COMCAST BUSINESS | MASERGY

WHAT YOU'LL LEARN

- Average salaries and costs
- The biggest threat to ROI
- Trends impacting TCO

E - GUIDE

Build or buy? Eight factors for measuring TCO on security operations centers

When it comes to security operations, most enterprises need to intensify their efforts with 24/7 threat detection and response, but what's the best approach? Is it more effective to expand your existing in-house resources or should you trust a provider to do the work? Analyzing the total cost of staffing a security operations center (SOC) can help you arrive at the right decision. Here are eight cost factors and some key trends to keep in mind as you decide if the do-it-yourself approach is best suited to strengthen your security posture.

Blurred borders call for scalability

With trends in edge computing, mobility, bringyour-own device, and IoT connected devices, the network is becoming an ever-expanding entity. Much like urban sprawl, these blurred borders create an increasing amount of "ground" that SOC teams must cover. The takeaway: The SOC's must be as fluid and adaptable as the extensive IT environment.

Human intelligence still critical

Today, there is a dizzying array of security products that claim to automate the collection, correlation, and analysis of everything happening on your network. While advancements in security technologies are taking us to new heights, these products still require a certain level of human effort to work as advertised.

More than a marginal level of significance, talent can be as much as 50 percent of the success equation:

- Machine learning and artificial intelligence is good at spotting anomalous behavior, but it still requires security analysts to investigate all of its findings.
- The cloud's shared security model is taking some security pressure off of SOC employees, but enterprises that have migrated infrastructure, platforms, and apps to the cloud do not shed all security responsibilities. Cloud-first enterprises must still ingest and evaluate security data. Plus, they must verify that the cloud provider is doing their job correctly.

ROI threat: skills shortage

The biggest problem with security operations is finding and keeping skilled security professionals.

- According to a Ponemon Institute study, 57% of companies are unable to hire the appropriate staff to deal with cyber attacks. A Global Information Security Workforce (GISW) Study found that two-thirds of its nearly 20,000 respondents said they lack the cybersecurity professionals needed for today's threat climate.
- Even with salary and budget increases, some estimates state there will be as many as 3.5 million unfilled positions in the industry by 2021.

Eight factors for measuring TCO

To arrive at an estimated total cost of ownership (TCO), CISOs should perform a cost analysis that accounts for SOC:

1. Staffing: Salaries for tier-1 talent can be estimated at $75-90,000/yr, tier-2 $80-110,000/yr
2. Time-to-Hire: time needed to recruit experienced talent
3. Tenure/Retention: average <12-15 months for a security analyst
4. Coverage (hours of service per day): 4 to 4.5 analysts required for 24/7 coverage
5. Training and Security Certifications: average training costs for tier-1 about $16,000
6. Technology: tools including behavior analytics and cloud protections
7. Threat intelligence subscription
8. Compliance auditing and reporting

When the average SOC requires at least eight employees, it's not uncommon for SOC costs to quickly rise above $100,000+ each month and be contrasted by service contracts that can start at a few thousand dollars monthly. The savings justification typically comes from the fact that staffing, time-to-hire, training, security certifications, 24/7/365 coverage, and tenured professionals are considered non-issues with the right partner. Plus, technologies, compliance, and threat intelligence are often included in the monthly service.

While many IT executives find it easy to build a financial case, the key is getting the most scalability and the best talent for your dollar. First, focus on flexible solutions that make it easy to activate and integrate only the security technologies you need to strategically fill gaps. Second, take a close look at the tenure of security analysts and professionals your partner brings to the table, as talent remains a large part of the job.