

Automating Security Intelligence

Somewhere deep inside the hundreds of millions of pieces of event data produced daily by routers, firewalls, identity and access management infrastructure, applications and all other components of a large enterprise network and security infrastructure are the key clues for how to avert potential disaster. In fact, there is everything you need to respond to ongoing threat levels, internally and externally. While manually sifting through it all is good practice for security forensics and essential for proving business compliance, it is typically a hugely inefficient process; even more so when placed under necessarily heavy scrutiny.

AUTOMATED IT RATING: 4.5

This advisory describes the process and impact of automating the security intelligence of your network.

- **Situation Analysis (Before & After Automation)**
- **The Business Criticality of Security Intelligence**
- **Automation Impacts**
 - **Running Costs**
 - **Time/Labour**
 - **Space & Power**
 - **Decision Making**
 - **Uptime**
- **Implementing Automation**
- **Q1 Labs Solutions**

Situation Analysis

Before Automation

- External attacks and fraudulent activity by insiders are missed
- It consumes large amounts of time and focus to manage the sheer weight of new security event data spewing out of your network's thousands of devices
- Network and security operations teams are silo'd from each other, cannot leverage key data of interest to both teams, and are slowed in response to network threats
- Each device or device-set has its own attendant proprietary logging system/protocol, which consumes additional resources including space and power. Stranded investments may also have already been made in log management products, network visibility products and obsolete security event management systems.
- The 'skill' of understanding how to collect and interrogate event data from disparate networked sources is difficult to transfer and is often exclusively silo'd among the team.
- On the surface, each piece of event data is conceivably of 'equal merit' in terms of its value to decision-making at least until it can be combined with context from other data sources. A tremendous amount of time is wasted in prioritising responses into a manageable range of tasks
- There is real concern that the present 'best effort' security intelligence system (should one even exist in whole or part) is not only inefficient, but also endangers the ongoing security and compliance status of the business. It is unlikely to offer any value in the event of a sustained attack, or an urgent audit.

After Automation

- Total security intelligence enables the detection of cross-enterprise threats that were previously being missed
- Time is no longer spent interrogating multiple sources for event data; instead all the information is collated into a single point and converted into security intelligence.
- Space/power and other resources are also conserved by a minimal hardware footprint for interpreting security intelligence.
- Out-of-the-box security value with easy to understand rules, results and reports, so any authorised member of the IT team can 'pick-up' security intelligence duties and search, analyse and respond to security log information.
- The IT team works from 10 or so prioritised tasks generated by the event log information, rather than randomly responding to issues of perceived importance that have been spotted 'out-of-context'.
- Compliance and security responsiveness is far more assured, even with respect to zero-day attacks and sudden audit impositions.

The Business Criticality of Security Intelligence

Networked infrastructure elements are good at collecting evidence, and lots of it. Yet it is the process of managing all of this data and converting it into intelligence about your threat/fraud detection 'must-dos', network/security operations needs and compliance outputs which is absolutely essential.

Automation Impacts

Running Costs

HIGH 😊

The bottom line impact of automating security intelligence is the radical reduction in operating costs, both in terms of skills employed and the consolidation of countless devices (log management products, network visibility engines, behavior analytics, proprietary logging appliances etc.) into a single interface stream/single product to configure, learn and maintain.

Time/Labour

HIGH 😊

The ability to locate and analyse information quickly – almost instantaneously – saves incredible amounts of time. For example, should a serious security incident be suspected, organisations may need to shut-down devices for several hours at a time and divert precious resources simply to find the location of a threat. A typical 500-user organisation will save between three and five man-days per month by automating security intelligence.

With a fully automated solution in place, IT departments can quickly – in a matter of minutes – locate the individual issue and shut down the activity before any damage can be wrought. Total security intelligence solutions can deliver significant data reduction capability for prioritised incident response to the order of 500,000:1 (accurately prioritising the one important incident out of 500,000 other pieces of security event information).

Automating security intelligence will also support the ongoing convergence and consolidation of network teams and security teams within your organisation. Even if your organisation is maintaining those teams as separate entities, automating security intelligence promotes the efficient sharing of critical data and avoids the possibility of anything important 'falling through the gaps'.

Space/Power

MED 😐

Automating security intelligence reduces the impact on space and power resources. For example, a large organisation generating 5,000 security events per second can run all of their security intelligence requirements out of a single 2U appliance. Using a virtualised form-factor, this impact can be reduced further still.

Beware of what analysts describe as 'first generation SIEM systems', which are essentially large 'ERP-like' software deployments with associated RDBMs costs. The next generation of SIEM uses far more efficient and performance-orientated database as well as an easy to deploy and maintain appliance form-factor.

Decision Making

MED 😐

Security information and log event data is critical to the decision making process, though its success rests upon deploying a system capable of converting that into reliable, rapidly accessible and priority-led intelligence. An automated approach achieves just that. In addition, it provides all the intelligence an auditor needs to undertake a compliance inspection, or for senior managers to interrogate any aspect of network history.

The heterogeneous nature to true automated approach to security intelligence also supports transparency and flexibility in the procurement process. Knowing how painful and time-consuming it can be (in terms of making provisions for security event data etc.) to introduce a new vendor technology into any existing infrastructure can cloud and constrain capital investment judgements. Now you can deploy what you want without concern for additional security intelligence overheads.

Uptime

HIGH 😊

An efficient, rapid and comprehensive security intelligence system will clearly mitigate the risks to your organisation. Specifically, it will lead to a reduction in human error in terms of preventing individuals from:

- jumping to the wrong conclusions and wasting valuable resources on wild goose chases because of a failure of analysis
- having to cover for absent team members who own device/technology specific event data skills
- forgetting or overlooking arcane processes which follow no policy or process other than those developed by habit, distant memory or scraps of paper.

Implementing Automation

Automating security intelligence can be accomplished within minutes, particularly if solutions with 'data discovery' and auto-configuration capabilities are employed. Even with tweaking and user training, the entire process can be accomplished within a few days. Additionally, it may even be the case that the act of implementing a solution to

automate security intelligence uncovers areas of historic processes which failed to account for individual devices and systems on the network.

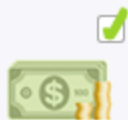
Available technology should be flexible to all deployment scenarios, including among comparatively small/mid-sized businesses who may not have considered security intelligence solutions previously. Only very large organisations generating over 500 million security events per day would conceivably require an architecture where more than a single SIEM unit would need to be run in alignment.

Q1 Labs Solutions

This advisory has been produced with support from Q1 Labs, a global provider of high-value, cost-effective network security management products. For more information on how Q1 Labs successfully integrates previously disparate functions such as log management, network behavior analytics and security event management into a total security intelligence solution for businesses of all sizes, visit www.q1labs.com

[Click here](#) to view a case study on UDR

[Click here](#) to download the Q1 Labs 'Business Case for a Next Generation SIEM' white paper



SLASH COSTS

- Lower hardware TCO
- Better use of existing hardware
- Slash opex for incident response by over 75%
- Less hardware needed
- Less than 12 month return on investment



SAVE MAN-HOURS

- Free up skills for innovation
- Support security/network team convergence
- Typical 500 user organisation can save 3-5 man-days per month



CUT SPACE/POWER

- Maximise virtualisation opportunities
- Reduce network and hardware footprint
- Better ROI for storage strategy



BETTER DECISION-MAKING

- Dramatically increase efficiency of security management and intelligence gathering (500,000:1 data reduction/prioritisation capability for improved incident response)
- Dedicate less resources to fire-fighting
- Immediate readiness for compliance/auditing
- Unconstrained future network/security procurement



BOOST UPTIME

- Underwrite critical network services
- Mitigate unnecessary human error/intervention
- Improve security, event zero-day attacks