Healthcare and BAP
By Jeffrey Lush

Healthcare and Cyber Threat Protection

BAP is a unique cyber security software that aligns cyber security events to cyber security policies that are designed to protect the IT environment. To date, cyber security solutions focus on either threat or standards, with no clear relationship between the threat and standards, and limited if any understanding of the impact of patient care activities.

Healthcare and Cyber Threat
Healthcare presents unique challenges with multiple sensors and access to critical patient information. Imagine collecting patient data electronically on a device that has moderate security, accessing data collected by sensors that are internal or external to the patient that have minimal, if any security, and transmitting the data to the data center with unknown levels of security. BAP provides the software that aligns threat to security standards. Understanding that a cyber compromise has occurred, without measuring risk and/or impact against the security standards, is like having a muscle with no brain to receive the result of the muscles effort. BAP builds the link between the threat (real-time events) and the security standards.

Threat Detection requires analysis
With security policies established, automated threat detection requires continuous monitoring of the “health”/viability” of the established security configurations. Analyze real-time events occurring within the environment and interpret them into cyber security threat, automatically. Today analysts review, often with the assistance of log aggregators, thousands of events to discover cyber threat within the organization. Unfortunately, due to the amount of data and cyber threat that exists within our environments today, automation, like BAP is needed to truly detect internal and external cyber threats.

Threat Detection: Mapping events to healthcare outcomes
Established security configurations and policies constitute a security baseline for your organization, although actively correlating hardware, software and security events within your environment truly protects an organization. Understand with exactness the origin of the threat in minutes® using the BAP Artificial Intelligence (bapAI) that constantly monitors threat providing near real-time impact analysis of the health of your security configurations. The bapFramework enables the environment to manage cyber security policies and configurations... while providing accountability through monitoring events that impact the cyber health of your organization. BAP is the next generation of automated threat detection.
Cyber security is not an annual event

Cybersecurity is not isolated to a point in time. Rather, cybersecurity should be continuous threat detection. BAP enables continuous threat detection by establishing security standards and security policies, creating a known good secure state and then validating the integrity of your established security standards and policies.

HIPAA (Health Insurance Portability and Accountability Act) provides direction for security standards and process that directly relates to healthcare. A security penetration / attack can result in loss of patient data and incorrect payee and payer data resulting in an adverse financial impact for the healthcare organization.

Security policy is the collection of security standards often motivated by compliance requirements like HIPAA, PCI-DSS, PII, etc. A known good secure state is a great point to measure success or failure with your cyber security strategy. To accurately measure threat within the environment, we must know what "right / secure" looks like, or in other words what is the known good secure state of my IT (Information Technology) environment.

Security Health

BAP provides the tools to establish security standards and policies coupled with the ability to measure the "health" of the security standard and its relationship to the security policy. BAP provides users with threat awareness based upon real-time events occurring within the environment that are then aligned to an organization’s security standards and policies.

The ability to measure actual events against established security policies and standards is unheard-of and greatly needed within IT environments. Many cybersecurity products measure threat to a specific component within your IT infrastructure. The collection of threats related to any number of components/variables in the environment, at a random collection sequence, is often the cause of an effective cyber attack.

Cyber Health and Patient Care

It is certainly advantageous to know that my firewall has been compromised, although as a result of that compromise how will the attack impact patient care? What does that compromise really mean as it relates with other security standards I have established within my environment?

An isolated, component-based threat detection is less effective than a "system" based threat detection that BAP provides. Cyberthrust includes multiple variables at an ever-changing frequency. If our cyber threat was always isolated to a specific component, like a firewall or a server within our IT infrastructure, then building a security wall around those components and monitoring for threat would be relatively straightforward.

However, history proves that cyber criminals attack every soft spot within our IT infrastructure, ranging from software to hardware and everything in between. If you’re going to accomplish cyber health, or at least get closer to a more secure environment, you must take a "system" view, a holistic perspective of cyber threat within your environment, and BAP software was designed specifically to address this need.
How can I use BAP to accomplish system-based threat detection?

The BAP framework is very flexible and can assist in the development of security policies and standards in multiple ways. The following is one example of how an environment might implement security standards and policy to enhance their security health.

1. What level of security do you need?

Is there a specific authorization, like HIPAA or certification that you require? You can leverage FIPS 199 or FIPS 200 to help find the level of security you need? You will need to establish what that baseline standard should look like. The BAP Welcome interview is designed to assist users in discovering their security needs.

2. Building backward

Once you’ve established your security needs, we can start building… backward. You have options at this point. Would you like to build security policy and standards within your organization? Or would you like to get a jumpstart by visiting the BAP marketplace and downloading security policies and standards for your environment? The BAP controls (standards) and BAP baselines (policies) are generic by nature and require some effort on your part, although in many cases the components (security standards/policies) you download from the BAP marketplace will get you about 85% the way to your cyber security objectives. If you do not have cyber expertise in house, BAP services can assist you in customizing your security standards and policies.

If you would like to build your policies and standards from scratch, the BAP framework enables that activity as well. The easiest way to get started is to define the key objectives for your cybersecurity policy. Some of those key objectives should include access control, contingency plan, media types, encryption, network, and many more.

Perhaps look at the control families established in the NIST 800-53, which may give you a good starting point for developing your own controls (standards). Many organizations leverage the NIST 800-53 controls at their starting point, then customize controls to meet specific needs in their environment. The BAP framework by default includes all the NIST 800-53 controls to get you started quickly.

3. Building your library

Once you have established your security controls (standards), you have a library you can build upon for multiple security policies (security baselines). A popular feature of the BAP framework is the ability to inherit any security standard that is being utilized in your system into multiple security policies (baselines) that define your organization’s objectives. This is a key necessity of any viable cyber security plan and something that BAP easily facilitates.

4. The security standard / control

Remember that a security control (standard) is made up of three primary subsections: the standard/objective, the implementation of that standard/objective within your environment and/or within a specific security policy, and the validation/validity/health of that security...
standard within your security policy. BAP provides flexibility to adjust the implementation of the security standard/control per security policy/baselines while maintaining the integrity of the security objective or what is referred to as the standard/control language. In addition, as security standards/controls are applied to specific, and often multiple security policy/baselines, the priority impact of that standard as it relates to that individual purity policy may be adjusted as well.

5. Real-time health of the standard

Now that we’ve established our security standards and policies, we need to understand the “cyber health” of the security standard implemented. To establish the real-time health of the security standard as an individual component or within your security policy, we must understand and process the hardware and software events that your environment will generate.

6. Hardware and Software Impact

Hardware and software within your environment play a very important role in establishing the integrity of a continuous threat detection monitoring architecture. Once you identify the hardware and software used in your environment, with the bapInterview assistance, you can leverage the BAP framework to establish a relationship between actual events and the security standards you have established. Events are aligned to the security standards and security standards are grouped by security policies.

Once the events generated by hardware and software are aligned to the security controls within your environment, your effort will be to align the security standards and policies moving forward. For many environments, established sets of security standard/groups with security policies serve as the foundation for cyber security strategy. With the BAP framework, customers can perform one-to-one mappings or many to one mappings to establish their security health.

“Cyber cost should decrease as you become more secure”

7. Drive down cost

BAP believes strongly that cyber security becomes easier as you secure more items within your environment. In addition, it should not cost more, in fact the BAP pricing model ensures that as you increase your security policies while inheriting security standards, your cost for new security policy decreases.