OTCEP
2023
OPERATIONAL TECHNOLOGY CYBERSECURITY EXPERT PANEL FORUM 2023

CSA SINGAPORE | SG Passion Made Possible

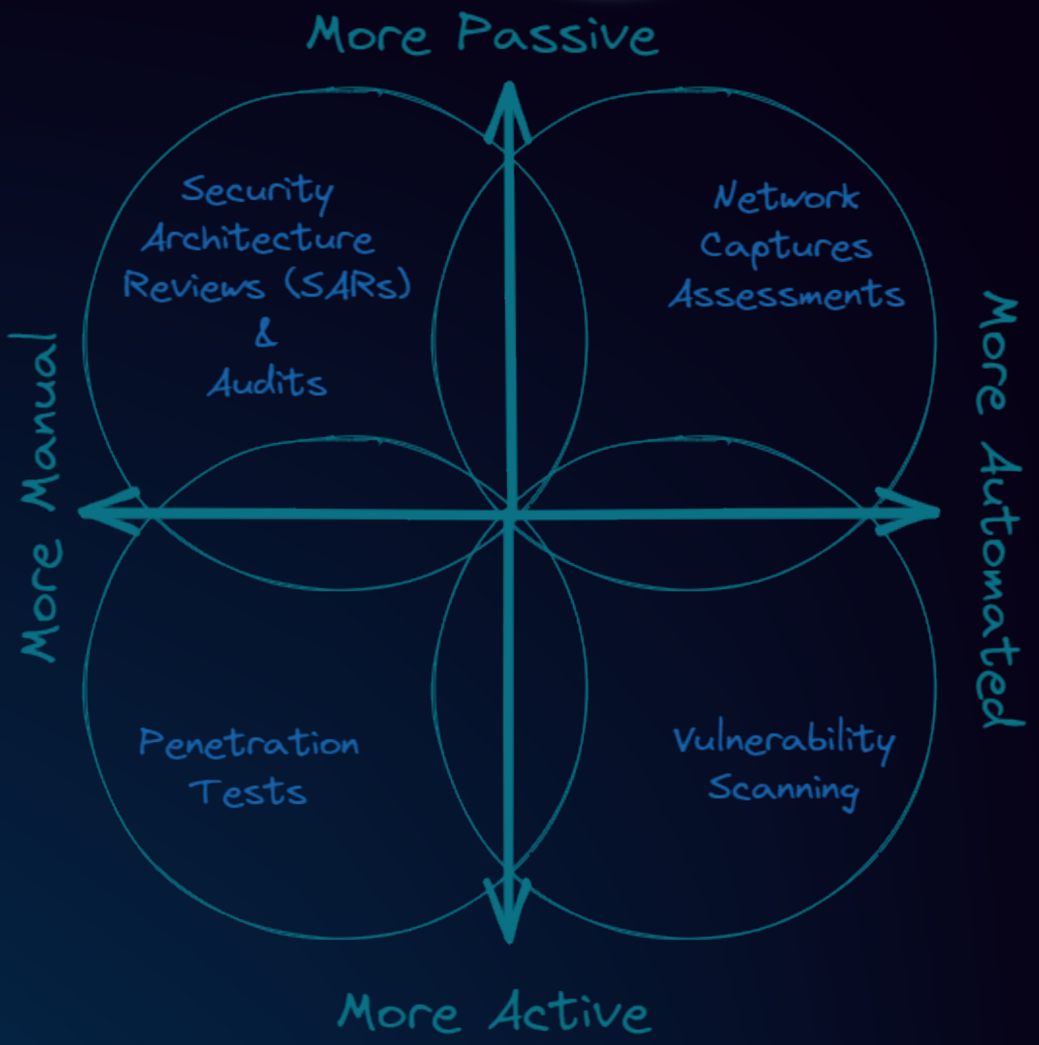
OPERATIONAL TECHNOLOGY CYBERSECURITY EXPERT PANEL FORUM 2023

22 – 23 AUGUST 2023

A Pragmatic Approach to Conduct OT Penetration Testing

Types of Security Assessments

- We can perform many different types of security assessments
  - Discover vulnerabilities in our systems and components
  - Weaknesses in our defenses
- Each assessment type uses a different perspective or set of facts
  - Human understanding via interviews
  - Documentation from the vendor or administrator
  - Configurations from the systems
  - Communication interfaces
- All types should be performed to gain a more complete picture
  - Some vulnerabilities might only be found using one type
  - Some tests increase system risk for increased visibility
  - Each type can be adapted to the system and company needs



What is a Penetration Test?

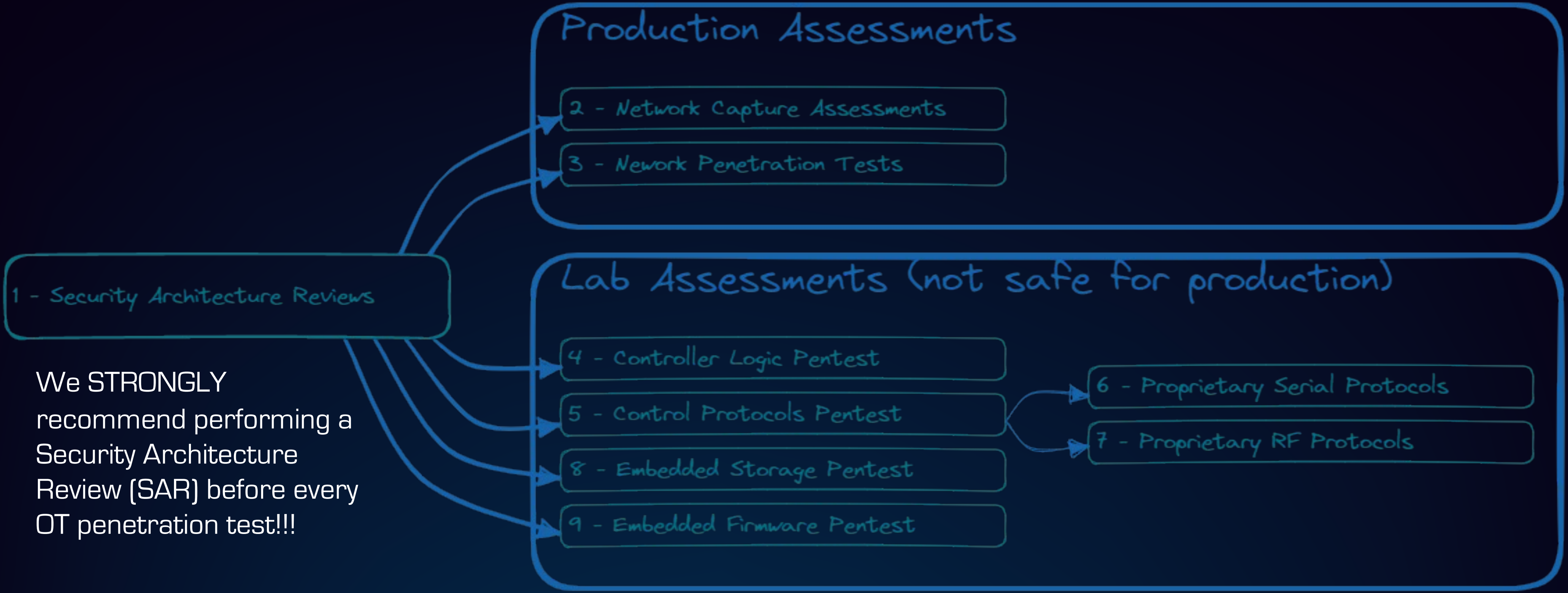
- Penetration testing is a unique form of security assessment
  - Uses the same tools and techniques attackers use to attack our systems
  - Validates the existence of vulnerabilities through exploitation

- Penetration testing benefits
  - Looks at components as an interconnected whole
  - Tests security defenses' effectiveness both in and around the target
  - Avoids assumptions and tests actual functionality
  - Measures a more realistic level of risk through exploitation
  - Discovers second and third layers of vulnerabilities

- Should be performed as a Grey-box or Crystal-box assessment for optimization
  - Provided with knowledge the attackers don't have
  - Access to administrative interfaces to aid in testing (if not in scope for testing)
  - Tests will still be performed with black-box testing tools

OPERATIONAL TECHNOLOGY CYBERSECURITY EXPERT PANEL FORUM 2023

ControlThings OT Penetration Testing Methodology


Production Assessments
2 - Network Capture Assessments
3 - Nework Penetration Tests
1 - Security Architecture Reviews
Lab Assessments (not safe for production)
4 - Controller Logic Pentest
5 - Control Protocols Pentest
6 - Proprietary Serial Protocols
7 - Proprietary RF Protocols
8 - Embedded Storage Pentest
9 - Embedded Firmware Pentest

We STRONGLY recommend performing a Security Architecture Review (SAR) before every OT penetration test!!!

More information can be found at https://www.controlthings.io

What is a Security Architecture Review (SAR)?

- A security architecture review (SAR)
  - Think pen-and-paper penetration test
  - Performed through interviews with personnel
  - Reviews network diagrams and asset inventories
  - Could include configuration review to clarify questions
  - Identifying actual and potential weaknesses in defenses

- A SAR is not an audit. What is an audit?
  - Big sheet of checkboxes for internal and/or external use
  - Often tied to regulation/guidance like NERC CIP or IEC 62443
  - Focuses on mid-level details of controls and programs
  - Often doesn't look at the network/system holistically

More on SARs

- Benefits of a SAR
  - Can be measured in days, not weeks
  - Focuses on high-likelihood and high-impact risks
  - Can be a stand-alone task for clients to help give them higher-level direction

- SARs should ALWAYS be performed before lower-level ICS assessments
  - Helps identify additional risks to your company, staff, and clients
  - Refines scoping and tools needed
  - Provides tasks and prioritization those tasks

- A SAR is going in with eyes wide open before taking any risks

OPERATIONAL TECHNOLOGY CYBERSECURITY EXPERT PANEL FORUM 2023

Common OT Network Penetration Tests

- On the IT/OT perimeter
  - Remote access from the Internet into the ICS networks
  - Connectivity from corporate/business networks to ICS networks
  - Public links carrying ICS traffic across public networks like the Internet
  - Semi-public / semi-private links such as MPLS, Cellular, satellite, etc…

- In OT testing and staging environments
  - New systems or devices in test labs before they are implemented
  - Any system changes or updates that are being tested in test or staging environments

- Should we do penetration testing on the production OT network itself?
  - Maybe. The risk might be too significant.

Penetration Tests in Production OT Networks

- Where risk is low, limited penetration testing should be considered
  - Testing only while processes are idle
  - Only exploit IT technologies inside the OT environment
  - Avoid interacting with any control protocol unless necessary
  - Focus on testing access to ICS components and interfaces
- To further decrease the risk
  - Know what equipment is in the subnets you are working with before starting
  - Test single systems slowly with engineers and operators on hand
  - Be VERY aware of your tools and what actions they perform
  - Avoid any problematic actions and NEVER perform risky actions
- Why even consider it?
  - Attackers attack production, not testing
  - Testing and staging environments may not exist
  - Testing and staging environments do not often have same security controls or configs

Penetration Testing Scope

- Determine the scope of the assessment
  - Multiple sites and connectivity between
  - A single site
  - One or more network segments
  - Single solution (field devices + controllers + servers)
    - Are there higher-level supervisory systems you need to do the testing?
  - Individual components of a solution
    - Are there other components in the solution you need to do the testing?

- Expect sliding project windows due to delays in
  - Purchasing process
  - Signing of contracts (vendor <-> asset owner <-> you)
  - Shipping of equipment (to asset owner and to you)
  - Configuration of equipment (non-trivial)

OPERATIONAL TECHNOLOGY CYBERSECURITY EXPERT PANEL FORUM 2023

Final Thoughts and Recommendations on OT Penetration Tests

- Always do an architecture review and network capture assessment first
  - Get to know the environment and teams first
  - Identifies which systems and networks are more sensitive/dangerous
  - Helps you identify resource needs like skill sets, tools, logistics
  - Refines scoping for a penetration test

- Share notes and reports with the penetration test team
  - Gives them a starting point
  - Allows them to optimize their tests
  - Lets them confirm the findings

- General guidance for the penetration test team
  - Know EXACTLY how each feature in your tools work
  - Always attempt to minimize the number of packets/interactions used
  - Include engineers and be transparent

Questions?

Justin Searle, Director of ICS Security, InGuardians

- Consulting Inquiries: jsearle@inguardians.com
- Training Inquiries: justin@controlthings.io
- Mobile: +1 801 784 2052
- LinkedIn: https://www.linkedin.com/in/meeas
- Website: http://www.controlthings.io

- Related Resources at https://www.controlthings.io/resources
  - Poster - 2020 Control Systems are a Target.pdf
  - Pentest Scoping Spreadsheet for ICS Systems.xltx
  - Scanning Highly Sensitive Networks - v3.pdf
  - Webcast - Dealing with Remote Access to Critical ICS