{S} Saltworks
An Orasi Company

DevSecOpsialidociousx Software Assurance Program

October 2019

Who am I

- 23 years in IT
- 13 years in Enterprise Security
- 10 years Application Security

Who we are

Saltworks is an application security company. We partner with organizations to build world class application security programs.

Why we exist

Obvious industry need for security partners that can provide a holistic end to end approach

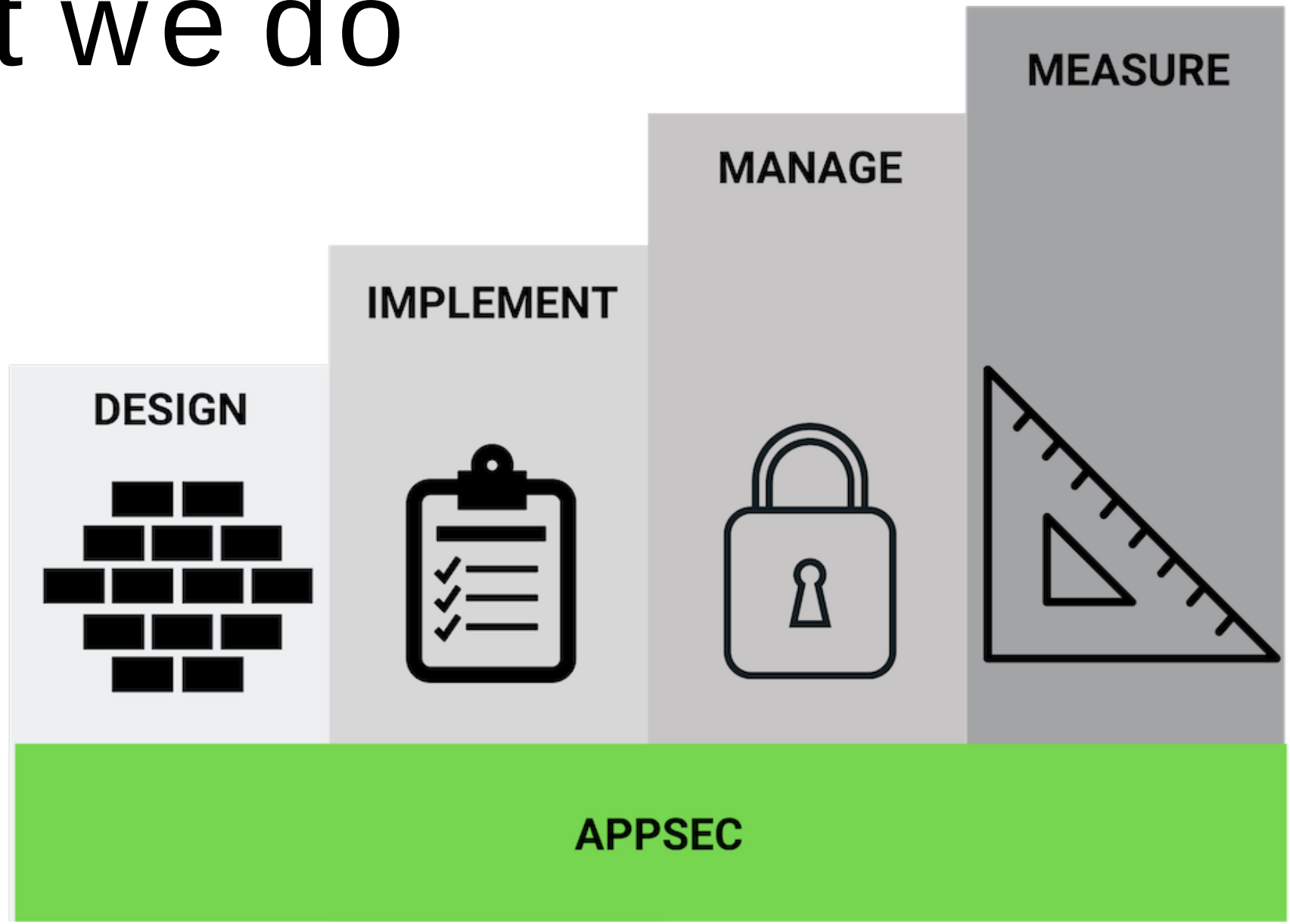
“Policy to Production”

Integrated (Dev & Sec)

Risk-Based App Sec Approach

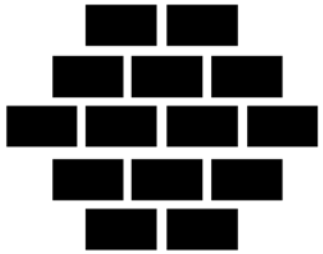
Measurable process

What we do



Design

Application Security that Keeps You Moving at Market Speed



Application security program design must balance the needs of security and business agility, and provide a clear path to releasing software on time and in compliance with corporate and industry standards. Successful programs work with - not against - your established software development culture and environment. We will…

- Study your software production pipeline
- Create a design that works with your established policies and procedures
- Work with your team to clearly articulate security requirements and milestones
- Actively avoid cookie-cutter templates and generic checklists in favor of thoughtful, customized design that meets unique needs

Maturity

- Maturity Assessments and Modeling

Governance & Policy Development

- Defining pre-production security standards
- Establishing governance to create the organizational support needed to ensure these policies are being followed and staying pertinent over time
- Developing both of these elements in the context of your business

Security Planning & Integration

- Reviewing current security activities to identify areas where changes are needed
- Creating new activities/tools and streamlining processes to align with current development procedures
- Working on design and architectural elements as well as coding activities and security testing.

Implement

Everything You Need to Hit the Ground Running

Our team of experts are program acceleration specialists. We will tool your DevOps pipeline to support your customized security plan. Today's market demands won't let software development wait for security to catch up. We have the expertise and experience to take your program from planning to reality quickly, efficiently and predictably.

Integrated Secure Design & Coding Practices

- Implementing customized solutions to seamlessly incorporate security activities across SDLC
- Leveraging automation wherever possible
- Working with a
- Improving security outcomes and minimizing release disruption

Testing & Validation

- Identifying security weaknesses before and after production
- Validating security practices through testing
- Evaluating the effectiveness of security practices

Training & Socialization

- Working closely with your team to train and educate
- Creating initiatives that deliver the right mix of knowledge and skills
- Working closely with developers to support, not impede objectives and workflows

Manage

Expertise where you need it, when you need it

The Saltworks team can help with the day-to-day management and tasks critical to the successful implementation of your customized application security program. We understand your DevOps pipeline and can plug in where and when you need us.

On-Demand Application Security Expertise

- Operating as your development team's application security "help desk," to provide the right mix of expertise
- Standing in to compensate for a shortage of application security professionals and software engineers trained in security
- Either providing help or supplementing your in-house enterprise to execute your application security program

Security Issues Management

As the security extension of your software development team, we will assist with the ongoing management of your application security program including:

- Working with agile teams
- Generating threat models or assisting your internal team in threat model generation
- Ensuring testing activities are being carried out appropriately
- Working with developers on remediation and fix verification
- Scheduling penetration testing

Measure

Metrics that Drive You Forward

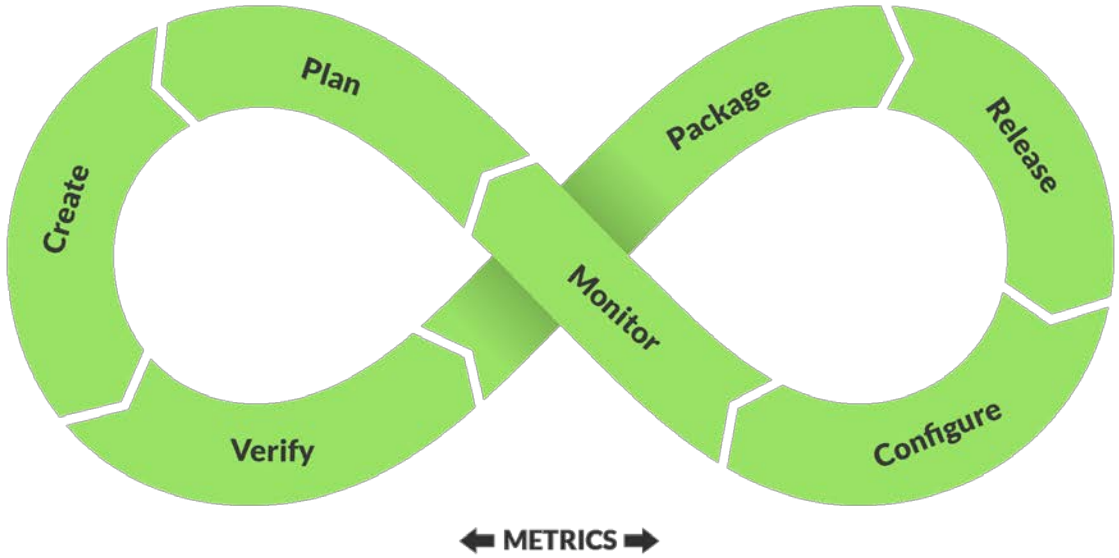
While historical metrics have their place, Saltworks is focused on providing you metrics that help with release decision-making. We'll plug into your DevOps pipeline and pull metrics out to validate the level of security vigor for each release cycle. Our unique measurement approach doesn't just look back, but rather helps drive you forward.

Measurement at Speed

- Setting up and managing an ongoing metrics tracking program to ensure continuous improvement
- Helping you track program implementation and activity verification metrics

We also help you with:

- Providing reporting to audit and compliance teams
- Providing executive-level reports to demonstrate program value
- Reporting vulnerability metrics and identifying key trends



App Sec in “A” DevOps Pipeline

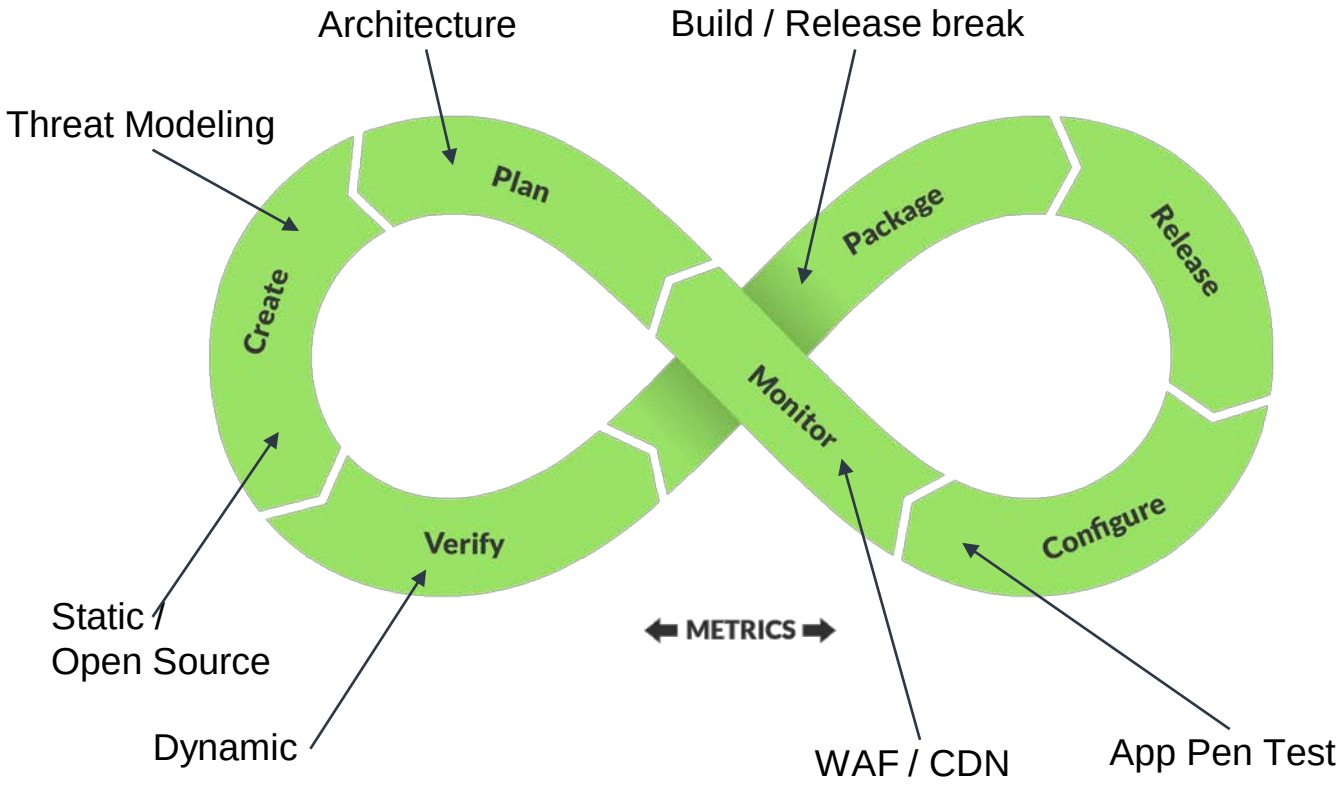
Metrics: Practice and Vulnerabilities focused

Cadence based metrics

- Done periodically, not “in line”
- Architectural review completed
- Threat Model is up to date
- Passing Penetration Testing

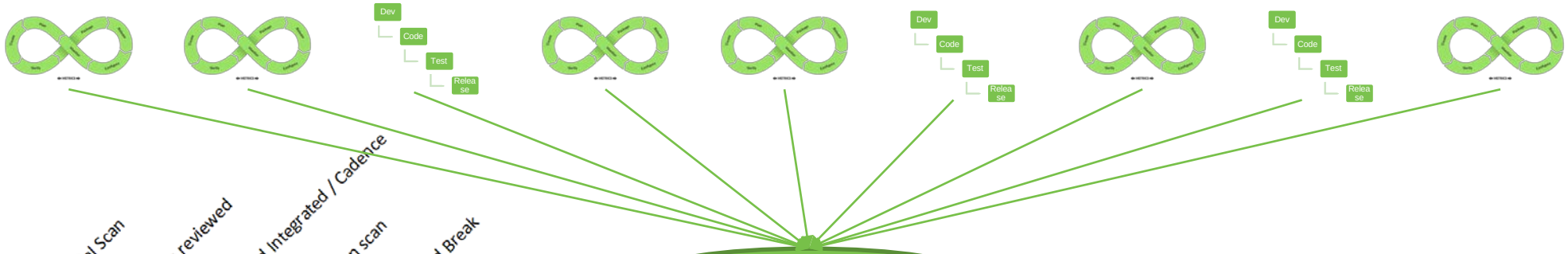
Inline, build break, metrics

- Static results
- Dynamic results
- Open Source results
- WAF events providing feedback on targeted areas



www.saltworks.io

Program (Enterprise) Level View



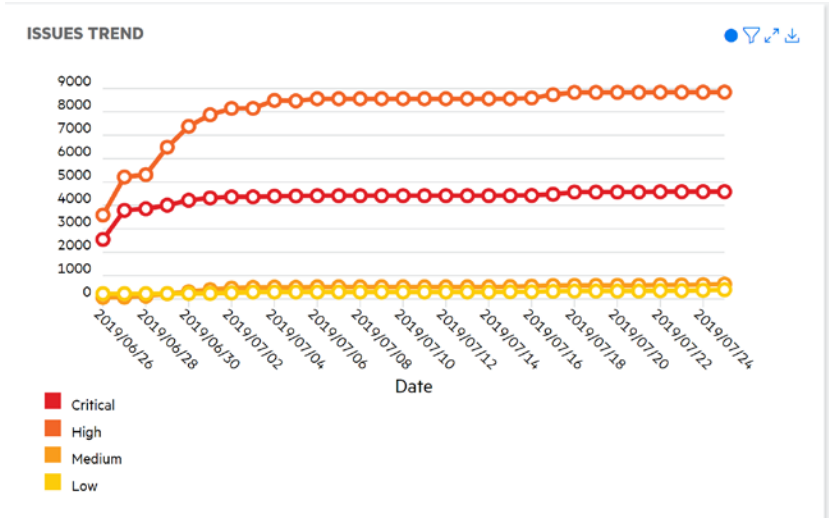
	Initial Scan	Scan reviewed	Build Integrated / Cadence	Clean scan	Build Break
Group 1					
App 1					
App 2					
App 3					
Group 2					
App 4					
App 5					
App 6					
Group 3					
App 7					
App 8					
App 9					

Key

- Activity has been done on cadence w/passing results
- Activity has been done on cadence w/failing results
- Activity not completed on cadence

Program Tracking DB

Metrics



www.saltworks.io

Sec to Dev Program Tracking

Development Teams

Requests for Support

App Onboarding

- Initial Static Scan
- Initial Dynamic San
- Scan Reviews
- Integration
- Build Break support
- Etc..

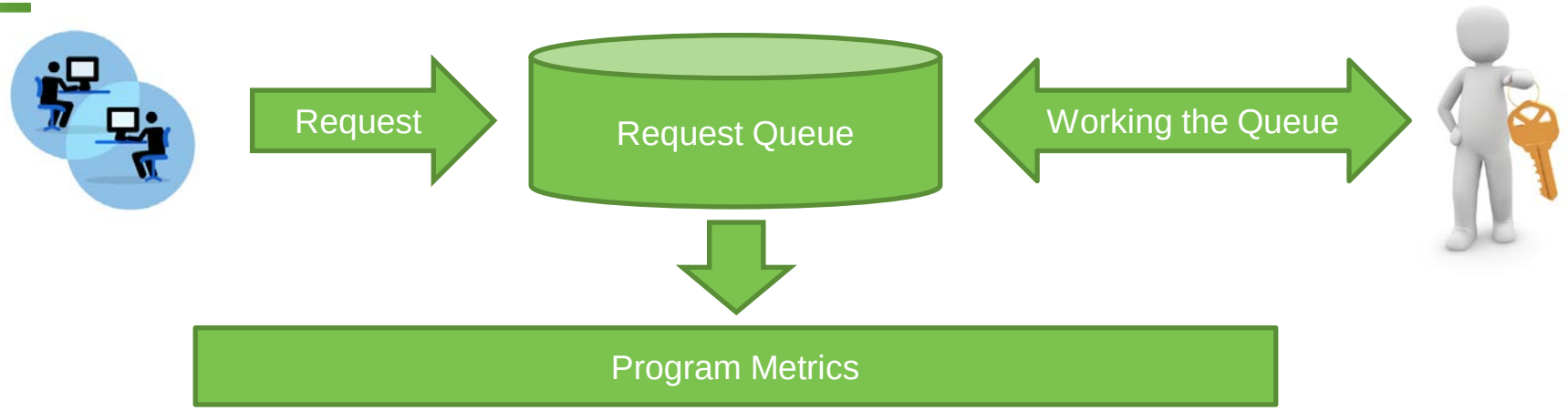
Pen Tests

- Baseline
- Rescan
- Approvals
- Consulting

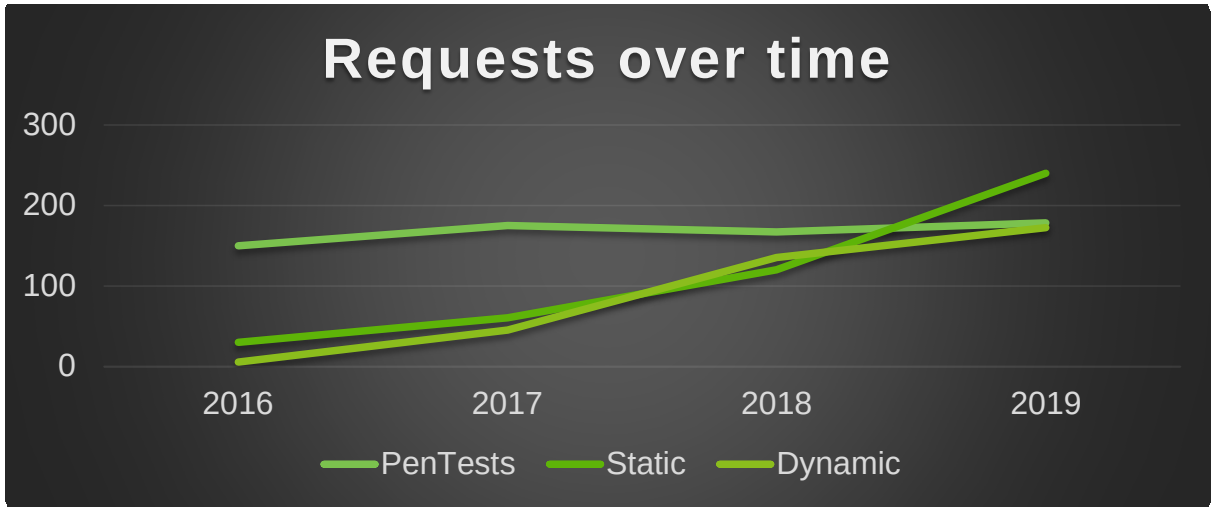
Security Team

www.saltworks.io

Program tracking and performance metrics



Time to service by type	
Scan Review	1 day
Integration	.5 days
Baseline PenTest	10 days
Remediation PenTest	5 days



Program Service request tracking and performance metrics

Thank You

Saltworks Security

@saltworkssec

sales@saltworks.io