Pivot Point
SECURITY

WHAT IS THE BEST WAY TO ENSURE & PROVE YOUR APPLICATION IS SECURE?

OWASP ASVS & SAMM (as perfect a combination as Peanut Butter & Chocolate)

COMPLEXITY IS CRUEL

A10:2017 INSUFFICIENT LOGGING & MONITORING

A2:2017 BROKEN AUTHENTICATION

COMMUNICATION SECURITY

ERROR HANDLING AND LOGGING

ACCESS CONTROL

ARCHITECTURE

A7:2017 CROSS SITE SCRIPTING (XSS)

A4:2017 XML EXTERNAL ENTITIES (XXE)

FILES AND RESOURCES

CRYPTOGRAPHY AT REST

SBOMSSDFNIST

CONFUSED?

SDLC800-218

AUTHENTICATION

SESSION MANAGEMENT

MALICIOUS CODE

CONFIGURATION

A8:2017 INSECURE DESERIALIZATION

APPLICATION SECURITY ASSESSMENT METHOD

BUSINESS LOGIC INPUT VALIDATION WEB SERVICES

A6:2017 SECURITY MISCONFIGURATION

DATA PROTECTION

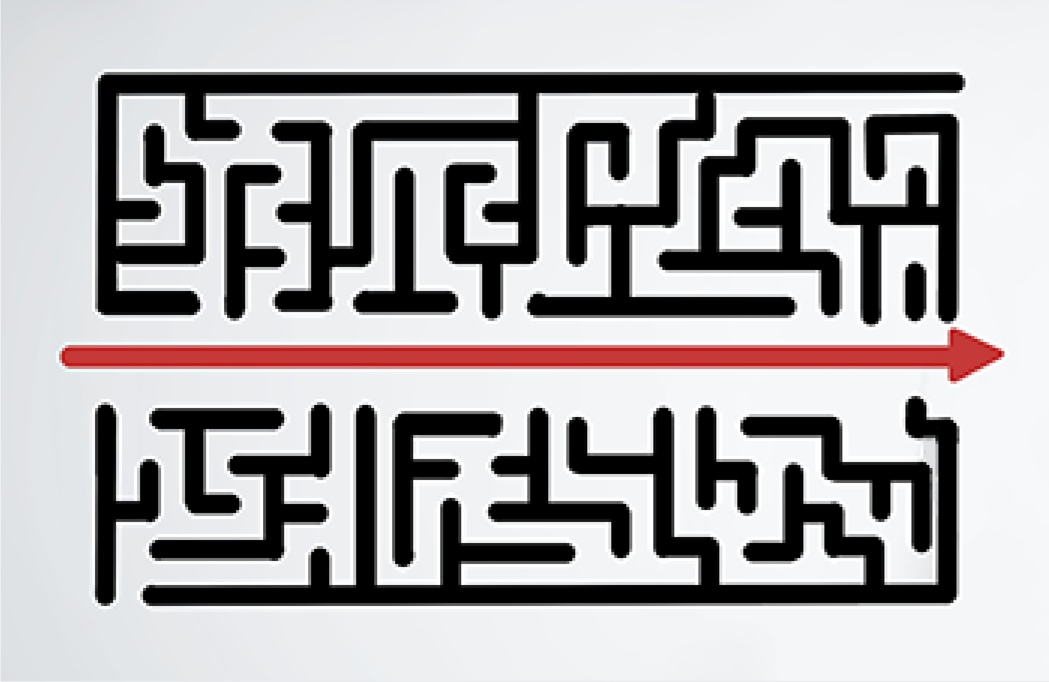
2017 A1:2017INJECTION

A5:2017 BROKEN ACCESS CONTROL

OWASP TOP 10 APPLICATION SECURITY RISKS

A3:2017 SENSITIVE DATA EXPOSURE

SIMPLICITY IS KIND



PIVOT POINT SECURITY IS AN ISO 27001 CERTIFIED & CREST ACCREDITED ORGANIZATION

We align customers with open & trusted frameworks

We have performed hundreds of notable Application Assessments over the last 20 years

OWASP

Open Web Application
Security Project

SINCE 2001, OWASP HAS BEEN THE LEADING SOURCE OF SIMPLE, UNBIASED ADVICE AND PRACTICAL INFORMATION TO HELP DEVELOP APPLICATION SECURITY PROGRAMS

OWASP ASVS

APPLICATION SECURITY VERIFICATION STANDARD

The 286 attributes of a highly secure application

Ensure your development team bakes them into your applications

Use it as testing criteria to validate that the application is secure and prove it to key stakeholders

An ASVS assessment validates and proves that your application is highly secure

```
//fires the appear event when appropriate
var check = function() {
    //is the element hidden?
    if (!t.is(':visible')) {
        //it became hidden
        t.appeared = false;
        return;
    }

    //is the element inside the visible window?
    var a = w.scrollLeft();
    var b = w.scrollTop();
    var o = t.offset();
    var x = o.left;
    var y = o.top;

    var ax = settings.accX;
    var ay = settings.accY;
    var th = t.height();
    var wh = w.height();
    var tw = t.width();
    var ww = w.width();

    if (y + th + ay >= b &&
        y <= b + wh + ay &&
        x + tw + ax >= a &&
        x <= a + ww + ax) {

        //trigger the custom event
        if (!t.appeared) t.trigger('appear', settings.data);

    } else {

        //it scrolled out of view
        t.appeared = false;
    }
};

//create a modified fn with some additional logic
var modifiedFn = function() {

    //mark the element as visible
    t.appeared = true;

    //is this supposed to happen only once?
    if (settings.one) {

        //remove the check
        w.unbind('scroll', check);
        var i = $.inArray(check, $.fn.appear.checks);
        if (i >= 0) $.fn.appear.checks.splice(i, 1);
    }

    //trigger the original fn
    fn.apply(this, arguments);
};

//bind the modified fn to the element
    one) t.one('appear', settings.data, modifiedFn);
     ettings.data, modifiedFn);
```

OWASP ASVS: FOUR WAYS TO PROVE YOUR APP IS SECURE

OWASP "TOP 10"

- Looks for 10 types of vulnerabilities which assesses against ~51 good application security practices
- Application Vulnerability Assessment & Penetration Test
- Per OWASP, "Level 1 is the bare minimum that all applications should strive for."

ASVS 1 - LOW RISK APPS

- Assesses 131 good application security practices
- Application Vulnerability Assessment & Penetration Test
- Sampled Manual Review: Configuration, Logging, Documentation, & Developers

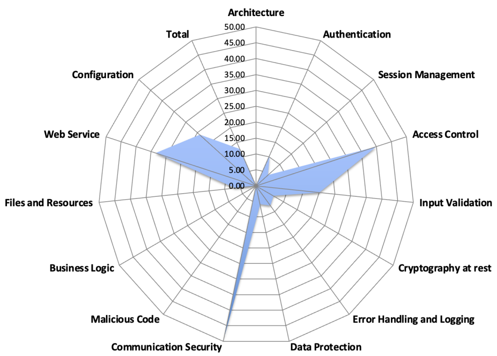
ASVS 2 - MOST APPS

- Assesses 267 good application security practices
- Application Vulnerability Assessment & Penetration Test
- Significant Manual Review: Architecture, Configuration, Logging, Documentation, Developers, & Source Code Analysis

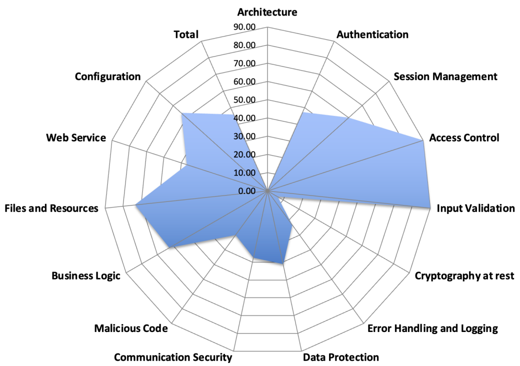
ASVS 3 - HIGH RISK APPS

- Assesses 286 good application security practices
- Application Vulnerability Assessment & Penetration Test
- Complete Manual Review: Architecture, Configuration, Logging, Documentation, Developers, & Thorough Source Code Analysis

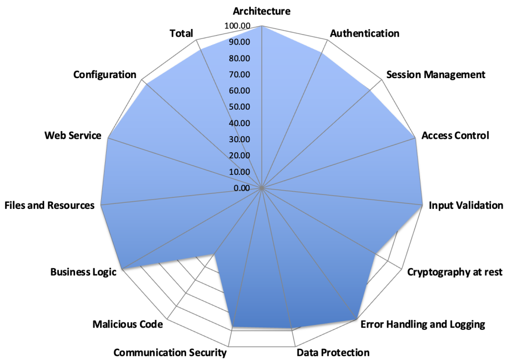
COMPARING OWASP TOP 10 TO ASVS APPLICATION SECURITY DOMAIN COVERAGE



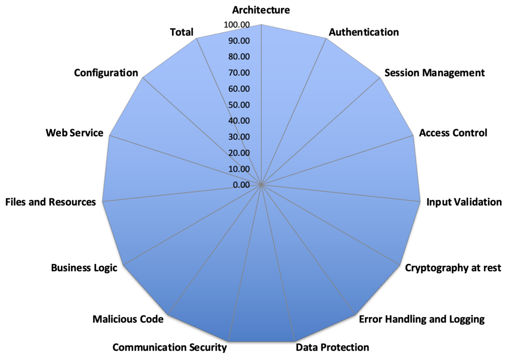
Top 10 Coverage



ASVS L1 Coverage



ASVS L2 Coverage



ASVS L3 Coverage

OWASP SAMM

SOFTWARE ASSURANCE MATURITY MODEL

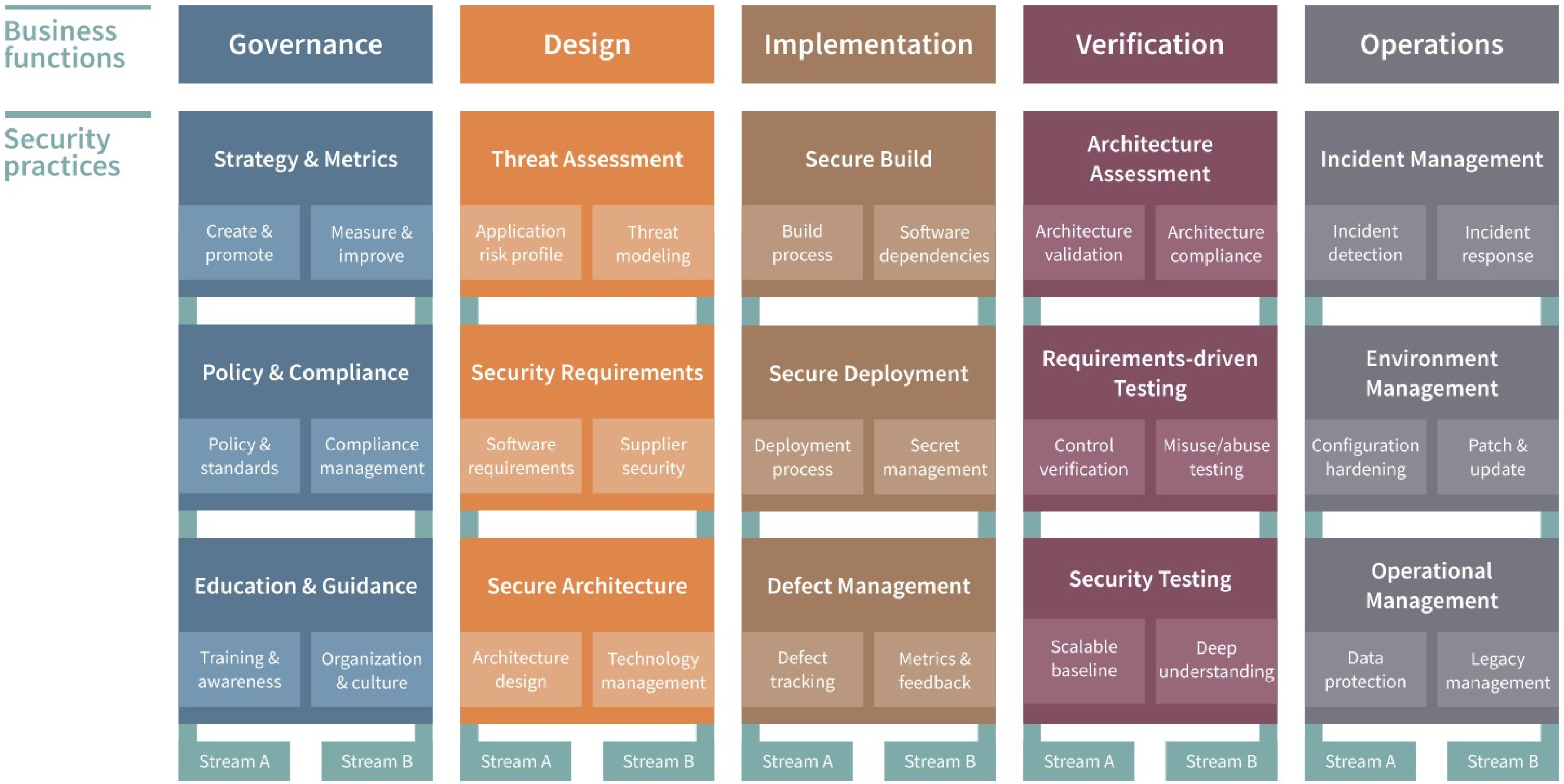
The 90 activities of an optimized Software Development Life Cycle (SDLC)

Give it to your development team to ensure they incorporate the required Governance, Design, Implementation, Verification, & Operational controls into your SDLC to repeatedly produce highly secure applications

Use it as testing criteria to validate that your SDLC process conforms with the US Governments mandate on Application Security (the Secure Software Development Framework (SSDF) (NIST 800-218))

A SAMM assessment validates that your SDLC will consistently produce highly secure applications

OWASP SAMM: 15 DOMAINS FOR COMPREHENSIVE APPLICATION SECURITY



Business functions	Governance	Design	Implementation	Verification	Operations
Security practices	Strategy & Metrics	Threat Assessment	Secure Build	Architecture Assessment	Incident Management
Stream A	Create & promote	Application risk profile	Build process	Architecture validation	Incident detection
Stream B	Measure & improve	Threat modeling	Software dependencies	Architecture compliance	Incident response
	Policy & Compliance	Security Requirements	Secure Deployment	Requirements-driven Testing	Environment Management
Stream A	Policy & standards	Software requirements	Deployment process	Control verification	Configuration hardening
Stream B	Compliance management	Supplier security	Secret management	Misuse/abuse testing	Patch & update
	Education & Guidance	Secure Architecture	Defect Management	Security Testing	Operational Management
Stream A	Training & awareness	Architecture design	Defect tracking	Scalable baseline	Data protection
Stream B	Organization & culture	Technology management	Metrics & feedback	Deep understanding	Legacy management

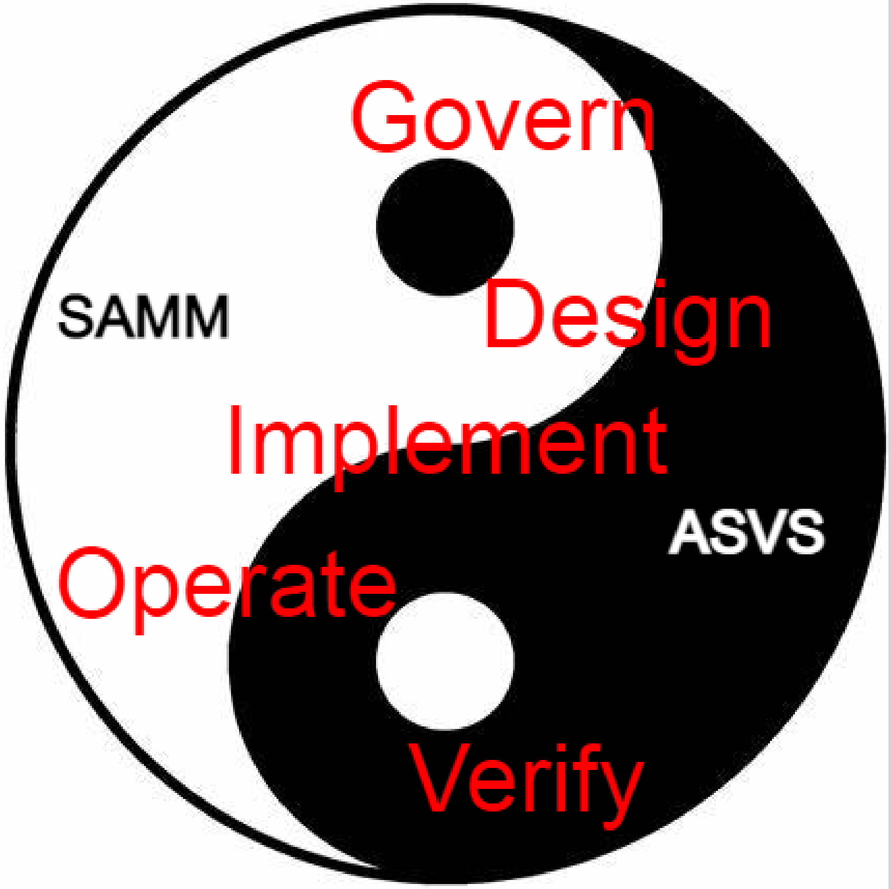
ASVS, SAMM, OR BOTH?

Arguably, they are equally important and ideally coexist and complement each other. Each framework, in turn, provides complementary and prescriptive guidance to ensure that you have the right information at the right time to take the right action to maximize security.

SAMM provides an overarching "recipe" (and some of the ingredients) for developing secure software. ASVS delivers vital ingredients to SAMM.

SAMM & ASVS are essential to fundamental security maxims like "Secure by Design" and "Shift Left Security," as well as conformance with the NIST Secure Software Development Framework (SSDF).

In short, a SAMM assessment tells you if the design of your SDLC is aligned with good practice and is likely to produce secure and compliant applications. An ASVS assessment validates that the SDLC was followed and effective.



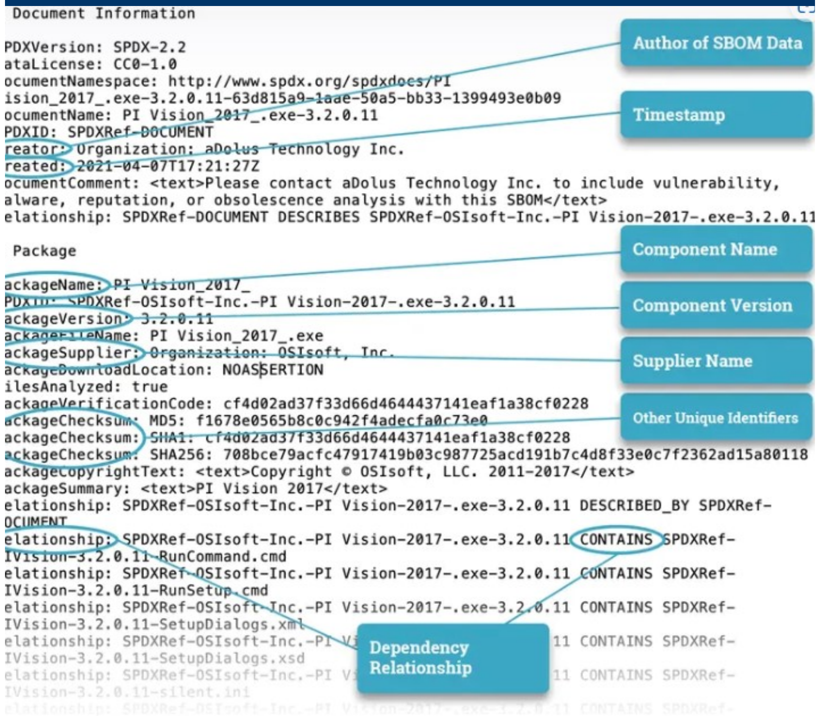
THE NIST SSDF

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

Mandates all software suppliers to the US Federal Government to comply with the NIST Secure Software Development Framework (SSDF).

SSDF focuses on the security of your code AND the code that your code leverages (e.g., your Software Supply Chain). It requires that your SDLC address 19 security practices divided across 42 tasks. The requirement to produce a Software Bill of Materials (SBOM) is how it explicitly covers the Supply Chain risk.

An SBOM is a a formal record containing the details and supply chain relationships of various components used in building software. It allows you, and the recipient, to determine if any of the underlying software components integrated into your code have any vulnerabilities of concern. Ideally you will be able to generate an SBOM in a Software Package Data Exchange (SPDX), Software Identification (SWID) Tagging, or CycloneDX format for automated review by your customer.



```
 Document Information

PDXVersion: SPDX-2.2
ataLicense: CC0-1.0
ocumentNamespace: http://www.spdx.org/spdxdocs/PI
ision_2017_.exe-3.2.0.11-63d815a9-1aae-50a5-bb33-1399493e0b09
ocumentName: PI Vision_2017_.exe-3.2.0.11
PDXID: SPDXRef-DOCUMENT
reator: Organization: aDolus Technology Inc.
reated: 2021-04-07T17:21:27Z
ocumentComment: <text>Please contact aDolus Technology Inc. to include vulnerability,
alware, reputation, or obsolescence analysis with this SBOM</text>
elationship: SPDXRef-DOCUMENT DESCRIBES SPDXRef-OSIsoft-Inc.-PI Vision-2017-.exe-3.2.0.11

 Package

ackageName: PI Vision_2017_
PDXID: SPDXRef-OSIsoft-Inc.-PI Vision-2017-.exe-3.2.0.11
ackageVersion: 3.2.0.11
ackageFileName: PI Vision_2017_.exe
ackageSupplier: Organization: OSIsoft, Inc.
ackageDownloadLocation: NOASSERTION
ilesAnalyzed: true
ackageVerificationCode: cf4d02ad37f33d66d4644437141eaf1a38cf0228
ackageChecksum: MD5: f1678e0565b8c0c942f4adecfa0c73e0
ackageChecksum: SHA1: cf4d02ad37f33d66d4644437141eaf1a38cf0228
ackageChecksum: SHA256: 708bce79acfc47917419b03c987725acd191b7c4d8f33e0c7f2362ad15a80118
ackageCopyrightText: <text>Copyright © OSIsoft, LLC. 2011-2017</text>
ackageSummary: <text>PI Vision 2017</text>
elationship: SPDXRef-OSIsoft-Inc.-PI Vision-2017-.exe-3.2.0.11 DESCRIBED_BY SPDXRef-
OCUMENT
elationship: SPDXRef-OSIsoft-Inc.-PI Vision-2017-.exe-3.2.0.11 CONTAINS SPDXRef-
IVision-3.2.0.11-RunCommand.cmd
elationship: SPDXRef-OSIsoft-Inc.-PI Vision-2017-.exe-3.2.0.11 CONTAINS SPDXRef-
IVision-3.2.0.11-RunSetup.cmd
elationship: SPDXRef-OSIsoft-Inc.-PI Vision-2017-.exe-3.2.0.11 CONTAINS SPDXRef-
IVision-3.2.0.11-SetupDialogs.xml
elationship: SPDXRef-OSIsoft-Inc.-PI Vi                   11 CONTAINS SPDXRef-
IVision-3.2.0.11-SetupDialogs.xsd
elationship: SPDXRef-OSIsoft-Inc.-PI Vi                   11 CONTAINS SPDXRef-
IVision-3.2.0.11-silent.ini
elationship: SPDXRef-OSIsoft-Inc.-PI Vision-2017-.exe-3.2.0.11 CONTAINS SPDXRef-
```

IMAGINE BEING ABLE TO SAY…

To Whom it May Concern,

Our application's security is tighter than a gnats ass and we can prove it (see attached ASVS & SAMM/SSDF reports). We are also fully NIST 800-218/Secure Software Development Framework (SSDF) compliant and have also included a full Software Bill of Materials (SBOM) in a machine readable SPDX format for your review.

Respectfully,
Your New SaaS Provider

____

Pivot Point

SECURITY

ANY QUESTIONS?
REACH OUT!

☎ 609-581-4600

@ info@pivotpointsecurity.com