SANS

Analyst Program

WhatWorks

WhatWorks in Reducing Compliance Costs and Increasing Resilience with Integrity Management Tools

CIMCOR

Introduction

Maintaining the integrity of critical files, executables and resource configurations is considered basic security hygiene. The Verizon Data Breach Integrity Report points out each year that the majority of security incidents are enabled by a failure to implement and monitor these controls, even though every major compliance regime requires compliance be regularly assessed and validated. Without achieving this essential level of security, enterprises are both at risk for business outages caused by successful attacks and for spending large portion of the security budget dealing with failed audits.

In this SANS What Works report, SANS Director of Emerging Security Trends John Pescatore interviews Dan Schaupner, head of Digital Security Consulting North America for Atos, to gain his insight on what he went through in the business justification and deployment of Cimcor's CimTrak file integrity monitoring tool as part of reducing the cost of securely managing a large customer environment, as well as reducing the time and effort of demonstrating compliance.

About the End User

Dan Schaupner is the head of Cloud and Innovation, Global Digital Security Consulting at Atos. He has been with Atos since 2017 and brings two decades of experience to his leadership of consulting activities. Previously, Dan was CTO at a Washington, DC risk management firm, advising the US government on cloud security (FedRAMP/Trusted Internet Connection). During his career, Dan has advised business and technical leadership in many industries including finance, healthcare, higher-education, manufacturing, and others. Dan is a graduate of the Atos Gold for Technology Leaders program, member of the Atos expert community, and provides mentorship to the Atos FUEL program for emerging professionals. Dan holds an MBA from Virginia Tech, an Engineering Bachelor's degree from the University of Michigan, and CISSP and CISM certifications.

About the Interviewer

John Pescatore joined SANS as director of emerging technologies in January 2013 after more than 13 years as lead security analyst for Gartner, running consulting groups at Trusted Information Systems and Entrust, 11 years with GTE, and service with both the National Security Agency, where he designed secure voice systems, and the U.S. Secret Service, where he developed secure communications and surveillance systems and "the occasional ballistic armor installation." John has testified before Congress about cybersecurity, was named one of the 15 most-influential people in security in 2008, and is an NSA-certified cryptologic engineer.

About SANS WhatWorks

WhatWorks is a user-to-user program in which security managers who have implemented effective Internet security technologies tell why they deployed it, how it works, how it improves security, what problems they faced and what lessons they learned.

Question

Tell us a little bit about yourself, your company, and the role you play there.

Answer

My name's Dan Schaupner. I'm the head of Digital Security Consulting North America for Atos. I've been working in the security business for over 20 years now. I started my career working for the United States Department of Defense and some work on the federal/civilian side. One of the things that I was privileged to work on was the FedRAMP cloud services program. For the last six years, I've been working at Atos with commercial and state government customers.

Dan Schaupner: So, in other words, we want to not only make sure that you're meeting compliance and risk management needs, but also how the security supports the customer's goals. One area that we're particularly focused on is application security. That's something where we have a relative strength, and we have a very solid team. I'm very lucky to have people who are themselves very distinguished in their careers—a lot of them former CISOs—and a great organization of rising talent.

Question

What was the problem area that caused you to look for solutions in file integrity management and integrity assurance overall?

Answer

We have a customer who needs to comply with a very strict compliance framework that is along the lines of FedRAMP high. The financial consequences of non-compliance are severe. They were technically compliant, but verifying that required a very labor-intensive, expensive manual process. This is a large customer, with over 1500 servers under management. We realized we needed to automate as much as possible and started looking at what tools were available.

We needed a solution that would reduce the effort to assess and validate, in particular, file integrity, but the larger need was overall change management assessment and verification. Enforcement and verification of the overall change management process was complicated by the fact that the contract specified joint management of assets. That is, the customer managed part of the system, while certain assets were managed by Atos as a service provider. We needed a product that could deal with that complication. To make a long story short, the Cimcor CimTrak product met all our needs.

CimTrak supported eliminating a lot of manual communication and interaction in the change management process.

It also provided a platform for our overall asset management and integrity verification that could expand to meet our needs for this contract and likely others.

The other product we looked at handled our FIM needs, but Cimcor was the only one that had a larger story, and their team was able to work with us to increase our level of automation for the broader processes.

Question

Can you give us some examples?

Answer

One of the key areas is interaction with our change management system through ServiceNow. The shared responsibility aspect of this contract meant some trouble tickets needed to stay within Atos, some had to be assigned to the customer, etc. That applied to issues that went well beyond FIM, and Cimcor handled it beautifully.

A longer-term need is integrating with other tools, such as endpoint monitoring products. We haven't done that yet under this contract, but it is a key strategic objective for us.

The Cimcor platform will be a key part of our overall security orchestration and automation strategy.

We started this as a need for this customer, but we are expanding it to other customers right now, including a manufacturing firm and another customer in Europe.

Question

What sort of metrics are you looking at to determine success?

Answer

Reducing the total time and cost of successfully passing audits was the number one objective.

CimTrak eliminated a lot of the manual communication and routing of messages across different organizational elements

to achieve that, as well as avoiding any financial penalties for not being able to demonstrate compliance.

Increasing our responsiveness definitely increased the customer level of satisfaction. Senior management at the customer saw a reduction in how long it took to notify them of an issue as well as their time to resolve. The auditors were also happier, as it made their job easier and shortened the time required for the audit.

Question

What support did you use from Cimcor, and how do you rate their support?

Answer

We had a great level of support from Cimcor.

They were very responsive to our needs, and all the support folks we were dealing with were not only articulate and knowledgeable about the CimTrak product but they were also able to use insight they gained from work they've done with other prominent customers in the past.

Question

How long have you been using this Cimcor product?

Answer

A little bit over two years.

Question

With two years of experience, are there any lessons learned or any things you would do differently that you could pass on to the audience?

Answer

Focusing on a platform, rather than a narrow FIM product, was probably key to our success. I would say one of the lessons learned is that if you are considering a specific problem, maybe like file integrity monitoring or endpoint protection, or even identity management, you should step back and ask yourself whether there is a bigger conclusion here other than this one domain of security. In the case with Cimcor, it really exposed the importance of understanding the full capability of solutions. We started out thinking about FIM, and when we looked more closely at CimTrak, we found, wow, there are things that they can provide beyond FIM that provide value, such as configuration management and endpoint management. We saw the platform approach could meet both our immediate needs on this contract but also support longer-term objectives.

We are now exploring expanded use of CimTrak as a cybersecurity awareness and enforcement platform. We are in a much better position to do that then if we had gotten locked into a single-purpose product.

Question

Is there anything you'd like to bring up that I didn't ask about?

Answer

As a cybersecurity consulting organization, we are really in the business of helping meet customers' business goals by improving cybersecurity levels to reduce both risk and cost. We think using CimTrak as a platform will help us work with customers to get them to a more adaptive level of security, especially as many of them are making the transition from all on-premises computing to cloud computing.

We try to make sure our solutions are scalable and flexible to support that, and Cimcor is a key part of that.