WE SEE WHAT YOU DON'T SEE

Integrated Cybersecurity Solution

A CYBERNATICS WHITE PAPER

WWW.CYBERNATICS.IO

cybernatics

A CASE FOR AN INTEGRATED CYBERSECURITY SOLUTION FOR SMALL AND MEDIUM ENTERPRISES

ABSTRACT

A key goal for companies today is business resilience, of which cyber resilience is a key contributor. For cyber this means focusing on how to continue operations, providing services to customers, in spite of cyber attacks and incidents. Although much of the emphasis must be on how to react appropriately, equally important are how the company secures its systems and access to those along with how it learns about an incident in a timely manner and how the company can deal in an automated fashion with more "routine" incidents and vulnerabilities. Critical to delivering more automation and a better view to deal with issues is a more integrated CAASM-SIEM-XDR-VM set of tools and capabilities for the infrastructure security, whether on-premise or in the cloud. Current versions of these tools generally come from multiple vendors and sit in layers but are not integrated to provide what most companies need – a means to deal in automated fashion with many identified vulnerabilities and routine incidents and provide the critical, timely information for senior management action when they need to respond personally. This paper explains the different components, their capabilities and benefits, and the overall benefit to resilience to be gained from more integration among these tools.

WHY CYBERNATICS?

Improve Threat Visibility

Integrate your on-premises and cloud security infrastructures to minimise risk.

Seamless Integration

Simplify cybersecurity with our all-in-one solution, consolidating services and eliminating complexity.

Achieving Regulatory Compliance

Achieve compliance effortlessly with our solution, ensuring adherence to regulations and maintaining robust security.

SME CYBER RESILIENCE REQUIRES MORE INTEGRATED CAPABILITIES

Cybersecurity must be a means to ensure a business remains operational for its customers: that its services are available when customers want them and that any data associated with those services is adequately protected and fit for purpose. This is the essence of cyber resilience. Tools and processes to achieve this outcome must help to prevent problems and detect and deal with problems as they arise. Given their smaller revenue, and consequently expense base, Small and Medium (SME) organisations in particular have to make the most of all the cybersecurity tools and the staff they employ or the services they outsource. SMEs do not have the luxury of multiple dedicated teams for each aspect of cybersecurity, nor of many specialised cybersecurity tools – integrated tools and services at a reasonable cost are needed.

ASSETS – START AT THE BEGINNING

Unfortunately, too few companies start where they should: with defining their assets and the importance of those assets to their business, and then with tracking security as it relates to the assets and the business. In 2022 Gartner pointed out the need for a better business understanding of the security posture:

"A programmatic approach to a set of questions that in their entirety begin to answer the question "how exposed are we?" is necessary. Organisations are beginning to reorient their priorities, end users are beginning to segregate these priorities into three distinct areas and ask: "what does my organization look like from an attacker's point of view, and how should it find and prioritise the issues attackers will see first?"; "what software is present and what configuration has my organization set that will make it vulnerable to attack?"; "what would happen if an attacker carried out a campaign against my organization's infrastructure, how would its defences cope and how would processes perform?"[i]

Organisations are starting to consider the asset attack surface and the effect of that on their risk posture, so tools to assist with this consideration are important. The recent Cyber Asset Attack Surface Management (CAASM) solutions assist organisations with asset related views by combining data from various underlying security systems together with threat data. CAASM solutions generally offer API integration to other cybersecurity systems along with the defined asset base to provide an asset-based view of the vulnerabilities and security issues, usually with a threat input and an ability to compare this view to regulatory and industry standards for compliance management. And theoretically this asset attack surface view should give organisations a better understanding of the risk involved with their assets, and of what they need to do to improve their cybersecurity situation and the resulting effect on business risk and resilience for resolving vulnerabilities. But does an SME actually need a separate solution (i.e., CAASM) to get this view?

CONFIGURATION, VULNERABILITY, MALWARE AND PROBLEM MANAGEMENT

Securing technology requires proper configuration and vulnerability management across all the assets, with the ability to understand when problems arise (such as from malware) and to deal with them in a timely and appropriate manner. Cybersecurity tools covering these areas tend to be specialised for Endpoint Detection and Response (EDR), vulnerability management (VM), views across assets (CAASM), logging and monitoring (SIEM), and automation of response to problems (SOAR). Extended Detection and Response (XDR) for endpoints is seeking to automate some detection and response for endpoints, but does not address the broader detection and response areas covered by SIEM/SOAR. From a technical and process perspective how much do these tools overlap or complement each other, and is there a case for integrating the capability more, at least for SMEs; can the integrated capability provide a better view of compliance to share with management, boards and regulators?

ENDPOINT PROTECTION: EDR/MDR/XDR

Endpoint protection started with tools to detect and deal locally with viruses and other forms of malware, and has expanded to address a variety of threats to endpoints, servers, cloud infrastructure, applications, and the like. Malware refers to any malicious applications or code that damages or disrupts endpoint systems or the data on the systems. Initial basic capabilities merged to become Endpoint Detection and Response (EDR), which Gartner described as "solutions that record and store endpoint-system-level behaviours, use various data analytics techniques to detect suspicious system behaviour, provide contextual information, block malicious activity, and provide remediation suggestions to restore affected systems. EDR solutions must provide the following four primary capabilities: (1) Detect security incidents, (2) Contain the incident at the endpoint, (3) Investigate security incidents, (4) Provide remediation guidance."[i] From the initial Endpoint Detection and Response (EDR) the industry has been shifting to Managed Detection and Response (MDR) and now to XDR.

MDR is a "cybersecurity service that combines technology and human expertise to perform threat hunting, monitoring and response"[iii] to achieve rapid identification of threats and limit their impact without increasing the number of staff. MDR increases the automation associated with identifying and responding to issues, so fewer people need to be involved in monitoring and responding to alerts and identified issues.

XDR builds on the MDR idea by increasing the capability with analytics, threat data and even AI to correlate alerts and automatically respond to some kinds of problems while alerting relevant staff to others. Again the idea is more automation to decrease the need for extensive monitoring of the alerts, and to increase the ability of the system to handle more alerts and issues before escalating to staff. For most companies increasing the capability of the system to deal automatically with many issues makes sense – in this case organisations may want the ability to modify the rules for when to apply automated responses, and how to handle escalation of more serious incidents.

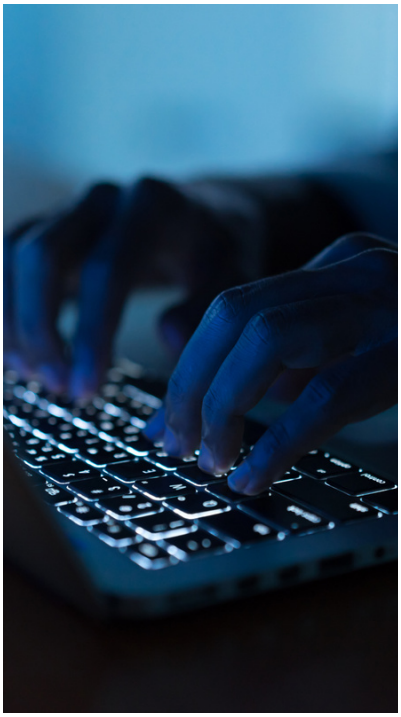
SYSTEM CONFIGURATION AND VULNERABILITY MANAGEMENT

Vulnerability management and configuration management complement one another for securing the organization's infrastructure, whether on-premise or in the cloud. Vulnerability management is a risk-based approach to discovering, prioritising, and remediating vulnerabilities and misconfigurations[iv]. Configuration management, on the other hand, helps to ensure that devices are configured in a secure manner (some aspects of "hardening"), that changes to device security settings are tracked and approved, and that systems are compliant with security policies[v].

Vulnerability management helps organisations identify and address potential security weaknesses, while configuration management helps ensure that devices are configured securely and remain so over time.By identifying vulnerabilities and misconfigurations, organisations can take steps to remediate them before they can be exploited by attackers. By ensuring that devices are configured securely, organisations can reduce their overall risk exposure and help prevent attacks from succeeding. Difficulties arise for most organisations in determining whether vulnerabilities are truly relevant for the systems used by the organisation, and the relative priorities for remediating those vulnerabilities and for scheduling remediations that are not urgent.

IDENTITY AND ACCESS MANAGEMENT (IAM)

Securing access to systems and data is equally critical for an organisation's security. Organisations need to implement controls to ensure least privilege access for both their staff and their customers. Essentially, people should only be able to access the systems, applications and data that correspond with their roles and the functions and data they need to complete their designated tasks. It also means that oversight of some activities should be empowered, and access to oversight functions should not be provided to the same person being reviewed.



Various functions and tools help to provide this capability along with a view of the control effectiveness of those tools. Identity management checks an access attempt against a database of users with the right to access certain systems and information. Note that the list should contain both the relevant user and the appropriate level of access for that use. This role could vary from a privileged role for an administrator to a read only role for someone reading data in an application (eg, checking the amount in a savings account). The process of checking the request to access against the approved list is "authentication". A password helps to ensure that only the specific user is allowed to gain the allowed access. Organisations use Multi-Factor Authentication to provide another layer of assurance that the user seeking to access a system, application or data is the correct user. Many companies use Single Sign On (SSO) to provide one means for users to access resources and applications. For enhanced protection of critical resources some organisations use Privileged Access Management that can include logging all actions conducted by any user that access these accounts.

From a management perspective an organization wants to know that the IAM controls it needs are deployed, being used correctly and that any identified issues and attacks are alerted to the appropriate staff and acted upon correctly in a timely manner. Such information can come directly from these systems or via a log collection and event management system such as a SIEM.

SIEM/SOAR

Security Information and Event Management enables an organisation to capture data on events and alerts across network and cloud assets, other security systems, users, and applications to detect security threats, analyze them and respond appropriately to security issues. Security Orchestration, Automation and Response (SOAR) augments SIEM by automating responses to certain kinds of alerts/incidents, usually using machine learning/AI together with threat intelligence to define the process and the response for the defined alerts/incidents.

Larger organisations may have their own Security Operations Centre (SOC) where an operations team uses the SIEM/SOAR systems to manage security incidents and responses to those incidents. Some SMEs may outsource this capability to a third party which then obtains the logs and other data from the SMEs' systems, and either responds directly or alerts the SME staff to respond depending on the severity of an incident.

Most SMEs have limited cyber teams and thus do not have Security Operations Centres, but still need some form of alerting and response management capabilities. Some SMEs may also need archives of logs to comply with regulatory requirements and show proper governance.

What Might Be Integrated?

Since most SMEs need a combination of the above capabilities, which of these might be integrated into a single solution to give a "minimum viable" cybersecurity solution covering the infrastructure and key alerts? The following table provides an overview of the main aspects for these capabilities, and highlights where the capabilities provide complementary protection and use similar data.

	CAASM	**XDR**	**SOAR**	**SIEM**	**VM**
Purpose	Asset & attack surface visibility & protection	Extended endpoint detection and response	Automation of responses for certain kinds of alerts/incidents to decrease response time	Proactive threat detection, investigation & response	Identification, assessment, reporting & managing remediation cyber vulnerabilities on endpoints & systems
User roles	• Security mgt • Compliance team • Risk • SOC team	• SOC team	• SOC team	• SOC team	• VM team • IT operations • Security mgt • Risk
Data inputs	• Asset list • Data from other cyber security systems via APIs • Scan results • Threat intelligence	• Telemetry from endpoints & systems • Data from other security systems (for network, email, identity, cloud, CASB, etc) • Threat intelligence	• Alert, event or other data that indicate a need to start a series of actions • SIEM data	• Logs from devices and systems on & part of network, security systems, applications, containers IAM systems, etc • Logs from cloud (can be preprocessed) • User log data • Incident elevation list • EoI/incident mgt tracking	• Threat intelligence • Vulnerability data • System data • Business priorities • Criteria for resolving priorities of vulnerabilities • Infra asset list • Remediation schedules & changes made
Result of processing	• Central view of all Cyber asset inventory • Feedback and reports in dashboards, charts • Automated handling of some actions • Query results	• Incident alerting • Automated responses to certain incidents • Explanations of attack contexts • Graphical displays where appropriate	• Automate repetitive tasks • Reports of actions status	• Monitoring for (identification of) events and differences from norm • Identification of possible incidents • Details for investigation • Tracking of actions taken	• Prioritised list of relevant vulnerabilities for remediation • Reports of list, remediation status & performance against agreed criteria

We can see that a SIEM-like solution could be a common platform for integrating the data for these capabilities, with EDR and VM components feeding into this platform that has CAASM-like abilities to manage assets and present the results. The common platform would also include the ability to apply ML/AI on the incoming data to deal automatically with some situations and to determine what events to report to whom and to track resolution of vulnerabilities and of events. Even logs from IAM systems could feed into this common platform to be part of the incident management process. The degree to which this common platform reveals the logging and monitoring details would match the need of the SME for a SOC or simply for a management, alerting and reporting system.

Summary

SME management (and boards) need to know that their systems and data are secure to meet their business requirements and need to be notified in a timely manner when problems exist that need attention. Securing infrastructure requires a combination of

- Hardening systems to have secure configurations
- Identifying and dealing with vulnerabilities in a manner appropriate to the business and its customers
- Controlling access to systems
- Identifying and managing cybersecurity issues to know about possible attacks and to manage any incidents in an appropriate manner
- Communicating the existence and effectiveness of the above both internally and externally sufficiently to provide evidence that these meet business, regulator and customer requirements.

Larger enterprises deploy a combination of best-in-class solutions to provide these security capabilities but a more integrated solution with chosen features from the best-in-class solutions could meet the needs of most SMEs.

[1] Gartner, Hype Cycle for Security Operations 2022 (July 2022), https://www.gartner.com/doc/reprints?id=1-2AM0TFXC&ct=220718&st=sb&__hstc=98938945.96343018ab6aed9cd2621541520c668d.1678429081995.1678429081995.1679294598286.2&__hssc=98938945.5.1679294598286&__hsfp=800668528hsCtaTracking=a7b30504-5af3-4236-84e9-23520fb5e3c7%7Cd3d519ea-a3e9-4b47-b1f8-25a590547891

[1] Gartner, Endpoint Detection and Response (EDR) Solutions Reviews and Ratings; https://www.gartner.com/reviews/market/endpoint-detection-and-response-solutions

[1] Crowdstrike, What is Managed Detection and Response (MDR)?; https://www.crowdstrike.com/cybersecurity-101/managed-detection-and-response-mdr/

[1] Summary
SME management (and boards) need to know that their systems and data are secure to meet their business requirements and need to be notified in a timely manner when problems exist that need attention. Securing infrastructure requires a combination of
- Hardening systems to have secure configurations
- Identifying and dealing with vulnerabilities in a manner appropriate to the business and its customers
- Controlling access to systems
- Identifying and managing cybersecurity issues to know about possible attacks and to manage any incidents in an appropriate manner
- Communicating the existence and effectiveness of the above both internally and externally sufficiently to provide evidence that these meet business, regulator and customer requirements.

Larger enterprises deploy a combination of best-in-class solutions to provide these security capabilities but a more integrated solution with chosen features from the best-in-class solutions could meet the needs of most SMEs.

[1] https://www.csoonline.com/article/2126267/configuration-management-definition-and-solutions.html

End Of Page