

In cybersecurity, an Indicator of Compromise (IoC) is evidence suggesting a system or network may have been breached, helping security teams identify and respond to potential or ongoing attacks is exactly what US ProTech delivers with its Anamo CDM software that correlates Host-Based Indicators with comparative HashID Analytics.

Clearly, businesses face a multifaceted cybersecurity landscape packed deeply with Technical Adversaries who seek to breach networks, elevate credentials, and exfiltrate the maximum value and Data possible. Targets include Intellectual Property, Assets, Personal Identifiable Information and much more. Tools and threats include Data Breaches, Ransomware, Unauthorized Privileged Escalation, Phishing Attacks, Command Injection, Buffer Overflow, Social Engineering, Malware, and the list goes on!

Over the next four months, we’ll highlight 7 key cybersecurity topics, threats and data breach risks including:

1. Cyberattacks: IoC Types & Impact
2. User-Based and Insider-Threat Based Risks
3. Industries at Risk
4. Mitigation Strategies
5. Artificial Intelligence Cyber Threats
6. DNS Tunneling
7. Insider Threats

This month let’s discuss the 1st of 7 important Cybersecurity considerations, “Cybersecurity IoC Types & Impact.” The overwhelming majority of Technology Executive and Cybersecurity leaders have absolute needs, these include:

**1. Definitive evidence that something is happening, right now**

**2. To understand the significance and importance of the activity**

**3. Immediate identification where the activity is being presented**

**3. Having knowledge of options on how they need to respond**

Essentially, software that correlates Host-Based Indicators of Compromise is the most effective process if delivering this information. By using the latest and most advanced comparative HashID Analytics, Cyber-practitioners are now capable of correlating data that has never been available until the advent of CDM. The concept of Continuous Diagnostics and Mitigation is over 10 years old with it’s origins dating back to 2013. Launched by CISA / DHS, today CDM is broadly used by over 300 Federal Agencies and is also commercially available as well. Anamo is a CDM that should be considered because it bridges the most significant attributes of SIEM, EDR, ASM, EPP, and other tools such as the gathering of data Forensics, delivery of eDiscovery, and more.

Here is an Explainer Video of Anamo CDM: <https://youtu.be/ByTKwyAzZB4>

**Cyberattack: IoC Types & Impact**

* [**DDoS attacks**](https://www.google.com/search?rlz=1C1GCEU_enUS905US908&cs=0&sca_esv=c40def4ba69778d6&sxsrf=AHTn8zrTH-Bo160u_o5JSYPvX-RmyWpPGA%3A1742514901607&q=DDoS+attacks&sa=X&ved=2ahUKEwipjcHt7ZmMAxXtOkQIHUucH9UQxccNegQIMhAE&mstk=AUtExfBUTzHg1wDzpJ4iA9mLVLKeZIT1MPCDXVbJJZp22QEY5sVyQ93MO4ga2HnFjyEZawadn-EM19aNXRjtcF9hqxMvUvvjQiT5IpFDTlirlFQ1-Zpy3CX8hvnatqaFdrY6zn8YxNryayadlt05wrZSSLlADdWEHLPNHjZMOIWDg7KvbZdLJUXeE7x2FS32aF6bOgkBk-PaC0C8vFiOT8EaTiCz3OjOA-rxpnJ8I_xX1aGT0Pok75Bhhauz7RYrpQygXnY&csui=3)**:**

These attacks aim to make an online service unavailable to its users by overwhelming it with traffic.

* [**Data breaches**](https://www.google.com/search?rlz=1C1GCEU_enUS905US908&cs=0&sca_esv=c40def4ba69778d6&sxsrf=AHTn8zrTH-Bo160u_o5JSYPvX-RmyWpPGA%3A1742514901607&q=Data+breaches&sa=X&ved=2ahUKEwipjcHt7ZmMAxXtOkQIHUucH9UQxccNegQINBAE&mstk=AUtExfBUTzHg1wDzpJ4iA9mLVLKeZIT1MPCDXVbJJZp22QEY5sVyQ93MO4ga2HnFjyEZawadn-EM19aNXRjtcF9hqxMvUvvjQiT5IpFDTlirlFQ1-Zpy3CX8hvnatqaFdrY6zn8YxNryayadlt05wrZSSLlADdWEHLPNHjZMOIWDg7KvbZdLJUXeE7x2FS32aF6bOgkBk-PaC0C8vFiOT8EaTiCz3OjOA-rxpnJ8I_xX1aGT0Pok75Bhhauz7RYrpQygXnY&csui=3)**:**

These occur when unauthorized individuals gain access to sensitive data, leading to potential financial losses, reputational damage, and legal consequences.

* [**Third-party breaches**](https://www.google.com/search?rlz=1C1GCEU_enUS905US908&cs=0&sca_esv=c40def4ba69778d6&sxsrf=AHTn8zrTH-Bo160u_o5JSYPvX-RmyWpPGA%3A1742514901607&q=Third-party+breaches&sa=X&ved=2ahUKEwipjcHt7ZmMAxXtOkQIHUucH9UQxccNegQIJhAE&mstk=AUtExfBUTzHg1wDzpJ4iA9mLVLKeZIT1MPCDXVbJJZp22QEY5sVyQ93MO4ga2HnFjyEZawadn-EM19aNXRjtcF9hqxMvUvvjQiT5IpFDTlirlFQ1-Zpy3CX8hvnatqaFdrY6zn8YxNryayadlt05wrZSSLlADdWEHLPNHjZMOIWDg7KvbZdLJUXeE7x2FS32aF6bOgkBk-PaC0C8vFiOT8EaTiCz3OjOA-rxpnJ8I_xX1aGT0Pok75Bhhauz7RYrpQygXnY&csui=3)**:**

A breach in a company's supply chain or a third-party vendor can expose the entire organization to risk.

* [**Cloud-based attacks**](https://www.google.com/search?rlz=1C1GCEU_enUS905US908&cs=0&sca_esv=c40def4ba69778d6&sxsrf=AHTn8zrTH-Bo160u_o5JSYPvX-RmyWpPGA%3A1742514901607&q=Cloud-based+attacks&sa=X&ved=2ahUKEwipjcHt7ZmMAxXtOkQIHUucH9UQxccNegQIJRAE&mstk=AUtExfBUTzHg1wDzpJ4iA9mLVLKeZIT1MPCDXVbJJZp22QEY5sVyQ93MO4ga2HnFjyEZawadn-EM19aNXRjtcF9hqxMvUvvjQiT5IpFDTlirlFQ1-Zpy3CX8hvnatqaFdrY6zn8YxNryayadlt05wrZSSLlADdWEHLPNHjZMOIWDg7KvbZdLJUXeE7x2FS32aF6bOgkBk-PaC0C8vFiOT8EaTiCz3OjOA-rxpnJ8I_xX1aGT0Pok75Bhhauz7RYrpQygXnY&csui=3)**:**

As businesses increasingly rely on cloud services, these become attractive targets for cybercriminals.

Data Breach Vectors:

* [**System intrusion**](https://www.google.com/search?rlz=1C1GCEU_enUS905US908&cs=0&sca_esv=c40def4ba69778d6&sxsrf=AHTn8zrTH-Bo160u_o5JSYPvX-RmyWpPGA%3A1742514901607&q=System+intrusion&sa=X&ved=2ahUKEwipjcHt7ZmMAxXtOkQIHUucH9UQxccNegQIPBAB&mstk=AUtExfBUTzHg1wDzpJ4iA9mLVLKeZIT1MPCDXVbJJZp22QEY5sVyQ93MO4ga2HnFjyEZawadn-EM19aNXRjtcF9hqxMvUvvjQiT5IpFDTlirlFQ1-Zpy3CX8hvnatqaFdrY6zn8YxNryayadlt05wrZSSLlADdWEHLPNHjZMOIWDg7KvbZdLJUXeE7x2FS32aF6bOgkBk-PaC0C8vFiOT8EaTiCz3OjOA-rxpnJ8I_xX1aGT0Pok75Bhhauz7RYrpQygXnY&csui=3)**:** Cybercriminals gain unauthorized access to systems or networks.
* [**Web application attacks**](https://www.google.com/search?rlz=1C1GCEU_enUS905US908&cs=0&sca_esv=c40def4ba69778d6&sxsrf=AHTn8zrTH-Bo160u_o5JSYPvX-RmyWpPGA%3A1742514901607&q=Web+application+attacks&sa=X&ved=2ahUKEwipjcHt7ZmMAxXtOkQIHUucH9UQxccNegQIQBAB&mstk=AUtExfBUTzHg1wDzpJ4iA9mLVLKeZIT1MPCDXVbJJZp22QEY5sVyQ93MO4ga2HnFjyEZawadn-EM19aNXRjtcF9hqxMvUvvjQiT5IpFDTlirlFQ1-Zpy3CX8hvnatqaFdrY6zn8YxNryayadlt05wrZSSLlADdWEHLPNHjZMOIWDg7KvbZdLJUXeE7x2FS32aF6bOgkBk-PaC0C8vFiOT8EaTiCz3OjOA-rxpnJ8I_xX1aGT0Pok75Bhhauz7RYrpQygXnY&csui=3)**:** Exploiting vulnerabilities in web applications to steal data or compromise systems.
* [**Miscellaneous errors**](https://www.google.com/search?rlz=1C1GCEU_enUS905US908&cs=0&sca_esv=c40def4ba69778d6&sxsrf=AHTn8zrTH-Bo160u_o5JSYPvX-RmyWpPGA%3A1742514901607&q=Miscellaneous+errors&sa=X&ved=2ahUKEwipjcHt7ZmMAxXtOkQIHUucH9UQxccNegQIPRAB&mstk=AUtExfBUTzHg1wDzpJ4iA9mLVLKeZIT1MPCDXVbJJZp22QEY5sVyQ93MO4ga2HnFjyEZawadn-EM19aNXRjtcF9hqxMvUvvjQiT5IpFDTlirlFQ1-Zpy3CX8hvnatqaFdrY6zn8YxNryayadlt05wrZSSLlADdWEHLPNHjZMOIWDg7KvbZdLJUXeE7x2FS32aF6bOgkBk-PaC0C8vFiOT8EaTiCz3OjOA-rxpnJ8I_xX1aGT0Pok75Bhhauz7RYrpQygXnY&csui=3)**:** Human errors or misconfigurations can lead to data breaches.
* [**Stolen credentials**](https://www.google.com/search?rlz=1C1GCEU_enUS905US908&cs=0&sca_esv=c40def4ba69778d6&sxsrf=AHTn8zrTH-Bo160u_o5JSYPvX-RmyWpPGA%3A1742514901607&q=Stolen+credentials&sa=X&ved=2ahUKEwipjcHt7ZmMAxXtOkQIHUucH9UQxccNegQIQRAB&mstk=AUtExfBUTzHg1wDzpJ4iA9mLVLKeZIT1MPCDXVbJJZp22QEY5sVyQ93MO4ga2HnFjyEZawadn-EM19aNXRjtcF9hqxMvUvvjQiT5IpFDTlirlFQ1-Zpy3CX8hvnatqaFdrY6zn8YxNryayadlt05wrZSSLlADdWEHLPNHjZMOIWDg7KvbZdLJUXeE7x2FS32aF6bOgkBk-PaC0C8vFiOT8EaTiCz3OjOA-rxpnJ8I_xX1aGT0Pok75Bhhauz7RYrpQygXnY&csui=3)**:** Using stolen usernames and passwords to gain access to systems.
* [**Human element**](https://www.google.com/search?rlz=1C1GCEU_enUS905US908&cs=0&sca_esv=c40def4ba69778d6&sxsrf=AHTn8zrTH-Bo160u_o5JSYPvX-RmyWpPGA%3A1742514901607&q=Human+element&sa=X&ved=2ahUKEwipjcHt7ZmMAxXtOkQIHUucH9UQxccNegQIPhAB&mstk=AUtExfBUTzHg1wDzpJ4iA9mLVLKeZIT1MPCDXVbJJZp22QEY5sVyQ93MO4ga2HnFjyEZawadn-EM19aNXRjtcF9hqxMvUvvjQiT5IpFDTlirlFQ1-Zpy3CX8hvnatqaFdrY6zn8YxNryayadlt05wrZSSLlADdWEHLPNHjZMOIWDg7KvbZdLJUXeE7x2FS32aF6bOgkBk-PaC0C8vFiOT8EaTiCz3OjOA-rxpnJ8I_xX1aGT0Pok75Bhhauz7RYrpQygXnY&csui=3)**:** Employee mistakes or lack of security awareness can be a major source of data breaches.
* [**Insider threats**](https://www.google.com/search?rlz=1C1GCEU_enUS905US908&cs=0&sca_esv=c40def4ba69778d6&sxsrf=AHTn8zrTH-Bo160u_o5JSYPvX-RmyWpPGA%3A1742514901607&q=Insider+threats&sa=X&ved=2ahUKEwipjcHt7ZmMAxXtOkQIHUucH9UQxccNegQIPxAB&mstk=AUtExfBUTzHg1wDzpJ4iA9mLVLKeZIT1MPCDXVbJJZp22QEY5sVyQ93MO4ga2HnFjyEZawadn-EM19aNXRjtcF9hqxMvUvvjQiT5IpFDTlirlFQ1-Zpy3CX8hvnatqaFdrY6zn8YxNryayadlt05wrZSSLlADdWEHLPNHjZMOIWDg7KvbZdLJUXeE7x2FS32aF6bOgkBk-PaC0C8vFiOT8EaTiCz3OjOA-rxpnJ8I_xX1aGT0Pok75Bhhauz7RYrpQygXnY&csui=3)**:** Malicious or negligent actions by employees can compromise data.

Contact US ProTech today to get your own free trial of Anamo CDM. You will immediately gain the insight needed to prioritize your security efforts. Allow Anamo CDM to deliver this essential data autonomously, automatically, and continuously, without any effort, complications, or any required scheduling on your part! Complimentary trials of Anamo CDM are available upon request, contact us online, by phone, or by speaking with a professional consultant or reseller, today.

Calendar for Future Topics:

**April: User-Based and Insider-Threat Based Risks plus Industries at Risk**

**May: Mitigation Strategies plus Artificial Intelligence Cyber Threats**

**June: DNS Tunneling plus Insider Threats**