Complete Network Security Awareness

cyber OBSERVER

"Organizations are *failing at early breach detection*, with more than 92% of breaches undetected by the breached organization. The situation can be improved with stronger threat intelligence, the addition of behavior profiling and better analytics." -Gartner

"As defenders, we have access to an extraordinary array of security tools and technology, security standards, training and classes, certifications, vulnerability databases, guidance, best practices, catalogs of security controls, and countless security checklists, benchmarks, and recommendations." But all of this technology, information, and oversight has become a veritable *"Fog of More"*. -SANS

Introducing Cyber Observer

Cyber Observer is the emerging market leader of a high-level awareness & visibility management tool designed for CISOs, CIOs, SOC & Senior IT managers to specifically address their pain points by providing security, comprehensive awareness, understanding and insight into the health and maturity of their entire enterprise cybersecurity ecosystem. Working across security domains, Cyber Observer connects to enterprise IT and security tools to continuously monitor optimization, gaps, and baseline network behavior via a patented core analytics engine. Using an intuitive score-based interface, Cyber Observer delivers the leading edge of comprehensive security management & awareness - cutting complexity, informing risk, driving workplans and powering critical budget decisions.

- Time to Deploy: Up to 4 hours
- Deployment method: OVA (Virtual Machine)
- Time to add new tool: 1-2 hours
- Real value Demonstrated: Within hours

Executive & Senior-level Security Management

Cyber Observer delivers value according to three broad vectors:

- Configuration & optimization analysis of each tool in your cyber security suite, providing insights and recommendations into tools that are unoptimized or misconfigured,
- Security gap analysis across the entirety of your network to indicate areas requiring investment and further attention, including recommendations to improve your network security maturity,
- Core analytics engine that establishes a baseline behavior of your network as a whole (not primarily reliant on often-unfeasible log file analysis & prioritization) and monitors in near-real time, sending alerts in cases of deviations.

Cyber Observer is not comparable to a bulky SIEM solution and can be deployed to any corporate or government network in up to four hours. In most instances requiring read-only permissions, Cyber Observer focuses on delivering comprehensive and intuitive information & insights that facilitate awareness and decision-making.

Figure 1: Cyber Observer CISO main screen – a healthy functioning network

Figure 2: Deviation from normal behavior. Drops below threshold behavior across multiple domains may be indicative of a security event.

Cybersecurity Domains

As the above two diagrams show, the platform measures network health out-of-the-box via pre-configured security domains, including:

- Account Management
- Malware Defenses
- Secure Network
- Secure Configuration
- Secure Application
- Data security
- Incident Management
- Security Assessment
- Physical Security

And is wholly configurable to add, remove, and create your own according to your internal enterprise priorities.

Critical Security Controls (CSCs)

Critical Security Controls (CSCs) are the most fundamental data, processes and actions that every enterprise should employ in order to prevent, alert, and respond to the attacks that are plaguing enterprises today.

Cyber Observer's methodology is based on continuously implementing, retrieving and analyzing CSCs from all relevant data sources existing in the organization. CSCs are customized to meet the needs of each organization, and quantified to establish baselines for each domain and for overall security within the cyber eco-system.

Cyber Observer's CSC database is based on recommendations from cybersecurity industry leaders including: NIST, ENISA, ISO, NERC-CIP, the Council on CyberSecurity and more, as well as requests from CISO's and the company's knowledge on how to effectively manage complicated cyber security eco-system. The CSC database is updated continuously based on new threats, relevant information, tools and intelligence received from cybersecurity agencies.

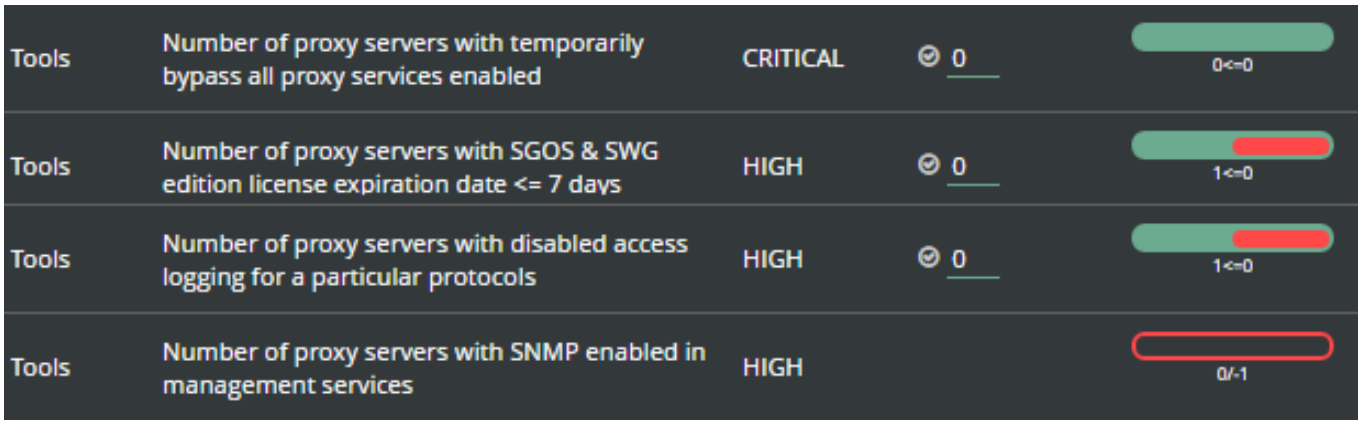

Figure 3: Sample SCSs, showing various criticalities and details.

Automatically Build a Cyber-secure Enterprise Ecosystem

Cyber Observer automatically builds and assesses a security eco-system based on an enterprise's existing cybersecurity infrastructure. It then quantifies baseline security and vulnerability levels in various domains and customizes Critical Security Controls to ensure continuous and robust enterprise protection.

Evaluate Security Status in Real-Time

Once the existing cybersecurity eco-system is defined and in place, Cyber Observer monitors and delivers alerts regarding deviations, security breaches, potential risks and threats, in specific areas and as they relate to other systems across the enterprise. Security status across the enterprise is quantified and presented in clear, easy-to-read infographic views.

Gain Comprehensive Coverage from Security Threats

Cyber Observer not only identifies threats, but also alerts to areas of vulnerability within the enterprise which compromise its security eco-system. These can include alerts regarding improperly functioning infrastructure in the face of emerging threats, or deviations from proper security processes operation. Cyber Observer also evaluates each domain in the security eco-system across three spheres: CISO POV as defender, Hacker POV as an attacker and IT Infrastructure POV as an attack/security event result. Based on the security eco-system installed, any suspicious activity across these spheres is detected, analyzed for potential inter-relatedness, and reported.

Proactive Cyber Security Approach

Effective cyber defense ideally prevent an incident from taking place. The best action is a pre-emptive and proactive approach. Cyber Observer utilizes a proactive mindset and approach in order to protect enterprise's infrastructure and sensitive corporate data from attack before the attackers strike. Cyber Observer's proactive cybersecurity approach provides actionable intelligence so you can recognize vulnerabilities and potential attack vectors and mitigate them before attackers gain a foothold in your network. Proactive Cybersecurity puts you firmly in control of your security eco-system.

Maintain Awareness in a Constantly Changing Environment

Cyber Observer enables security professionals to maintain management control in a highly dynamic environment, where new technologies are constantly being introduced, along with new and unexpected threats. Data is provided in a clear, real time, role-based views, with a design emphasis on communicating data clearly and easily to ensure that CISOs and senior Infosec managers received the relevant data easily, expediting decisions and facilitating competent accountability for network security.

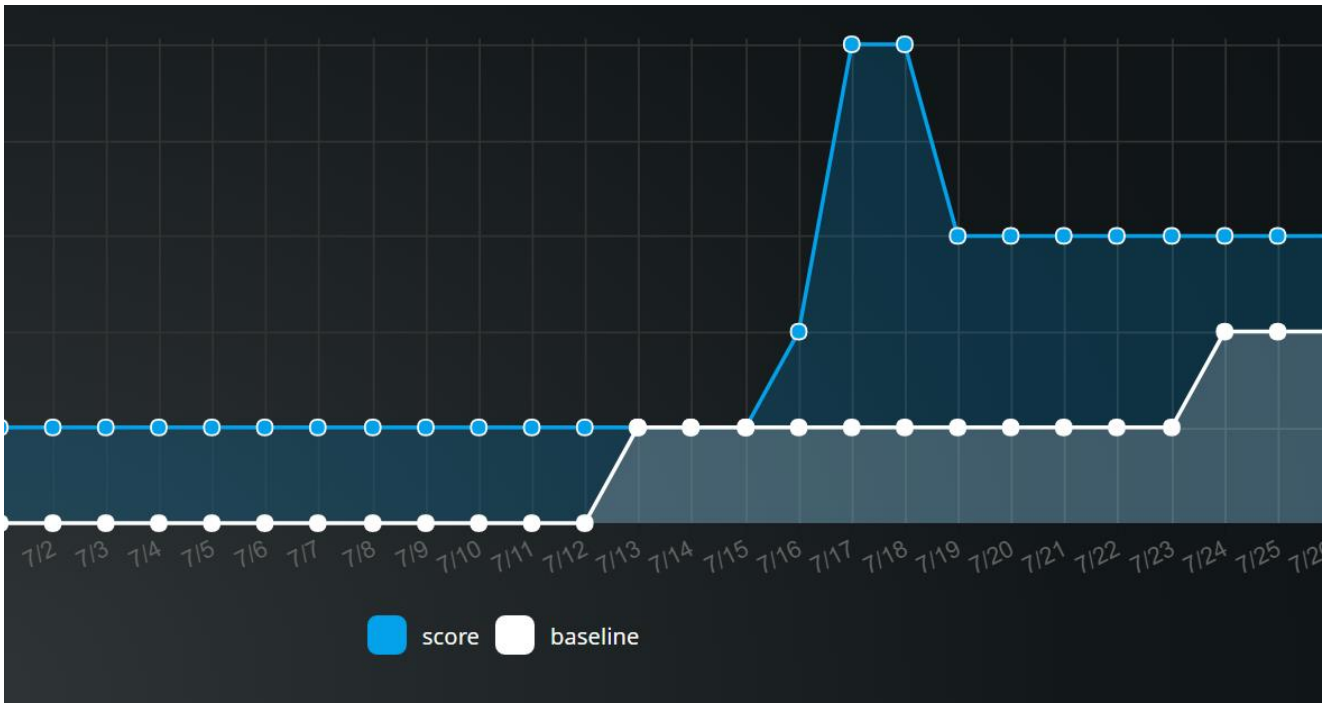

Figure 4: Historical Reference, showing improving overall (blue) and baseline (white) scores.

Cyber Observer – Complete Executive-Level Network Cybersecurity Awareness