6 PRACTICES IT OPERATIONS CAN LEARN FROM ENTERPRISE SECURITY

Introduction

At this point, most IT leaders have realized that security must be integrated into every aspect of the organization. No longer can we leave risk management to a separate group that works in isolation from the rest of the IT groups. Nor can security be an afterthought. In my experience, the best way to get two teams more tightly integrated is to have them work on projects in which the team lines are blurred or erased entirely. By applying some of the practices in the security team, IT operations can gain a better understanding of what they do and how more tightly integrate their work with Security.

Event Correlation

Early in my career as a server administrator, I looked at logs when there was a need to. If something was not working right or there was a performance issue, I'd dig through the log on the affected server. Sometimes I'd discover something useful, other times I'd just find obscure references to support articles that no longer existed.

Every security team I have ever worked with seems to be obsessed with centralizing logs. I never really truly appreciated the reasoning behind this until I was forced to centralize logging by policy. Have you ever wondered how the security team knows about a compromise before it affects your

servers? It's because they've been aggregating logs from firewalls, switches, and Intrusion Detection Systems for years. The security team has become an expert at looking at data across devices and assembling that data into knowledge about what is going on in the environment.

You might say, "I've been doing that for years." I know exactly what is going on with the servers I'm responsible for. Most operations staff are familiar with the component of the operation that they are responsible for. Are you leveraging the operational data contained across the entire environment? Can you look at that data in multiple dimensions? Can you look at all the database servers in one view? Can you then change perspective and correlate all the events across the application stack to simulate customer experience? If not, explore your toolset and reach out to the CISO. Chances are you will find an opportunity to collaborate.

Incident Response Plans

Does your operations team know how to respond to the unknown, when it's not a full disaster? Are there procedures in place to connect all the right people to ensure prompt resolution to issues? More importantly, have your response (not disaster) plans been tested?

One of the most important functions of the security team is to be prepared for security incidents. Every team I have worked with has a robust incident response plan. Conversely, most operations teams will have a disaster recovery plan or a business continuity plan. This approach falls short and provides yet another opportunity to learn from the security team.

The Importance of the Baseline

How many of you have been part of a successful intrusion detection system implementation? If you haven't, go talk to the security team. The level of effort that goes into tuning an IDS and reducing the number of false positives is nothing short of monumental. However, once the work is done, the security team gains a valuable tool that helps inform when security incidents may be occurring. This investment in time upfront provides a significant level of proactive management.

On the operations side of the house, it can be equally useful to establish a robust understanding of the baseline of the applications / systems you are running. Is that database server CPU spike caused by a poor query or from an increased number of user sessions on the web application? Can you tell the difference and respond appropriately?

The security team has had to learn the importance of the baseline to accomplish their goals. The operations side can be guilty of throwing resources at a problem until it goes away because it's easier. However, now that we operate environments where the customer experience is the ultimate metric of performance, operations must be able to identify to and respond to possible issues (without the noise of false positives) to deliver the results most organizations need to be successful. Having tools and practices to ensure you understand the normal operations of your servers and applications can enable you to respond faster and more effectively to problems that arise.

Don't Compromise on Talent

CISO's recognize that failing to invest in the best talent that they can afford increases risk to the organization. Operations teams in the past have had several "crutches" to lean on when it comes to system outages or unplanned downtime. There are so many variables and so much complexity in

modern large IT environments that redundancy of systems can give operations staff (and leadership) a margin of error not afforded to the security teams. Additionally, security professionals are in very high demand. As a result, CISO's have become excellent at not only recruiting staff but at retaining them as well.

Budget Management

Managing the IT security budget can be a maddening exercise. One of the most challenging tasks of a CISO is to explain to a board why they should make a significant investment in something that they don't understand, whose success is defined by "something (breaches and exposure) not happening." Because of this, CISO must be champions at understanding the right level of investment. They must balance the amount of spend with the amount of risk the organization is willing to tolerate. Spend too much and they can be viewed as wasting money. Spend too little and the organization can be open to increased risk and be held accountable for not doing enough. If you're having trouble "selling" the operations budget to senior leadership, consider a conversation with your peers in the security team. Chances are they can provide you some negotiating tips as well as help you ensure that you are spending "just enough."

Tool Selection

Security tools by their very nature must have the capability to operate across the organizations. On more than a couple occasions, I have seen the NOC have separate monitoring protocols from the application administrators (or other areas). When looking for enterprise management tools and systems, look for systems that provide a meaningful picture across the organization. Dashboards that combine the needs of the CISO and the CIO can be game changers. Share the data between security and operations. You will find that you have a much stronger, more agile organization if the two teams are collaborating instead of complying with each other's requirements.