accenture

Accenture Cybersecurity Forum

Threat & Operations Community

Reducing Supply Chain Risk Through Improved Tradecraft

The Accenture Cybersecurity Forum (ACF) Threat and Operations Community convened a virtual roundtable, "Identifying Supply Chain Risk Through Better Tradecraft: Deploying Risk Identification Approaches, Including Threat Hunting & Simulations to Reduce Supply Chain Risk," on December 7, 2021.

During this roundtable Accenture subject-matter experts joined Community members to share leading supply chain security tradecraft for detecting and responding to cyber attacks and achieving a more secure and resilient supply chain.

The roundtable was conducted under the Chatham House Rule: ACF Threat & Operations Community members are free to use the information shared, provided that neither the identity nor the affiliation of the speakers, nor participants, is revealed.

Below is a brief summary of the call:

No "silver bullet" for supply chain cybersecurity

Community members agreed on the critical importance of protecting the enterprise supply chains, but acknowledged, as one subject-matter expert said, that "No one has entirely solved the challenge of third-party risk yet."

Several factors contribute to the complexity of supply chain cybersecurity, including:

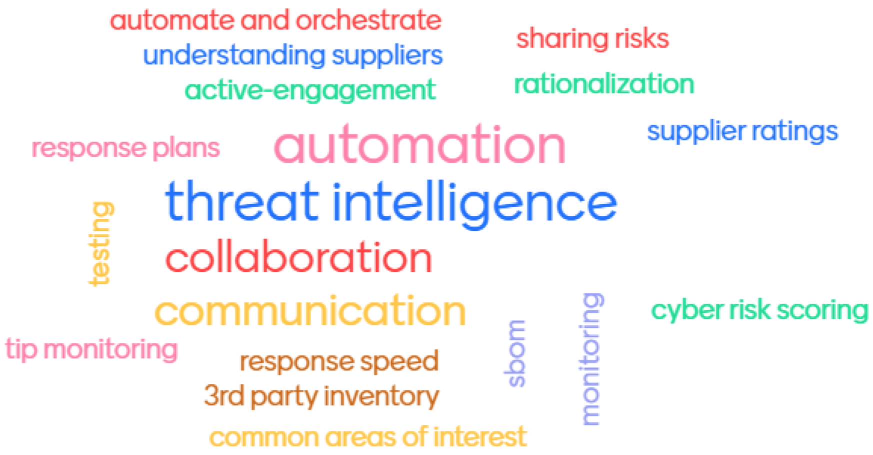
- **A large inventory of third parties**—The proliferation of third parties in an enterprise ecosystem typically increases the attack surface, in part because software purchasers in some functions may not consider security as a critical feature in their purchasing decisions. In addition, smaller third parties might bring innovation to the table, but lack the resources to make cybersecurity a top priority. It can also be difficult to get larger vendors to respond to risk assessment questionnaires or engage in cyber discussions.

- **Lack of transparency into actual security posture**—Information about vendor risk profiles typically resides in multiple silos and can be difficult to compile into actionable insight. Community members endorsed a single-pane-of-glass view into third-party risk, but that goal has not been achieved.
- **The signal/noise ratio of threat intelligence**—While Community members cite the value of threat intelligence in reducing supply chain risk, several also noted the challenge of collecting and analyzing the information that is most relevant to their enterprise and industry.
- **Inadequate threat modeling**—Cybersecurity teams are often stretched too thin to unearth details about the types of threat actors, their tools, risky user behavior, business resiliency and the current state of software architecture.
- **Lack of accountability**—Internally, different functions may not see or appreciate how their unilateral supply chain decisions contribute to enterprise risk. "They need to own the risk," said a Community member. "Collaboration will occur when they are accountable and understand the consequences, including the risks that are outside of their sphere."

  While external third parties may be willing to answer annual risk assessment questionnaires, they may not be forthcoming about their own threat posture for a variety of legal and reputational reasons.

What area of supply chain security tradecraft offers the most promise for reducing supply chain risk?

Community members answered a polling question with a variety of responses but threat intelligence and automation were cited most frequently as having the most promise for reducing supply chain risk.



An opportunity for differentiation

Because many enterprises are third parties in other supply chains, Community members cite the value of cybersecurity as point of market differentiation. “Apple does a good job of this,” said a Community member. Added another, “Cybersecurity is a key element of our value proposition.”

Leading practices in supply chain tradecraft

The group shared the following insights and recommendations:

- **Consider threat modeling**—This can be critical to deconstructing the security challenges presented by third parties. Fresh insights as the supply chain evolves can support more effective remediation.
- **Focus on the most critical assets**—Establish a consistent process for working with the rest of the business in analyzing where to devote limited cybersecurity resources. As a subject-matter expert said: “You can’t be everything for everybody all the time.”
- **Evaluate the “middle ground” of third-party partners**—This is the category of suppliers where enterprises can have the greatest impact in improving supply chain cybersecurity.
- **Assess third-party security posture before signing the contract**—Community members pointed out the risks inherent in the common practice of not addressing cybersecurity concerns upfront. “More preemptive analysis before the contract is signed can avoid a lot of problems,” said a subject-matter expert. Other business functions also need to adopt this mindset, said several Community members.
- **Keep an up-to-date inventory of third parties**—Strive for greater transparency, breaking down the silos of data that make it difficult to create and analyze accurate profiles of third parties in the ecosystem. While several security executives said this is a difficult challenge, it is also an area that could benefit from automation.
- **Reduce the attack surface by rationalizing vendors**—Implement a consistent framework for assessing vendors, including their security posture and potential risks, and that of their own critical supply chain partners.
- **Create a solid architecture**—The fundamentals matter, so keep the playbook up to date. with regular penetration testing, for example. Practice your incident response. Consider a zero-trust access model. Confirm your enterprise’s own risk profile, particularly your tolerance for third-party risks.
- **Engage beyond the annual vendor assessment questionnaire**—Stronger personal relationships can contribute to great cybersecurity, said a subject-matter expert. Conduct conversations with third parties more frequently. Consider establishing a forum where open discussion is encouraged across your supply chain. “It’s for the good of all,” said a Community member.
- **Share intelligence**—A Community member suggested participating in your industry’s ISAC (Information Sharing and Analysis Center), adding that enterprises with robust cybersecurity

capabilities should actively collaborate with their smaller third-party partners—sharing threat intelligence and even helping to fund cyber investments.

On behalf of the Accenture Cybersecurity Forum Threat and Operations Community, we thank our subject matter experts and those of you who were able to join the roundtable for your valuable contributions.

Robert Boyce
Accenture Managing Director—Global Cyber Response & Transformation
Accenture Cybersecurity Forum Threat and Operations Community Host
LinkedIn

About Accenture

Accenture is a global professional services company with leading capabilities in digital, cloud and security. Combining unmatched experience and specialized skills across more than 40 industries, we offer Strategy and Consulting, Interactive, Technology and Operations services — all powered by the world's largest network of Advanced Technology and Intelligent Operations centers. Our 624,000 people deliver on the promise of technology and human ingenuity every day, serving clients in more than 120 countries. We embrace the power of change to create value and shared success for our clients, people, shareholders, partners and communities. Visit us at www.accenture.com.

About Accenture Security

Accenture Security is a leading provider of end-to-end cybersecurity services, including advanced cyber defense, applied cybersecurity solutions and managed security operations. We bring security innovation, coupled with global scale and a worldwide delivery capability through our network of Advanced Technology and Intelligent Operations centers. Helped by our team of highly skilled professionals, we enable clients to innovate safely, build cyber resilience and grow with confidence. Follow us on @AccentureSecure on Twitter or visit us at www.accenture.com/security.

View the entire suite of ACF roundtable summaries on our webpage – here.