Connecting the Dots in Enterprise Security: Getting Started

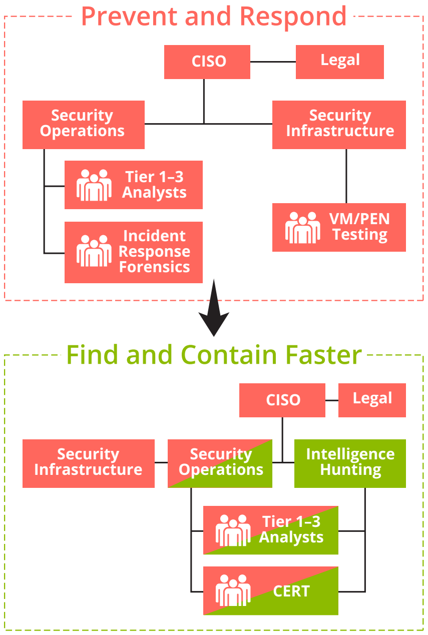
"According to the 2015 Verizon DBIR, the detection deficit—the difference in length of time between detecting an advanced attack and the time to compromise—continues to grow."

2015 Data Breach Investigations Report

Introduction

The potential economic, regulatory and brand ramifications posed by today's advanced threats represent a serious challenge to protecting your business. Advanced threats target a specific company, are designed to bypass traditional controls, and comprise a planned and orchestrated set of attack activities. For the enterprise security professional, business as usual is no longer a viable option; a purely reactionary, respond-to-alerts based security posture will not protect you from advanced threats.

You need to be able to detect and identify real threats by "connecting the dots", that is place indicators or alerts into a contextual chain of events over time. This is easier said than done for a security team of any size. Connecting the component dots of stealthy, multi-stage attack campaigns is even more challenging given that larger, more complex distributed networks increases vulnerable attack surfaces and make comprehensive visibility harder. Even with better visibility, without a new approach managing the increasing volumes of alerts is unsustainable: the negative effects of alert fatigue and false positives are well documented. The time (and resources) it takes to investigate priority alerts and false positives will wear down the best security teams.



The prevailing wisdom is that adding a hunting for threats mindset, a capability to connect the dots, is only for larger security teams. Only these larger organizations have the budgets and decades-long experience, typically gained in top government bureaus and their contractors. Dedicated Intelligence and Incident Response (IR) teams are for the privileged few, while the rest of us chase more and more alerts from firewalls, sandboxing and perhaps a SIEM system.

But this is not the reality—nor the path to greater enterprise security. Initiating and nurturing a hunting mindset can also start simply with re-focusing the right staff, empowering new skill sets and better aligned processes. Though enhanced technology certainly plays a role—with more automation, better integrated threat intelligence and faster, broader visibility into network traffic—developing a truly proactive security posture can and should be evolutionary. The goal is to re-direct some resources and augment your layered defense with a proactive component, to build in more sleuthing capabilities in your staff and support them with the right processes.

Below are two common scenarios derived from Arbor Networks' in-depth interviews across multiple verticals with CISOs, security operations and IR leads. This work was used as the basis for developing our security posture maturity profiles.

The Overlay

A fast growing, "Web 2.0" online consumer company was focused on fraud and web application security. The company has less than 500 employees, with three datacenters distributed in North America and Europe. Their existing security team is relatively small, with an outsourced Security Operations Center (SOC). The IR team was focused on employee issues. Recent theft of valuable Intellectual Property (IP) got the attention of the executive team and they lit a fire under the Security Architect.

The Security Architect "re-directed" 2 Security/Network Infrastructure Analysts to grow into new roles. They were sent to short training courses on threat hunting and intelligence, and instructed to institute a workable and consistent set of processes the team could use to approach investigations and importantly, guardrails to keep them on track and measure progress. To get started, they picked high priority alerts sent over from the out-sourced SOC to investigate on the ground, in-house.

ARBOR® NETWORKS

Results: New proactive approach found 10 targeted attacks in less than 12 months that did or could have seriously impacted their business. The new processes and success helped build more awareness across the team and throughout the organization of the world of advanced threats and security risks to the company. The real benefits was emergence of a culture of hunting and of the power of proactive sleuthing. There was more confidence in their ability to understand and protect the network and IP. This also laid a solid foundation for expanding staff, or even bringing some capabilities back from SOC.

The Skunk Works

A retail company with a slightly bigger Security Ops Team was focused on traditional, primarily reactive security measures: deployed antivirus, intrusion detection systems (IDS), web application firewalls (WAF) with sandbox capability, and security information and event management (SIEM) system. They had a cyber threat intelligence team that looked at raw intelligence and for threats on the horizon.

Still 90% of the "heavy-lifting" was outsourced. When it came to IR the organization had a handful of FTE's that worked closely with the outsourced services. They focused only on top 10%/20% of "high interest alerts or events" surfaced. Metrics included the number of threats blocked and Time of Incidents Resolved. But steady drumbeat of negative headlines rattled management—particularly in their industry sector. Should we be doing more to protect the business?

They recruited 3 analysts including a manager from their existing FTEs and began proactive threat hunting. Their skills sets, primarily penetration background, was not sufficient for advanced threat sleuthing, so provided additional training on output synthesis. In practice this was a natural evolution for certain team members.

They began by leveraging insights from their intelligence team, and were able to find attacks before they exfiltrated data. Their new approach also strengthened security by identifying locations and use of third-parties to gain access to sensitive assets. New metrics included dwell time of incidents found. The results galvanized management and the team has begun quarterly reporting to the Board. They have since expanded the scope of the hunter team and are far better positioned to head-off potential advanced threats before they end up in the headlines.

Taking Those First Steps

Re-orienting the focus of a security team is always a challenge, but finding today's advanced threats demands new approaches. Adding to your security posture a proactive puzzle-solving capability to help mitigate threats can be done in incremental steps. Some common steps include:

- Reduce the number of Tier 2–3 analysts working on security events, and have 1–2 analysts focus solely on hunting for threats in areas of their network/business.
- Look to enable in-house hunting skill sets with selective training. Individuals and teams of all sizes are looking for a new, more effective models, where their day is more productive and they can make forward progress against advanced attacks.
- If you don't have one already, set up a cyber intelligence team. Start by aggregating alerts from law enforcement, vendors, Intelligence/IR firms, etc. This alone will help shift the organizational focus from looking at potential indicators of compromise to indicators of attack.
- Look to set up new alert workflows and investigatory processes that include this intelligence passed to hunting-focused analysts. Change focus by creating a threat and risk-based view of assets within the network. For example for retailers: certain POS locations during Black Friday to Valentine's Day, or highlight "blind spots" where perimeter devices and end-user controls may be more limited, such as at subsidiary or remote locations.
- Consider outsourcing an SOC altogether, and retaining a set of Tier 3 analysts with both core "responding" and hunting skills. If you outsource, be sure to retain a set of Tier 3 analysts with both core "responding" and hunting skills to investigate critical issues/events passed from the SOC.

Organizations of any size are perfectly capable of proactively, connecting the dots. We have seen how small teams, even a sole actor responsible for policing the activities of an outsourced NOC or SOC, can transform their organization's approach to security. Re-purposing some staff, enhancing hunting skill sets with initial training, and re-engineering investigative processes first can yield security benefits today, and lay a solid foundation for better advanced threat protection in the future.

ARBOR®
NETWORKS

Corporate Headquarters
76 Blanchard Road
Burlington, MA 01803 USA
Toll Free USA +1 866 212 7267
T +1 781 362 4300

North America Sales
Toll Free +1 855 773 9200

Europe
T +44 207 127 8147

Asia Pacific
T +65 68096226

www.arbornetworks.com