Key lessons learned from the former State of Maryland CISO.

Why Maryland? Its proximity to Washington DC makes it the cybersecurity capital of the world in terms of infrastructure, skilled personnel, and capabilities. Below are the key takeaways from a conversation with the former Chief Information Security Officer for the State of Maryland.

Environmental Drivers

- All government services at all levels operate in an online model, making the entire domain susceptible to cyber attacks.

- The impact and magnitude of events are increasing, and the associated effects are more pervasive due to technology interdependencies.

- No systems exist in isolation; if one system is affected, other downstream systems are at risk.

NET RESULT?

Security breaches punch far above their weight.

Operating Model Variations

State-level cybersecurity is implemented under three different and uncorrelated models:

Centralised

Centralized model for the executive branch: Cybersecurity and IT run by a single organization

Federated

Federated Model: Shared services across state entities.

Decentralised

Decentralized Model: Everyone does what they want.

Cybersecurity Challenges

Visibility

Understanding and having immediate access to online risks, vulnerabilities, and threats.

Actionability

IT and Cybersecurity environments change very quickly, organizations lack an actionable view of their technology and security infrastructure.

Vulnerability

Shadow IT continues to be a real problem, driving how often new vulnerabilities are introduced and published.

Automation

Organizations can no longer rely only on people to analyze the volume of events coming in, making security analytic platforms a force multiplier for security teams.

Context

Analysts do not always know what type of incident or threat to look for: there is too much non-contextualized information coming in to derive meaningful insights.

Prioritisation

Cyber Threat Intelligence (CTI) is the core of any security posture; providing context to deliver the who what when where, and why to drive priorities.

Interdependencies

Software is more subtle and interdependent than hardware; most organizations are not efficient enough to manage software security issues effectively.

Impact of Failure

1. Public sector cybersecurity failures are not only about financial impact, there is also a risk to lives because of the impact of an attack on critical government functions.
2. Resilience must be baked into a public model: anti-fragility is core to any cybersecurity program, and CTI is a primary enabler.
3. While a single attack can compromise one system, if information on the attack is shared with operational or supply chain partners, the whole system becomes stronger and more resilient.

Executive Buy-In

The role of the CISO is expanding from highly technical to evangelical/influential, focusing on driving positive change to reduce organizational risk. The budget conundrum:

If something bad happens:
Cybersecurity gets their budget cut.

If nothing bad happens:
There's no reason to invest.

These constraints need to push the conversation away from features and benefits to one around value.

It is incredibly important to have the right technology partners and support organizations such as ISACs.

Value Delivered by Anomali

1. Anomali Reduced the state's cyber threat response time from days to minutes.
2. Anomali ThreatStream is the central repository for global cyber threat intelligence and is the core enabler of actioning operational responses from intelligence.
3. Anomali Integrator gets information out to their security apparatus and uses Anomali Security Analytics when information indicates something happened. Those indicators are loaded into ThreatStream to see if there is any risk associated with the specific IoCs (indicators of compromise).
4. Anomali Lens+ is used to identify and load indicators into the system to supercharge Security Operations Center analysts.

Summary

- Effective, pervasive cybersecurity needs strong and consistent buy-in from upper-level management.

- The approach needs to be specific to the information needs of the business or operational entity.

- People who write really big checks are generally not technical; it is imperative that the cybersecurity industry focus on the business value of their solution, and not on specific product features.

© 2023 Anomali. All rights reserved.
Anomali and the Anomali logo are trademarks of Anomali.