Pacific Northwest
NATIONAL LABORATORY

Secure Software Central

Threat Based Software Analysis
Secure Software Development

Chance Younkin
Cyber Security Engr, Cyber Security Group, C&A, NSD

VOLTTRON™

Pacific Northwest NATIONAL LABORATORY

Q Does cybersecurity in software matter?

Early 2017
"Smart" Teddy Bear
Computerworld

Spring 2018
Vegas Casino
Business Insider

A Yes! Even in fish tanks and teddy bears it matters!!

Q Should it matter at PNNL?

Fall 2018
VOLTTRON™

A Yes! VOLTTRON™ is widely used, highly visible!!
And they've done something about it!

Pacific Northwest NATIONAL LABORATORY

Is software really where the problem lies?

Gartner

- **75% of security breaches happen at the application**
  - **Not the network layer**
- **Over 70% of vulnerabilities are at the application layer…**
  - **Not the network layer**

NIST National Institute of Standards and Technology U.S. Department of Commerce

- **92% of reported vulnerabilities are in applications not in networks**

Yes! The app is where it's at!!

Pacific Northwest NATIONAL LABORATORY

Q Where in the software lifecycle should cybersecurity be dealt with?

Gartner

- **If only 50% of vulnerabilities were removed prior to production…**

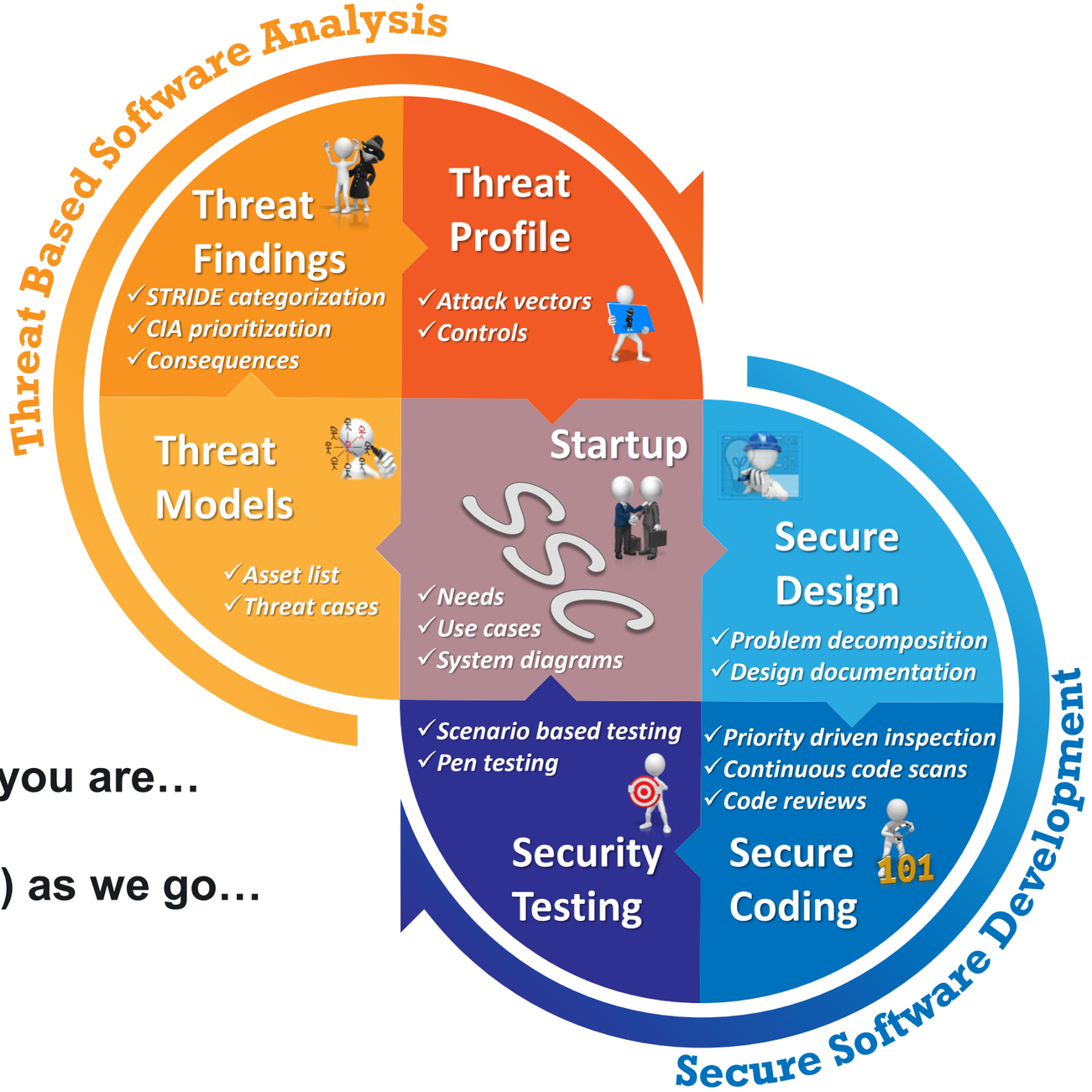
  Costs would be reduced by 75%

NIST National Institute of Standards and Technology U.S. Department of Commerce

- **The cost of fixing a bug in the field: $30,000**
- **The cost of fixing a bug during development: $5,000**

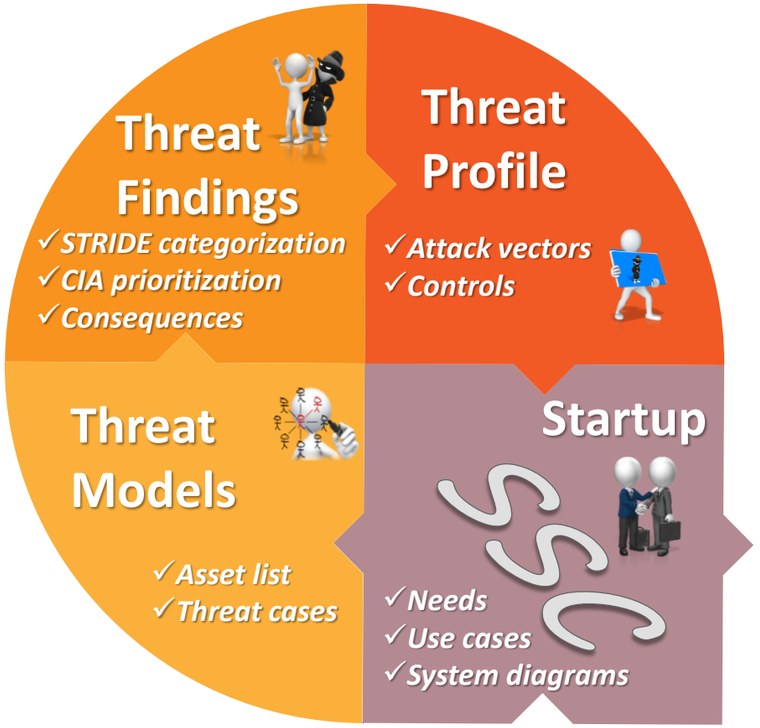
A Everywhere!

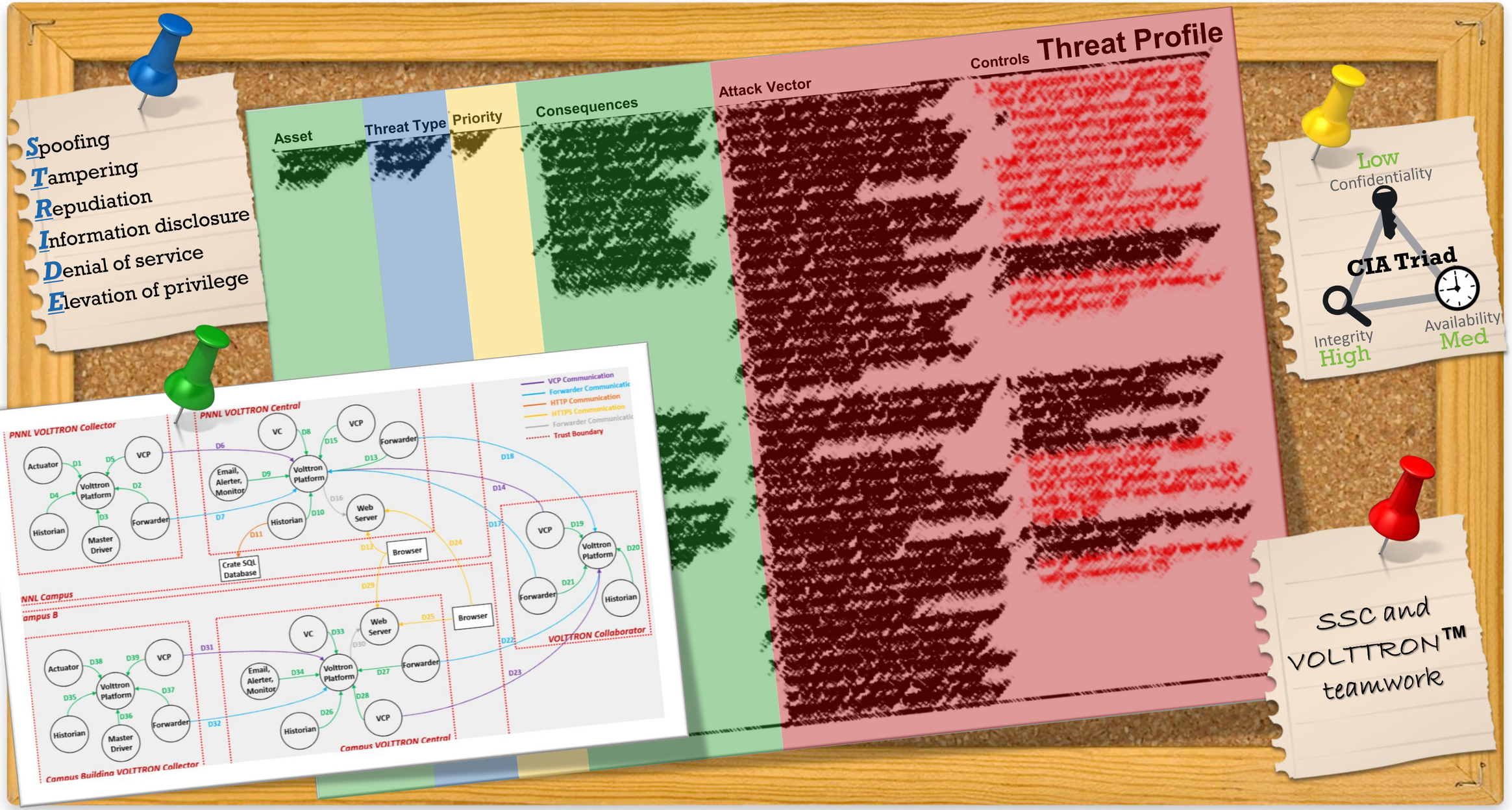
So what is Secure Software Central?



- Meet you where you are…
- In & Out…
- Teach (and learn) as we go…

Pacific Northwest
NATIONAL LABORATORY




Spoofing
Tampering
Repudiation
Information disclosure
Denial of service
Elevation of privilege
Asset
Threat Type
Priority
Consequences
Attack Vector
Controls
Threat Profile
Low
Confidentiality
CIA Triad
Integrity
High
Availability
Med
SSC and VOLTTRON™ teamwork
PNNL VOLTTRON Collector
PNNL VOLTTRON Central
VCP Communication
HTTP Communication
HTTPS Communication
Trust Boundary
Actuator
VCP
Volttron Platform
Historian
Master Driver
Forwarder
VC
Email, Alerter, Monitor
Web Server
Crate SQL Database
Browser
VOLTTRON Collaborator
Campus Building VOLTTRON Collector
Campus VOLTTRON Central

Pacific Northwest
NATIONAL LABORATORY

Startup

- ✓ *Needs*
- ✓ *Use cases*
- ✓ *System diagrams*

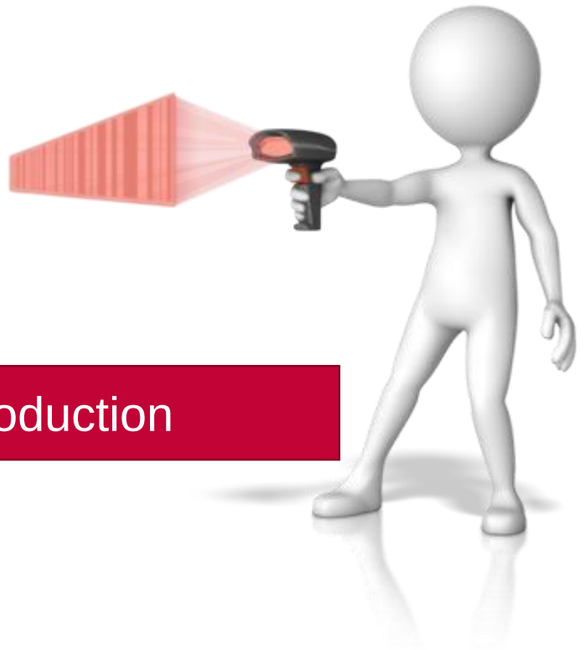
Secure Coding 101

- ✓ *Priority driven inspection*
- ✓ *Continuous code scans*
- ✓ *Code reviews*

Pacific Northwest NATIONAL LABORATORY

Q How was it done?

A Vulnerability scans at the end of testing



Design	Develop	Build	QA/TEST	Production

- “One and Done” scanning mentality.
- Only had a hand full of licenses/resources to use scanning tool.
- Results were handed over to developers without explanation.
- Due to delayed scanning, fixes were harder and took longer.

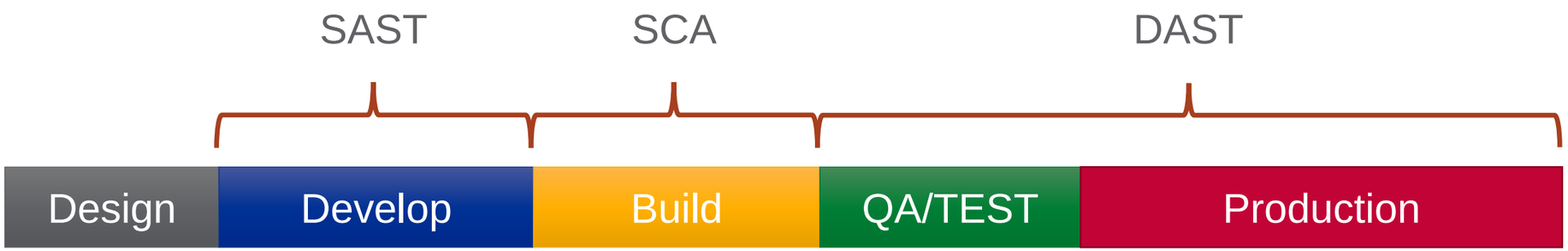
Pacific Northwest NATIONAL LABORATORY

Q How is it done now?

A Throughout the software lifecycle

CHECKMARX

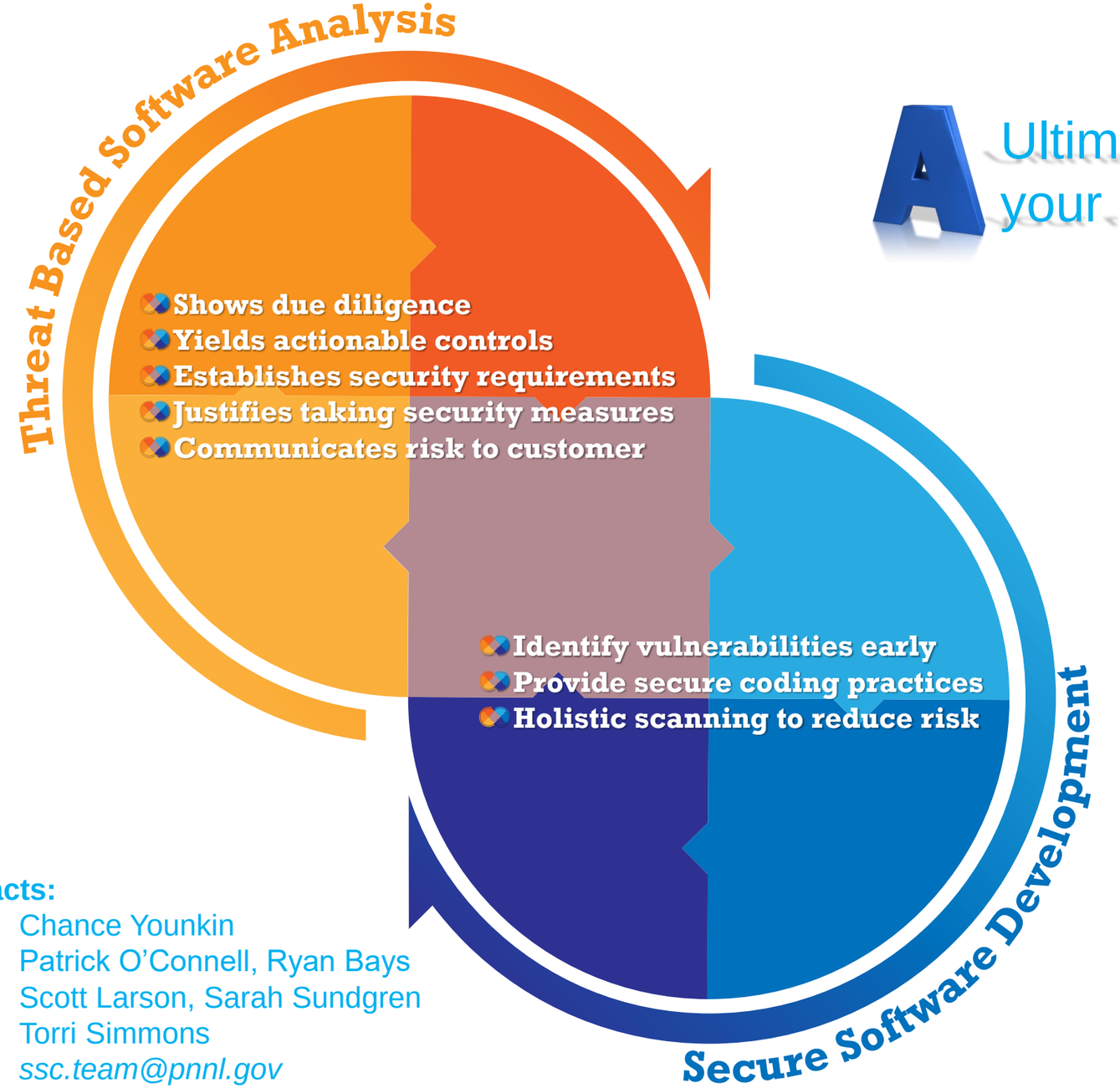
appspider



- SAST – Static Application Security Testing
- SCA – Software Composition Analysis
- DAST – Dynamic Application Security Testing

Pacific Northwest NATIONAL LABORATORY

Q So what is the value?



A Ultimately it protects your reputation!!

Secure Software Central Contacts:

Lead:	Chance Younkin
Threat Based Software Analysis:	Patrick O'Connell, Ryan Bays
Secure Coding/Checkmarx:	Scott Larson, Sarah Sundgren
Administrator/Facilitator	Torri Simmons
All of us:	*ssc.team@pnnl.gov*

Pacific Northwest
NATIONAL LABORATORY

Thank you