Office of Security Management

Year in Review

As we close out 2021, I think it's a valuable exercise to look back at the immense achievements of the team. While the Office of Security Management (OSM) was formed by Executive Order in July of 2019 and we have made great strides in improving the security posture of the State since then, tremendous progress has been made in 2021.

Team Growth

2021 saw explosive growth for the OSM team. What was previously a three-person group supported mainly by contractual resources and services, is now an in-house team that is growing into providing world-class cybersecurity services. The leadership team, which is responsible for driving strategy for the team, represents some of the most influential growth:

- Laura Gomez-Martin - Deputy CISO (Now the State Chief Privacy Officer)
- Ian Goodhart - Director of Cybersecurity Operations
- Mike Stallings - SOC manager
- Jeff Winkler - Cybersecurity Solutions Architect
- Ron DeLeos - Threat Intelligence Lead
- Mike Hooper - Senior Vulnerability Manager

Splunk Growth and Adoption

One of the single biggest challenges that we overcame in 2021 was the inability to leverage the signals generated by the network for security investigations. Splunk was originally configured for a much smaller use-case, and our need was exceeding the capacity we had. This was the year for us to tear it down and rebuild it to better support the ever increasing security needs of the state.

More data ingested by Splunk

- 275% increase in the number of hosts sending events to Splunk (from 250 to 1300)
- 300% increase in GB per day (from 200GB to 800GB per day)
- 260% increase in events per day (from 500M to 1.8B per day)

Completed multiple major projects

- Rebuild of infrastructure
- TrackMe data tracking system
- Complete rewrite of asset reporting
- Creation of the CISO Dashboard and MFR reporting
- Ingestion and parsing of dozens of new data sources

This wouldn't have been possible without the tireless work of the Splunk team. Special thanks goes to Rob Chester, Jesse Henderson, and Nick Spencer!

Security Operations and Incident Response

From 2015 until early 2021, Security Operations were performed by a contractor as a service. In April of 2021, we moved this to a DoIT run, in-house service with true 24x7 coverage. The impacts of this change were both immediate and positive. Ticket accuracy improved and Service Level Agreement targets are now constantly exceeded.

2021 saw no shortage of opportunity for incident response; everything from the Solarwinds supply-chain attack, Hafnium Exchange Server attacks, phishing campaigns (including those launched by CISA against the State), and a host of other incidents. The 4,656 Security Operations Center (SOC) tickets these attacks generated represents approximately 80% of the total tickets responded to by this team in 2021. The number of incident related tickets more than tripled from the previous year.

All of this was done with a team and operation that was built in 2021

In addition to responding to these attacks, we've developed a host of new capabilities, including those provided by Google Workspace Enterprise (phishing investigation, containment, and eradication), host isolation and endpoint detection and response through Tanium.

We have also implemented a new capability on the networkMaryland network - Denial of Service (DoS) protection. As the frequency and severity of DoS attacks increases, specifically volumetric Distributed Denial of Service attacks, this new capability helps us to maintain availability for our customers.

In addition to our inward-facing accomplishments, we've also taken on criminal fraudsters by using capabilities within the Recorded Future Fraudwatch system to remove countless unemployment insurance fraud sites from the internet. This is something that we do behind the

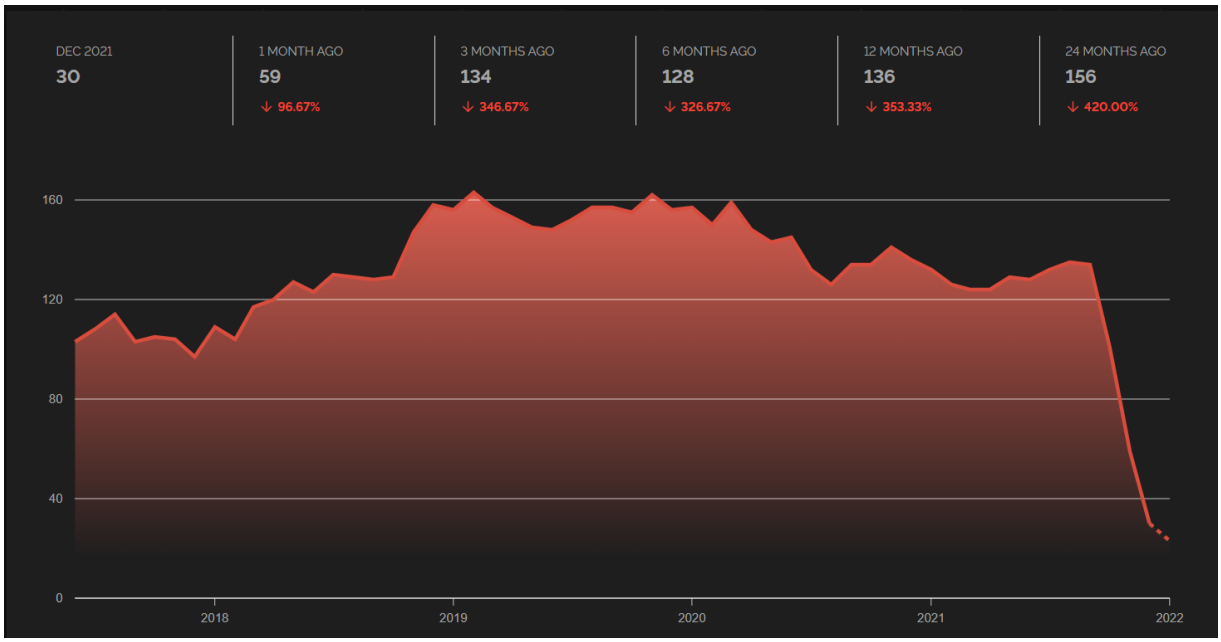
scenes that has a real impact on the citizens of the State. We have chosen to keep these capabilities widely unpublicized, but instead let our success be the noise.

Vulnerability Management

2021 also saw significant growth and maturation for the vulnerability management program. With the addition of Mike Hooper and Brian Jester, what was previously performed as an ad-hoc function has grown into a sustainable capability supported by an independent team with strong leadership.

However, the data is the best indicator of performance. Please note the point in time in the five year graph where incidents of obsolete encryption on public websites drastically declined.

Instances of Websites Running SSLv2, SSLv3, TLS1.0, and TLS1.1



NICE - The framework for Cybersecurity Workforce Development

While we started the initiative in 2020, in 2021 we became one of the first States to begin using the National Institute of Standards and Technology's (NIST) National Initiative for Cybersecurity Education (NICE) framework as described in SP 800-181 Rev. 1. This represents a fundamental shift in using nationally consistent language to describe work roles and their associated knowledge, skills, abilities, and tasks. Using this framework provides current and potential employees with clear expectations for progressing their careers.

ServiceNow GRC/SecOps

servicenow

SecOps
Q4 2021 saw the deployment of the ServiceNow Security Operations (SecOps) application. SecOps is a security work management engine leveraging orchestration, automation, and cross tool data enrichment to improve the State's security response capabilities.

Connecting new and existing security tools to aggregate vulnerabilities, events and incidents in one place, enables prioritization and response using data that used to exist in separate systems and was unable to be correlated.

Governance, Risk and Compliance
Alongside SecOps we added the capability to track and manage organizational risk using the ServiceNow Governance, Risk and Compliance (GRC) application. With ServiceNow GRC we are able to do away with cumbersome spreadsheets and manual data mapping; processes which make it difficult to view and report on the data. ServiceNow GRC promotes efficient and effective data collection and reporting processes which enables us to manage risk and increase resilience across the organization.

Threat Intelligence

Another new capability in 2021 came from the purchase and integration of Anomali, Recorded Future, and Shodan. With this toolset, we began to receive immediate feedback about compromised credentials, fraudulent sites impersonating the State, known bad-hosts, and many other forms of valuable intelligence. As we begin to feed back threat intelligence into the platform, we're doing so in partnership with other States.

In late 2021, we began integrating this into ServiceNow Security Incident Response, enabling more seamless imports of threat intelligence and more robust sharing capabilities. While we have just begun extracting the value, the coming months will see an even greater return on our investment for our security operations.

Annapolis Cybersecurity Summit

Governor Hogan convened a cybersecurity summit at the Maryland State House in Annapolis focused on coordinated federal, state, and private sector efforts to prepare for and address cybersecurity threats to the State and Critical Infrastructure partners.

The summit brought together senior government officials, including leaders from the White House, Congress, the National Security Agency (NSA), and the FBI, as well as governors, academic leaders, and private sector experts.

The summit yielded several deliverables, three of which directly impact our team, including:

- The creation of a State Chief Privacy Officer, ensuring consistency in privacy governance - filled by our Deputy CISO Laura Gomez-Martin
- The creation of a State Chief Data Officer, creating a consistent framework for data governance - filled by a previous DoIT employee Pat McLoughlin
- Establishing the Maryland Institute for Innovative Computing at UMBC, which will partner with the Office of Security Management for several capabilities.

Looking forward to 2022

We are extremely proud of our 2021 accomplishments, and remain forward thinking and are continuously evaluating ways to improve upon the capabilities we have already built and looking at new capabilities to expand OSM effectiveness. Our hope is that our 2021 accomplishments will pale in comparison to the progress towards security excellence we make in 2022.

Professional development
One opportunity that we have to make the whole team better is by supporting each other in growth. With a.gov email, team members have access to the Federal Virtual Training environment, which contains a plethora of cybersecurity-focused training materials to help advance your capabilities.

Find a buddy, make a plan, and start training - now.

https://fedvte.usalearning.gov/

MD-ISAC
In the last week, the Security Operations Center generated nineteen new observables, such as Indicators of Compromise and Indicators of Attack, in ThreatStream. That comes out to around 1,000 per year.

Imagine if we pulled all of our observables into ThreatStream.
Imagine if we pulled the same from every county, city, and school system in the State.
Imagine the value that information would have in protecting us.
Imagine how it could protect them.

Let's see if we can find out.

Security Operations Improvements
How do we enable the team to work on bigger and better things? Get out of the robotic items. Security operations will continue to see a push to automate more and more, through ServiceNow, Splunk, and our tool stack. This creates opportunities for the team to learn automation and focus on deeper incident response before escalation.