Cyber ranges and exercises

*Continuous assessment of talent, teams and tools*

October 21, 2021

11th ANNUAL CONFERENCE: Integrated strategies for cyber talent and technology

Pending inclusion of poll results
(not sure where to put them in terms of the flow)
What is a cyber range?

A virtual environment used for cyber training, software development and testing

ACSC is running three cyber range exercises this year with seven of our lead partner organizations
Example: Cyber Red/Blue exercises for assessing DoD Cyber Protection teams
What’s the issue?

- **People**: Limited use of sophisticated platforms and practices to train and develop cybersecurity defender teams in realistic environments.

- **Process**: Still too many barriers preventing partnerships within and across organizations and between the public and private sector.

- **Technology**: Untapped opportunity to assess new technology tools efficiently and realistically using sophisticated platforms that align to internal environments.

All these challenges lend themselves to collaboration that will accelerate solutions, reduce costs and improve security.
Range-based exercises accelerate innovation, reduce cost and improve security

<table>
<thead>
<tr>
<th>Current Practice</th>
<th>Emerging Practice</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Non-technical tabletop exercises – low technical fidelity</td>
<td>• Range-based training exercises – high technical fidelity – well-suited to</td>
</tr>
<tr>
<td>• Single enterprise, no outside collaboration</td>
<td>emerging cloud environments</td>
</tr>
<tr>
<td>• Limited range marketplace and vendor-specific platforms to assess tools</td>
<td>• Multiple, collaborating enterprises, including state and federal government</td>
</tr>
<tr>
<td>• Few opportunities to develop and assess front-line defensive teams</td>
<td>• Data-driven tool acquisition, integration, assessment</td>
</tr>
<tr>
<td></td>
<td>• Significant value at all levels of the enterprise</td>
</tr>
</tbody>
</table>
Cyber exercises provide significant impact over time

Exercises on ranges provide an opportunity to develop and assess the continuous evolution of people, process and technology.

Emerging model: Developing and assessing SOC staff with metrics and range exercises

Major bank

- Identify individual & team gaps with data
- Mentorship program & training
- Individual exercise opportunities
- Cyber range team exercises
- Reassess and identify new gaps

Framed around a career path for cybersecurity analysts and architects
The ACSC opportunity for collaborative defense
*Cyber ranges in action*

<table>
<thead>
<tr>
<th>People</th>
<th>Parallel play teams</th>
<th>Joint teams</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Individual exercises highlight gaps, track progress and provide peer benchmarks</td>
<td>• Staffs learn from peer organizations</td>
</tr>
<tr>
<td></td>
<td>• Shared takeaways across organizations</td>
<td>• Build peer networks across organizations</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Process</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Internal collaboration across technical and business functions in an organization</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• External collaboration across private and public sectors</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Technology</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Assess new technologies and innovative tools in a secure environment through collaborative sandboxes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Accelerate innovation and reduce costs</td>
<td></td>
</tr>
</tbody>
</table>
Mission:

Collaborative Defense

The region's only non-profit, member-driven, cross-sector organization operating under an NDA and committed to strengthening member cybersecurity defenses, building effective collaboration with the public sector, and preparing the region’s response to large scale cyber threats.

The ACSC is uniquely positioned to ensure our members and the region are national leaders in "Collaborative Defense."
Member organizations and leaders

Abacus Insights – Bill Brown
Brandeis University – David Albrecht

Founding Member & Lead Partner:
Commonwealth of Massachusetts – John Merto

Founding Member & Lead Partner:
Dell Technologies
Everbridge – Sonia Arista
Foley Hoag

Founding Member & Lead Partner:
Federal Reserve Bank of Boston – Anjan Bagchee
Foundation Medicine – Robert Marcotte
Harvard University – Nathan Hall (acting)

Founding Member & Lead Partner:
Liberty Mutual – Katie Jenkins

Founding Member & Lead Partner:
Manulife/John Hancock – Tom Laroche & Greg Thompson

Lead Partner:
MassMutual – Ariel Weintraub
Mimecast – Neil Clauson

Founding Member:
MIT Lincoln Laboratory – Brian McCarthy

Founding Member:
MITRE Corporation – Mick Costa

Lead Partner:
MunichRe – John Schramm & Greg Brinkman

Northeastern University – Harry Hoffman
Point32 Health – Mark Teehan

Lead Partner:
PTC – Eric Hussey
Rapid7 – Tas Giakouminakis

Lead Partner:
Schneider Electric – Patrick Ford

Founding Member & Lead Partner:
State Street Corporation – Liz Joyce
Veracode – Sohail Iqbal
VHB – Greg Bosworth
VMware Carbon Black – Chris Weldon
Thank you to our 2021 conference research partners…

…and our conference sponsors