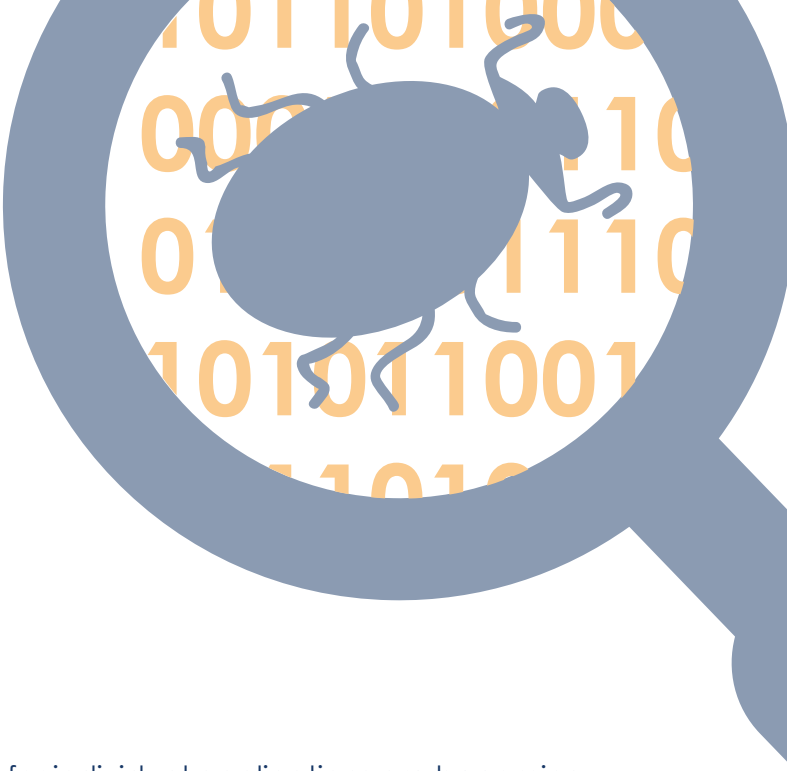
BLACK OPS ADAPTIVE SECURITY

WORK QUICKLY & SECURELY

Enterprise Integration | entint.com | 888-848-9332 | info@entint.com



We've all heard about the benefits of automating system configurations to avoid human error, but introducing it to your infrastructure may be easier said than done.

Is your business protected against security threats? The answer may depend on how often your engineers do manual work.

Smart business leaders will minimize the probability of human error, and security automation is the best way to minimize risk. However, many enterprise organizations struggle with implementing holistic solutions.

Automation is the force-multiplier enterprises need. IT is expected to be leaner and more responsive to new lines of business, while maintaining more complex infrastructure with the same (or fewer) staff. On top of that, custom hybrid architectures for individual applications are becoming more common. Budgets and engineering time are spread thin.

AUTOMATION ALLOWS ENTERPRISES TO MATCH STARTUP PROJECT DEVELOPMENT SPEEDS

Automation may not shrink your engineering headcount, but it will allow your engineers to work more quickly and securely. Ultimately, automation will help enterprises move as fast as startups. As abstraction increases, it doesn't matter if you're deploying to 10 servers or to 10,000 servers. Automation puts enterprises that want to match startup project development speeds on an equal playing field.

Enterprise Integration ("EI") recognized the need for a holistic approach to threat management from the endpoint to the cloud and has spent many years developing the process and the technology required to gain the full value of that automated approach to security. Having a layered approach with interwoven technologies provides an enterprise with the best possible identification and threat resolution paths.

AUTOMATED SECURITY MONITORING WITHIN THE SERVICE DESK

Enterprise IT environments have never been more complex. Hybrid clouds are on the rise, and hundreds or even thousands of applications are spread across multiple environments at varying stages of cloud readiness.

When multiple clouds support individual applications, it is crucial that engineers are able to monitor the entire infrastructure in a single interface looking for IOCs. When downtime or security attacks occur, it usually takes more time for an engineer to find the problem than to fix it. Unified monitoring gives engineers the intelligence they need protect core assets and contain the attack. Enterprises already use tools to monitor their environments, but only monitor individual systems without a full 360° view of the endpoint or multiple clouds. Instead, they look for tools that offer automated reporting and trend analysis across on-premises and cloud environments, sophisticated intrusion detection tools, and governance features to help stay compliant.

The missing link in identifying the root cause of a problem, or correlating incidents across the environment has been having the ability to know what happened just before the alert was issued, before the user clicked on the link, or before an odd behavior was recognized.

CHECKING INSTANCES ACROSS THE ENVIRONMENT

On the day Heartbleed was announced in 2014, many companies found themselves scrambling to update SSL across hundreds of thousands of servers and virtual instances.

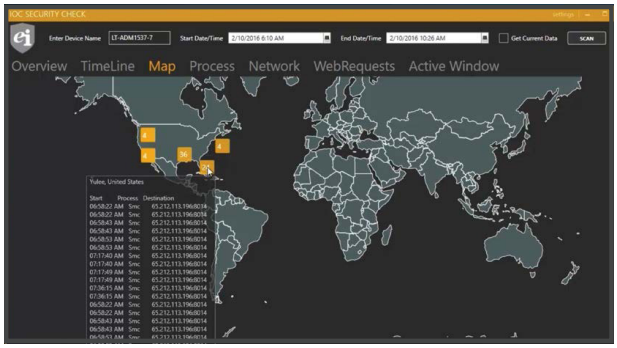
In traditional IT, a major vulnerability like Heartbleed would mean every system engineer on staff working furiously for 18 hours to manually patch servers. For companies with Digital Robotics, the only necessary change was a single line in the manifests to make sure the newly released version was running instead.

Digital Robotics are declarative management tools that monitor, configure instances, virtualized servers, or even bare metal servers. When a new instance is launched, these tools are responsible for getting that instance ready for production, including security-sensitive configuration tasks like binding the

instance to central authentication, installing intrusion detection agents, requiring multi-factor authentication, etc.

But crucially for security, these tools also enforce their manifests and will proactively change configurations on previously launched instances. This has two implications. First, as described above, it is possible to respond to security vulnerabilities quickly across all environments. Second, it also means companies can guarantee that these historical vulnerabilities stay patched, since any changes or mistakes on individual instances will be automatically updated once the script interacts with the instance. This prevents accidental regressions in security configurations.

LEVERAGING DIGITAL ROBOTICS TO IDENTIFY THREATS AND PROVIDE AUTOMATED ACTIONABLE PATHS TO RESOLUTION



Monitoring can be seen as a necessary evil depending of you are monitoring, being monitored or responding to monitoring alerts. Quite frankly, when something goes wrong, the first question is often "Was this being monitored?" followed by "Why didn't the monitoring catch it?" and "Why didn't we respond to the alert?"
Monitoring can help identify trends, which can reduce time to respond and ultimately mitigate threat. Monitoring is so much more than up/down and integrating the various functions of a device into monitoring is most valuable. Here are a few examples.
Years ago, EI created a Threat Service, which reads from real-time threat feeds and blocks malicious entities of all nature. This has reduced support costs, increased the security response time to the evolving and ever changing threat landscape.

EI also created an Endpoint Diagnostics tool, which in seconds, can provide system information (workstation name, image version and backup info); IP information (including DNS and DHCP); Hardware information (model, serial number, memory and available C drive space); and Application Information (OS, AV and application versions). Lastly, the tool can does automatic connectivity tests showing connectivity as up/down and the average wait time.

The missing link in identifying the root cause of a problem, or correlating incidents across the environment has been having the ability to know what happened just before the alert was issued, before the user clicked on the link, or before an odd behavior was recognized.

Most recently, EI's office of Automaton has developed a revolutionary tool that lets you go back in time. The Indicator of Compromise tool enables service desk and security personnel to see what was happening on an endpoint prior to the alert.

The tool can tell where the user was going on the internet, what processes were running, if any of those processes were impacted in some way, if any unusual activity was generated on the endpoint, if there was a suspicious communication to or from the device.

OUR SECURITY

PROTECTION & RESOLUTION EFFORTS ARE

PROTECTIVE NOT REACTIVE

Better yet, the tool can correlate the logs to tell if this was a single hit or if there is about to be a much larger problem, which in turn makes the security protection and resolution efforts protective rather that reactive.

Response time can be dramatically reduced and response can be targeted to specific instances for a much more expedient resolution. In addition, detection of such instances enables security engineers to further automate recognition and response, which in turn reduces overhead and risk. Lastly, this tool has great value in the compliance space.

ENTERPRISE INTEGRATION

ADAPTIVE SECURITY

entint.com | 888-848-9332 | info@entint.com