Challenges and Opportunities:

Challenges
Enterprise security teams in organizations large and small are pushed to their limits. Delivering support to business initiatives, IT projects and their own security initiatives, all the while continuing to perform operations functions requires a small army. Unfortunately, we’ve never met a CISO that has all the staff they need – there’s always a staff shortage. Further complicating things is the resulting role confusion when staffing levels are sub-optimal. When your team has to both build it and run it, unfortunately the operations function often doesn’t get all the attention it needs.

And staffing isn’t the only complication.

Somewhere between applying patches, identifying vulnerabilities, pushing firewall rules, updating signatures and monitoring the security infrastructure – your operations team has real work to do. Today’s operations teams don’t just wait for malicious operators to make themselves known. Elite analyst hunt teams analyze available threat intelligence and scour logs and systems for signs of infiltration to identify malicious activity and reduce attacker dwell times. These specialized security operations functions require expertise, resources and most of all people.

So with limited staff, an abundance of tools and a steady flood of alerts while facing adaptive adversaries – it’s really no surprise security operations organizations are going through a reinvention period. The job description is no longer “keep the security stuff running” but rather “be the operational nerve center of the cyber security organization.” That’s a tall order that requires an innovative approach.

Key Issue:

It’s Time to Rebalance the Three-Legged Stool: Build vs. Buy vs. Partner

Traditionally, security operations teams were the maintenance part of the plan-build-run trifecta. Someone would design the security mechanism, then others would build it out and hand it off to the security operations team for operation and maintenance. It was the “Steady Eddie” of information security – after the innovation and engineering of the tools and processes was done, this was where they were maintained. Innovation wasn’t a core strength of the security operations team – until recently.

Security operations teams have been busy reinventing the core constructs of their role, fueled by talent shortages and exacerbated by wave after wave of significant breaches. The security operations (sec ops for short) teams have found themselves at the center of a battlefield, with a sudden need to rebalance what they do in-house, what they outsource and what effective partnerships can offer – and the results may surprise you.

Progressive security leaders are throwing away failed traditional models of security operations, such as outsourcing the Security Operations Center (SOC) and performing operational functions including patch management and security infrastructure management through the internal security team. Now, they are replacing these functions with innovative and increasingly effective next generation models. For many security leaders, striking the optimal balance between in-house, outsourced and partnered security operations has become the driving force for innovation, efficiency and effectiveness.
**Opportunities**

The opportunity before us is a chance to reinvent the who and what behind security operations functions. The question of how to rebalance build vs. buy vs. partner for security operations is one of joint investment and operational strategy. How the security leader envisions their role within the enterprise dictates where investments are made. Highly dynamic organizations that require rapid adaptation to market demands and stressors tend to develop partnerships where security operations can continue to be innovative while staying highly flexible and scalable. Because innovation requires significant capital investment, partnerships are rapidly becoming the preferred route.

Developing partnerships is not only for innovation and scale. Leveraging external expertise for advanced functions such as threat hunting or holistic endpoint management allows your limited in-house resources to focus on critical business-focused enterprise tasks, such as developing resilient architectures and innovative, secure products. This approach requires that you provide intelligence to your partner, such as your company’s critical business assets and processes and a baseline for “normal” operations. Otherwise your partner must operate in unfamiliar territory with little likelihood of success. Forming a partnership means that both sides are vested in the mutual success of the relationship. The reasons for developing key partnerships in security operations can be quite compelling if the role of the partner is well-defined and managed.

There is a new trust aspect to the evolution of security operations. Enterprises are moving from their internal resources or “one throat to choke” to a multi-dimensional dependency model. This spans across security controls, advanced analytics and speed to mitigation and remediation.

**The Path Forward:**

For many security organizations, struggling to keep up with the growing demand on their time, the opportunity to scale their operations, increase innovation and focus their internal teams on core business-supporting functions is irresistible. Three key factors will determine how your organization approaches this type of opportunity.

- **Company profile** – The dynamics of the enterprise strongly influence the decision of how to balance security operations. Highly dynamic, agile enterprises will find great value in the ability to scale on-demand (both up and down), and allocate their security resources away from traditionally operational roles. In current market conditions, there is no shortage of companies that are focusing precious security resources on high-value activities like innovation, strategic roles and engineering functions rather than traditional roles such as endpoint management. Instead of spending time on selecting, testing, deploying, managing and maintaining their endpoint tools, these progressive security leaders are passing the entire function of endpoint security to a partner for management. Shedding day-to-day operations functions allows the security staff to focus on high-value activities such as threat hunting to identify attacks and kick out attackers before they can cause serious damage. Though this type of leap requires a great deal of trust, operational rigor and planning, it yields market-moving results.

- **Security role in the enterprise** – The way a company’s structure perceives an enterprise security team bears a significant amount of weight to how the team operates. Where security is perceived to be a low-value, non-strategic activity, (and yes, these situations are still unfortunately common) security will be reduced to an operational role. Patching, managing endpoint and infrastructure security – mostly tactical and management/maintenance activities – become the core function so
there is little internal drive to push that activity outside the company. In situations like this where partnerships develop, they are for low-value activities such as log monitoring and alerting and the traditional “firewall management” type of function.

- **Available resources** – The security job market is absolutely on fire. With dire warnings of “negative unemployment” (more open roles than qualified candidates) it is truly a job-seeker’s market. For companies that require security employees to be located in specific places, hiring can be a challenge. Security operations roles at higher Tier 2 and Tier 3 designations can be challenging to find. More to the point, security operations staff with expertise in specific market niches – for example, industrial controls networks – can be challenging to find just about anywhere. With these headwinds, security leaders who need to fill expertise are turning to their partners for support. Functions such as Cyber Threat Intelligence (CTI) operations analysts may be difficult to hire directly because of the rarity of qualified analysts. In this case, an effective partnership may not only provide the progressive security leader with expertise and scale, but add the benefit of visibility across more than just one specific network attack surface.

---

**Call to Action**

The days of security operations teams viewed as firewall management and alert triage are rapidly disappearing in the rear view mirror. Modern, progressive security leaders are leveraging security operations functions to not only effectively manage their company’s IT risks to tolerance, but are also innovating at the same time. This move into innovation – through partnerships, internal innovative strategies or entirely outsourced functions – is changing the face of enterprise security.

How does your company view its security operations team? Does that team push the boundaries of innovation or have they been operating in the same mode for a decade? Right now is a perfect time to stop, reflect and make a decision to reinvent your security operations function. Talk to Optiv, let us show you how.

---

**Rafal Los**
Managing Director
Solutions Research and Development

**Pat Patterson**
Vice President, Enterprise Security Architecture
Office of the CISO

Optiv is a market-leading provider of end-to-end cyber security solutions. We help clients plan, build and run successful cyber security programs that achieve business objectives through our depth and breadth of cyber security offerings, extensive capabilities and proven expertise in cyber security strategy, managed security services, incident response, risk and compliance, security consulting, training and support, integration and architecture services, and security technology. Optiv maintains premium partnerships with more than 350 of the leading security technology manufacturers. For more information, visit www.optiv.com or follow us at www.twitter.com/optiv, www.facebook.com/optivinc and www.linkedin.com/company/optiv-inc.

© 2017 Optiv Security Inc. All Rights Reserved.
1125 17th Street, Suite 1700 | Denver, CO 80202 | 800.574.0896 | www.optiv.com