Cyber attacks against financial institutions are sophisticated and continue to get worse. Staying on top of cybersecurity can seem like an impossible task, given the increasing complexity of attack vectors and growing industry regulations.

Troy Wunderlich, Vice President – Director of Operational Risk at Washington Trust Bank remarks, "I think future cybersecurity oversight will focus more on the management process and less on checking the boxes on security tools deployment. Regulators and industry experts realize that there are enough technical solutions out there to consolidate information and data from our networks to provide real-time alerting.

Now, there is a real need and requirement to demonstrate that you can both manage your information security and have adequate reporting coming out of your cybersecurity program that can be used to demonstrate to senior leadership, the board and to regulators that you have your arms around this from a management standpoint. We've got to continue to build out tools and processes to stay ahead of the game."

Troy's forward-thinking approach led him to look for a new type of security data platform.

BUILDING MANAGEMENT PROCESSES AROUND CYBERSECURITY

WA Trust was actively looking at various options that would enable them to build management processes around cybersecurity.

"DefenseStorm consolidates technical tools for monitoring your network and remediating incidents with built-in management processes that are linked to your policies," said Troy.

"And, I can report in real-time to my board and to regulators on how secure our network is. The ability to get quality reports that are meaningful to management is something that DefenseStorm brings to the table that we just didn’t have."

“We really couldn’t find another solution in the market that did what DefenseStorm did, in terms of bringing together IT governance and incident management workflow into a single system.”

– Troy Wunderlich
Vice President – Director of Operational Risk at Washington Trust Bank
WHAT IS SOMETHING YOU CAN DO WITH DEFENSESTORM THAT YOU COULDN’T DO BEFORE?

Troy
I think the first ‘ah-ha’ moment, in terms of doing something we couldn’t do before, was getting information about the number of alerts and the amount of incidents that we have coming from our systems. It is kind of a wakeup call when you see the amount of data and information coming off of your alerting systems. Also, because management now has visibility into Alerting and Incident Management, the biggest interaction change we’ve had between management and our technical security team is that we are able to ask very intelligent questions about what we’re alerting on, why we are alerting on them and why we have a certain severity level on those alerts. It became a very management-focused process, not just a technical process, once we gained visibility into what was happening.

Brian
I would say the main change is that the prior system we used was something that we ran in-house, and it required additional maintenance to keep that tool running and tuned. We’re spending less time keeping the tool maintained and upgraded, so now we can just focus on building new alerts and researching threats, logs and events.

WHAT DOES THE ABILITY TO TIE POLICIES AND INCIDENTS TOGETHER DO FOR YOU?

Troy
It demonstrates to management, the board and regulators that our policies on information security are adequate.

Top concerns that led to selecting DefenseStorm:

Having real-time, comprehensive reports that prove WA Trust’s alerting capabilities are linked to their policies and that they are managing alerts and incidents in a timely fashion is important because WA Trust wants its Board of Directors to engage with actual metrics, instead of just telling them to trust that the IT security team is doing the right things.

By linking every alert to a policy, WA Trust is able to measure the effectiveness of its policies and controls to see what policies are being violated and how frequently violations are happening. This data can be used to justify additional employee training or even a policy modification.

Troy states, “We had some tools before, but those tools were independent of each other, so different things might have triggered different alerts. With DefenseStorm, we can correlate everything together and determine what’s an incident versus what’s a false positive that doesn’t require attention. We can filter those out so the analysts can focus on the true incidents that need to be remediated and not waste time on things that are not a real issue for us.”
WHAT DOES A UNIFIED CYBERSECURITY MANAGEMENT SOLUTION DO FOR YOUR TEAM?

Brian
Having tickets centralized in DefenseStorm as a “one-stop shop” in which analysts can get the alert email is valuable. They can go into the system, perform the search and also track the history. And from the management side, they can see the status, the SLA and if we complied with all of our policies or if we missed anything. Before, everything was done with a separate ticketing system and then it was tracked through email that was sent to the entire team. Whoever saw it would grab the ticket and hopefully reply. There wasn’t a central place to find all the tickets or research what was out there to help us.

Troy
It helps us handle the challenges around being secure by giving us the ability to correlate different events that might turn into something more significant. This helps our analysts in evaluating something that’s occurring before we’re even sure what it is. We turn it into an incident, remediate it and monitor the activity and the remediation process to ensure that we’re reacting to things quickly. It’s helping our analysts become more efficient.

WHY IS REAL-TIME MANAGEMENT REPORTING SO IMPORTANT?

Troy
I appreciate the ability for both myself, as the manager, as well as for our CFO, to go into the tool and view a dashboard where we can see the events that have occurred, the incidents that are being handled, those that have been in remediation, those that still need to be remediated, who’s working on each and the current status.

We get executive summary information out of the tool that we use, but also then take the information to our various committees and our audit board to let them know how this tool is helping us to address our consistent security concerns or incidents that have occurred.

All of our systems in the past were each reporting independently. Now that they’re all reporting into one consolidated system with management reporting, we’re able to gain much better visibility into what we have to manage and how we have to manage it. Plus, we’ve become more efficient by eliminating duplications. Being able to tie that to your policies and then manage to those service levels – that’s the part that no one else can do right now. And that’s where we’re making the most progress.
WHAT IS YOUR FAVORITE FEATURE(S) OF THE DEFENSESTORM SOLUTION?

**Brian**
My favorite thing is the very responsive nature of the product. I can type in a query and have results back instantly, like Google, whereas before there were more hardware limitations.

I also like ThreatMatch because it provides automatic hits back. When there is an FBI flash alert, DefenseStorm will give me a hit back without doing anything, which definitely saves 5-10 minutes per search.

**Troy**
My favorite feature of the system is the ability to get management reporting that tells me the number of incidents we’ve had, the criticality of those incidents and how our team has been able to dispose of and rectify them. The time frame in which DefenseStorm has been able to do that and provide reports on a comprehensive and regular basis has helped give us the comfort that our cybersecurity is being managed correctly.

I also like the dashboard. I like how it brings things together because we have a lot of various systems with events and logs that are feeding into DefenseStorm, so having one tool to manage the whole security process is one of the biggest benefits that I see. We’re not trying to bring in separate things and manually correlate or report on them: it’s all within the tool. We see one view, one picture of everything that’s happening.

WHAT WOULD YOU TELL A FUTURE USER ABOUT DEFENSESTORM?

**Troy**
I think some technical engineers and security people will think that DefenseStorm will just duplicate what they already have, which could be solutions that consolidate alerting data. But what those technologists need to realize is that management needs systems that bring those things together to report and demonstrate that our technicians are doing what they’re supposed to be doing, and doing it in a critically timely fashion. Timely responses to alerts and incidents are what often make or break a security event.

You prepare as best you can by putting in as many layers of protection and security as possible to prevent breaches from occurring, and then add to that preparation with a tool like DefenseStorm that allows you to quickly respond and remediate anything necessary to minimize your exposure and the potential harm to customers.

“The product itself is very streamlined and it has a skilled team behind it that is very knowledgeable and experienced in security and banking, which I think is a huge value add.”

– Brian Kinsley
IT Security Lead at Washington Trust Bank