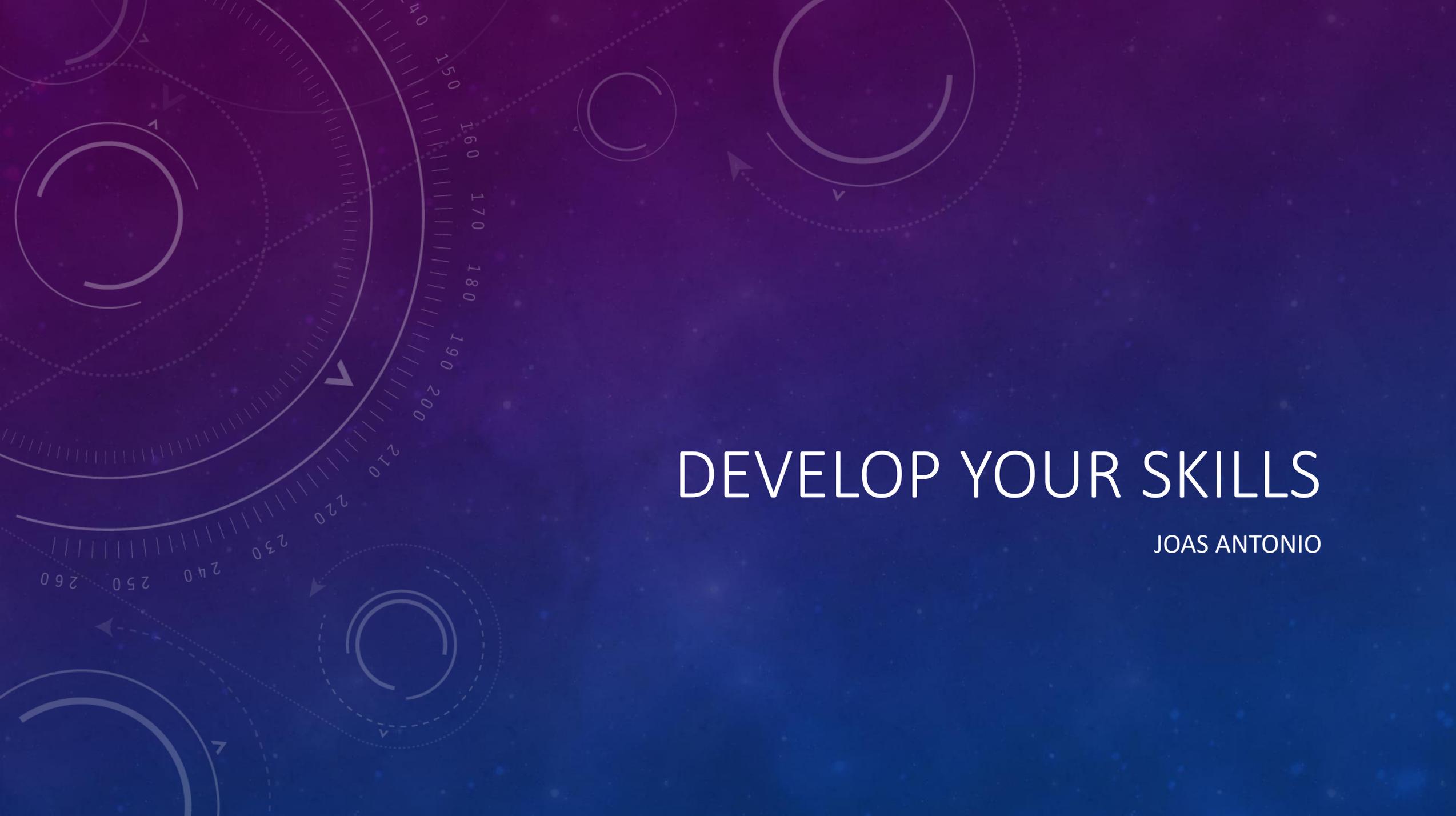
- Fiz esse PDF após ver uma vaga na SpiderLabs sobre Consultor de Segurança com foco mais Ofensivo, claro que não contém todos os detalhes, mas apenas para se ter uma noção, assim como fiz com a vaga que encontrei referente ao time Storms da Intel;
- I made this PDF after seeing a vacancy at SpiderLabs about Security Consultant with a more Offensive focus, of course it doesn't contain all the details, but just to get an idea, as I did with the vacancy I found referring to Intel's Storms time;
- <https://www.linkedin.com/in/joas-antonio-dos-santos>

# RESPONSABILITIES

- Knowledge Application Security and Penetration Testing
- Expected to own and run key customer engagements as directed by their manager
- Perform deep, detailed and advanced security assessments and penetration tests
- Creates organizational knowledge about key technologies, tools, and methodologies
- The candidate will have the opportunity to perform security research involving bug hunting, exploit development, reverse engineering, and cryptography.
- Developing tools and processes to automate and simplify penetration testing.
- The opportunity for more specialized engagements such as red teaming, OSINT, mobile application, and SCADA testing depending on skills and experience.

# SKILLS

- Deep knowledge in Web, IoT, Scada/OT, Network, Wireless, Mobile PenTest;
- Know the main PenTest methodologies;
- Excellent English Language Communication Skills;
- Ability to create and maintain methodologies and process definitions
- Experience developing, delivering and managing large consulting engagements
- Skills in developing tools and exploits
- Knowledge of security in both Linux and Windows environments as it pertains to web application, middleware, database, and identify management platforms.
- Knowledge of TCP/IP networking.
- Knowledge of modern web application technologies and architectures.
-

The background is a dark blue gradient with a subtle pattern of white dots. On the left side, there are several overlapping circular elements. A prominent one is a large circular scale with tick marks and numbers ranging from 140 to 260. Other circles include dashed lines, solid lines, and arrows, suggesting a technical or scientific theme.

# DEVELOP YOUR SKILLS

JOAS ANTONIO

# TCP/IP

- <https://www.ibm.com/docs/en/zos/2.1.0?topic=concepts-tcpip>
- <https://searchnetworking.techtarget.com/definition/TCP-IP>
- <https://www.britannica.com/technology/TCP-IP>
- <https://www.avast.com/c-what-is-tcp-ip>
- <https://www.fortinet.com/resources/cyberglossary/tcp-ip>
- <https://www.bigcommerce.com/ecommerce-answers/what-is-tcp-ip/>
- <https://www.techopedia.com/definition/2460/transmission-control-protocolinternet-protocol-tcpip>
- <https://www.pcmag.com/encyclopedia/term/tcpip>

# WEB PENTEST

- <https://github.com/enaqx/awesome-pentest>
- <https://github.com/infoslack/awesome-web-hacking>
- <https://github.com/arch3rPro/PentestTools>
- <https://github.com/OWASP/wstg>
- <https://github.com/e11i0t4lders0n/Web-Application-Pentest-Checklist>
- <https://drive.google.com/drive/u/0/folders/12Mvq6kE2HJDwN2CZhEGWizyWt87YunkU>

# MOBILE PENTEST

- <https://github.com/tanprathan/MobileApp-Pentest-Cheatsheet>
- <https://github.com/kyawthiha7/Mobile-App-Pentest>
- <https://github.com/vaib25vicky/awesome-mobile-security>
- <https://github.com/OWASP/owasp-mstg>
- <https://github.com/tsug0d/AndroidMobilePentest101>
- <https://github.com/jdonsec/AllThingsAndroid>
- <https://github.com/mirfansulaiman/Command-Mobile-Penetration-Testing-Cheatsheet>

# OT/SCADA PENTEST

- <https://github.com/hslatman/awesome-industrial-control-system-security>
- <https://github.com/reaperb0t/awesome-iot-ics-embed-pentest>
- <https://github.com/ITI/ICS-Security-Tools/blob/master/guides/roblee.md>
- <https://github.com/dave36/pdt>
- <https://github.com/moki-ics/moki>
- <https://ics-training.inl.gov/learn/mycourses>

# NETWORK PENTEST

- <https://github.com/Muhammd/Awesome-Pentest>
- <https://github.com/enaqx/awesome-pentest>
- <https://github.com/CyberSecurityUP/Powershell-for-PenTest>
- <https://github.com/CyberSecurityUP/Awesome-PenTest-Practice>

# CLOUD PENTEST

- <https://github.com/CyberSecurityUP/Awesome-Cloud-PenTest>
- <https://pentestbook.six2dez.com/enumeration/cloud/gcp>
- <https://securelayer7.net/aws-penetration-testing>
- <https://infosecwriteups.com/deep-dive-into-aws-penetration-testing-a99192a26898>
- <https://asecure.cloud/tools/>
- [https://www.youtube.com/watch?v=IOhvloOWzOg&ab\\_channel=SANSOffensiveOperations](https://www.youtube.com/watch?v=IOhvloOWzOg&ab_channel=SANSOffensiveOperations)
- [https://www.youtube.com/watch?v=fiSJQfiS21c&ab\\_channel=SANSOffensiveOperations](https://www.youtube.com/watch?v=fiSJQfiS21c&ab_channel=SANSOffensiveOperations)
- [https://www.youtube.com/watch?v=aqumgrSBDM4&ab\\_channel=VTFoundation](https://www.youtube.com/watch?v=aqumgrSBDM4&ab_channel=VTFoundation)
- <https://www.netspi.com/security-testing/cloud-penetration-testing/>
- <https://www.guidepointsecurity.com/education-center/cloud-penetration-testing/>

# BINARY EXPLOITATION

- [https://www.youtube.com/watch?v=tMN5N5oid2c&ab\\_channel=JohnHammond](https://www.youtube.com/watch?v=tMN5N5oid2c&ab_channel=JohnHammond)
- [https://www.youtube.com/watch?v=i5-cWI\\_HV8o&ab\\_channel=JohnHammond](https://www.youtube.com/watch?v=i5-cWI_HV8o&ab_channel=JohnHammond)
- [https://www.youtube.com/watch?v=gxU3e7GbC-M&ab\\_channel=SourceMeetsSink](https://www.youtube.com/watch?v=gxU3e7GbC-M&ab_channel=SourceMeetsSink)
- [https://www.youtube.com/watch?v=WnqOhgl\\_8wA&ab\\_channel=PwnFunction](https://www.youtube.com/watch?v=WnqOhgl_8wA&ab_channel=PwnFunction)
- <https://trailofbits.github.io/ctf/exploits/binary1.html>
- [https://www.youtube.com/watch?v=72GShSHsRZI&ab\\_channel=PinkDraconian](https://www.youtube.com/watch?v=72GShSHsRZI&ab_channel=PinkDraconian)
- [https://www.youtube.com/watch?v=Hp\\_YVg5QFEw&ab\\_channel=AmritaInCTFJunior](https://www.youtube.com/watch?v=Hp_YVg5QFEw&ab_channel=AmritaInCTFJunior)
- <https://github.com/r0hi7/BinExp>

# REVERSE ENGINEERING

- <https://github.com/CyberSecurityUP/Awesome-Malware-Analysis-Reverse-Engineering>
- <https://github.com/tylerha97/awesome-reversing>
- <https://github.com/ReversingID/Awesome-Reversing>

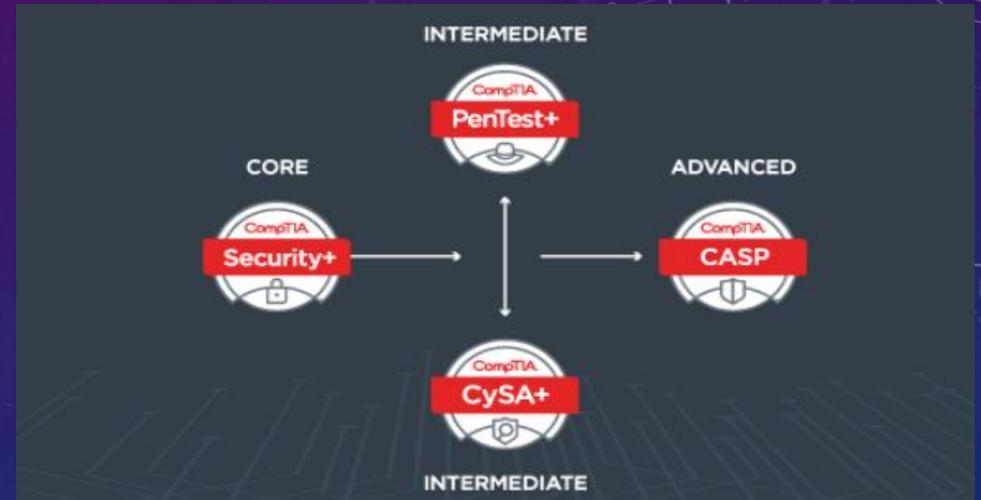
# RED TEAM

- <https://github.com/yeyintminthuhtut/Awesome-Red-Teaming>
- <https://github.com/infosecn1nja/Red-Teaming-Toolkit>
- <https://github.com/CyberSecurityUP/Awesome-Red-Team-Operations>
- <https://github.com/CyberSecurityUP/Cracking-The-Perimeter-Framework>

# PROGRAMMING LANGUAGE

- <https://www.learnpython.org/>
- <https://www.coursera.org/courses?query=python>
- <https://medium.com/swlh/5-free-python-courses-for-beginners-to-learn-online-e1ca90687caf>
- <https://www.udemy.com/topic/python/free/>
- <https://www.pluralsight.com/courses/c-programming-language-in-action>
- [https://www.youtube.com/watch?v=KJgsSFOSQv0&ab\\_channel=freeCodeCamp.org](https://www.youtube.com/watch?v=KJgsSFOSQv0&ab_channel=freeCodeCamp.org)
- [https://www.youtube.com/watch?v=Bz4MxDeEM6k&ab\\_channel=CalebCurry](https://www.youtube.com/watch?v=Bz4MxDeEM6k&ab_channel=CalebCurry)
- <https://www.udemy.com/topic/c-programming/>
- <https://www.edx.org/learn/c-programming>
- <https://medium.com/javarevisited/9-free-c-programming-courses-for-beginners-2486dff74065>
- <https://www.douglashollis.com/best-assembly-language-course-training-class-tutorial-certification-online/>
- <https://www.udemy.com/topic/assembly-language/>
- <https://siit.co/courses/assembly-language-course-and-certification/989>
- <https://githubmemory.com/repo/Binject/awesome-go-security>

# CERTIFICATIONS



CRTP



CRTE



CARTP



PACES

# CERTIFICATIONS

