CASE STUDY

AlienVault USM Powers Brier & Thorn's Managed Security Services Practice

Founded in 2010 and headquartered in San Diego, California, Brier & Thorn is a global IT risk management firm that supports companies in their important strategic decisions on operational security, IT risk management, and managed security services. For delivery of their managed services from their global security operations centers in the U.S. and Europe, Brier & Thorn turns to the AlienVault Unified Security Management™ (USM) platform.

Brier & Thorn first began searching for an all in one security solution in early 2013 when, as a risk management consultancy, they were tasked with conducting an incident response investigation for one of their clients.

Their client had clicked on a weaponized attachment that led to a Spear Phish attack. This required Brier & Thorn to identify what the hackers had access to in their clients network and if any data exfiltration was occurring.

At the time, Brier & Thorn was lacking visibility into their client's network so they needed an incident response forensics tool that enabled them to see traffic going in and out of the network.

"We needed something that could be deployed quickly and was capable of detecting and alerting on communication with known malicious hosts," said Alissa Knight, Group Managing Partner at Brier & Thorn, Inc.

> "It was the technology that we first looked at in deciding to go from only providing IT risk management consulting to also offering managed security services."
>
> *–Alissa Knight, Group Managing Partner at Brier & Thorn*

In their search for the right solution, Brier & Thorn came across AlienVault's Unified Security Management (USM) platform and its Open Threat Exchange™ (OTX). After a few conversations with AlienVault, Brier & Thorn determined that the functionality provided by USM delivered the ideal tool set for their incident response investigation.

Once acquired, AlienVault USM enabled Brier & Thorn to determine the source of the Spear Phish attack, which country it was coming from, and which machines on their client's network had been compromised.

"As soon as we deployed USM (without having to rely on any network IDS signatures at all) OTX began immediately flagging egress traffic from the network to hosts in Russia. We then began further forensics work based on this suspect traffic that allowed us to quickly find and remedy all of the affected hosts in the network," said Knight.

Company name : Brier & Thorn

Industry: Global IT Risk Management

Headquarters location: San Diego, California

Employee count: 51-200

Website Link: www.brierandthorn.com

After the investigation, Brier & Thorn decided to take a hard look at the IT risk management consulting services they were providing. As they did, they determined that by building an Information Security Management System ("ISMS"), performing penetration testing, and incident response for clients, they were only addressing one small part of their client's problems. Their original service was geared towards resource-strapped clients, and required that their clients continue to monitor and manage the devices on their own after they had been implemented.

This realization propelled Brier & Thorn to develop a service that would support their clients' security needs post-implementation. It was at this time that they built their first Security Operations Center (SOC) and added a new managed security services practice to their service portfolio. In order to provide a managed service that could scale to disparate

"As soon as we deployed USM (without having to rely on any network IDS signatures at all) OTX began immediately flagging egress traffic from the network to hosts in Russia. We then began further forensics work based on this suspect traffic that allowed us to quickly find and remedy all of the affected hosts in the network."

-Alissa Knight, Group Managing Partner at Brier & Thorn

locations around the world, Brier & Thorn needed to find a solution that would federate all of the network security events from their customers' networks into a single console user interface.

Since USM proved to be a perfect fit for Brier & Thorn's previous incident response investigation, it was the first solution they evaluated to power their new managed services program.

"It was the technology that we first looked at in deciding to go from only providing IT risk management consulting to instead also offering managed security services. The fact that AlienVault USM not only acts as a SIEM solution that allows us to federate all of our customer network events together into a single dashboard, but also provides additional solutions such as network intrusion detection, vulnerability management, and host intrusion detection – all in a single pane of glass. This single-solution advantage is what really made AlienVault the perfect fit for us. Without USM, our clients would have had to purchase both a SIEM and an IDS and that would be very cost-prohibitive for them – especially in large-scale deployments. The fact that USM bundles all of that into one solution is a huge cost savings," said Knight.

Key Benefits:

#1 - AlienVault USM allows Brier & Thorn to detect and alert on communication with malicious hosts on their clients' networks.

#2 - Brier & Thorn is able to provide their clients with a huge cost savings because of USM's all-in-one, single pane of glass design.

#3 - Brier & Thorn use AlienVault USM to help their clients more easily meet security compliance standards.

START YOUR FREE TRIAL ▸

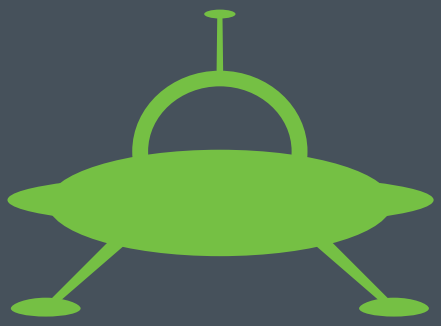
As Brier & Thorn integrated AlienVault USM into their SOC and managed services practice, they quickly experienced the benefits that the solution could provide to their clients. One such benefit was how AlienVault USM helped their clients meet regulatory compliance needs.

Many of Brier & Thorn's clients, whether it be retail customers like sports apparel, financial services, oil & gas companies, or registered investment advisers, all of these verticals have regulatory compliance requirements. These compliance standards can include HIPAA, PCI-DSS, ISO 27001 etc. and all require a central logging and management infrastructure or intrusion detection.

"AlienVault USM strengthens the capabilities our customers need to meet these compliance standards. It also allows our customers to be able to answer security compliance questionnaires, RFPs, and RFIs. These questionnaires are basically asking if there is a central log management system, if there is a network intrusion detection system in place, if there is a security information and event management (SIEM) solution in place, and if there is a host intrusion detection system in place. With AlienVault USM, our customers can easily answer "yes" to those questions.

Several of Brier & Thorn's clients also have aggressive merger and acquisition (M&A) strategies. In these environments, the successful integration between company networks requires the confirmation that both company networks are secure before they are merged. One of the first things that Brier & Thorn does when their client completes an acquisition is to deploy AlienVault USM on the network to ensure that nothing in the network is compromised that could potentially pivot to the acquiring company's network after it's connected.

Now, three years after using USM as a managed services provider for their client's incident response investigation, Brier & Thorn is one of AlienVault's largest MSSP partners and has the largest number of AlienVault sensors under management in a single deployment. In total, they currently have over 100 sensors under management across 70 countries and have just built their second AlienVault powered SOC in Stuttgart, Germany. Together with AlienVault, Brier & Thorn seeks to become one of the top managed service providers fully equipped to meet the ever evolving security needs of organizations all over the world.



About AlienVault

AlienVault has simplified the way organizations detect and respond to today's ever evolving threat landscape. Our unique and award-winning approach, trusted by thousands of customers, combines the essential security controls of our all-in-one platform, AlienVault Unified Security Management, with the power of AlienVault's Open Threat Exchange, the world's largest crowdsourced threat intelligence community, making effective and affordable threat detection attainable for resource-constrained IT teams. AlienVault is a privately held company headquartered in Silicon Valley and backed by Trident Capital, Kleiner Perkins Caufield & Byers, Institutional Venture Partners, GGV Capital, Intel Capital, Jackson Square Ventures, Adara Venture Partners, Top Tier Capital and Correlation Ventures.

For more information visit www.AlienVault.com or follow us on Twitter (@AlienVault).