EventTracker
www.eventtracker.com

How To Succeed at SIEM

Issue 3

2 Welcome

3 SIEM Architecture and Operational Processes

18 SIEM Simplified

21 About EventTracker

Featuring research from

Gartner®

Welcome

To succeed at SIEM, you must buy the tools, grow the people and mature the processes. This requires skill and discipline, all too rare in the typical medium enterprise. Not surprisingly, these are the very same reasons why SIEM implementations fail to deliver value. This paper presents an "output-driven" and structured approach designed to let you get value from your investment. We also discuss when to support SIEM with services

SIEM differs from broad scope log management which is usually aimed at general system troubleshooting or incident response support. While EventTracker can do both, an output-driven approach requires that you admit data into the solution only when you have a clear understanding of its utility and presentation. This approach avoids the common implementer's dilemma of "now I have all this data, the SIEM is very slow and unusable".

"You can buy a SIEM tool but you cannot buy a security monitoring capability."

– Gartner Security & Risk Management Summit 2014

While there is a greater awareness of both security and compliance needs by upper management, the reality on the ground of a typical IT Department is a lack of skilled resources and a limit on hiring and retention. For mid-size enterprises with several hundred employees, IT security is a constant struggle. They are frequently targeted by hackers who want sensitive information they have, yet are hampered by lack of a budget or manpower for dedicated IT Security. Hackers are highly motivated to monetize their efforts and will cheerfully pick the lowest hanging fruit they can get, leaving the limited IT staff of these companies in a constant state of fighting fires and limited to only keeping things operational while on a tight budget.

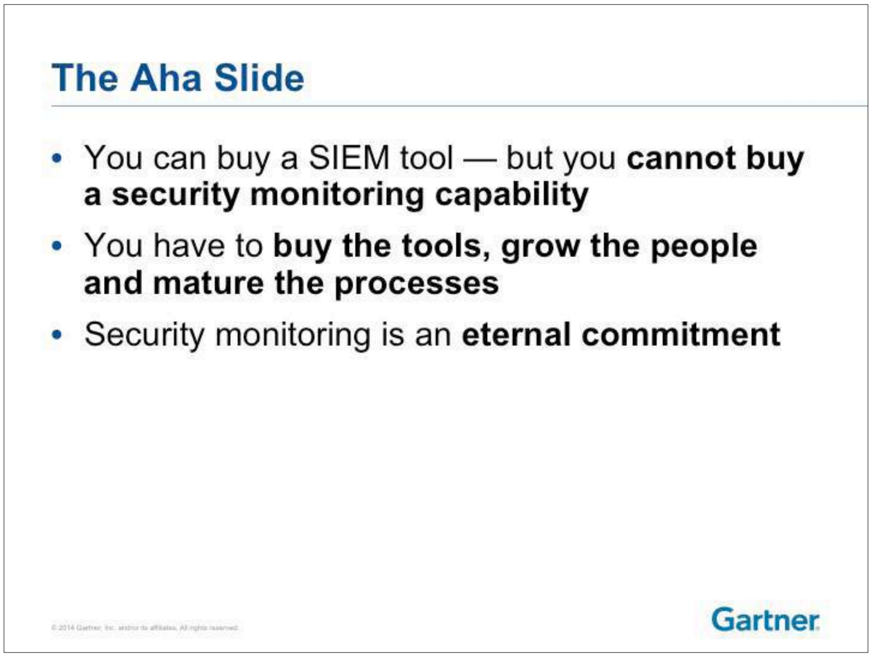
Supporting SIEM with services is attractive in cases where the IT team does not have the necessary expertise in house but is subject to attacks and faces regulatory compliance pressures. SIEM technology can also deliver operational benefits as an added plus.

The buyer gets sophisticated technology that can be customized to their specific needs, and delivered by experts, and yet at a price point that is far more palatable than the do-it-yourself approach. In return, some degree of sovereignty in a specialist area is lost to the outsourcer. When the advantages of security and cost savings are understood, using services to support SIEM implementations becomes attractive.

The first section of this newsletter is "SIEM Architecture and Operational Processes" a Gartner presentation that was delivered at the 2014 Security & Risk Management Summit which describes how to plan, deploy and expand a SIEM solution and what key processes and practices are needed for success. It is followed by a description of our SIEM Simplified offering, which uses these techniques every day for our customers. The goal is to help you realize value from a well-designed and managed SIEM implementation.

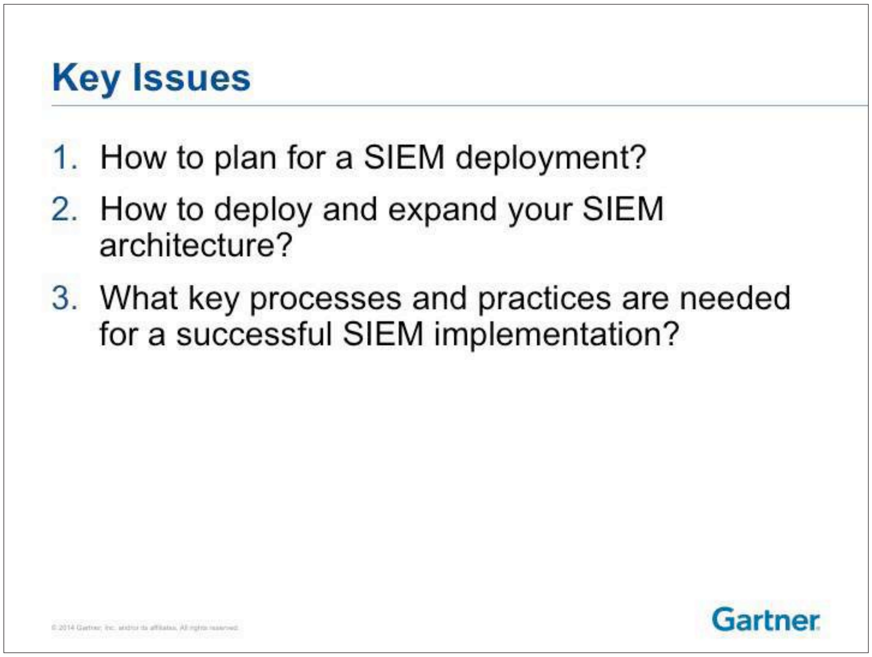
Best Regards,
A. Ananth
President

SIEM Architecture and Operational Processes



The Aha Slide

- You can buy a SIEM tool — but you **cannot buy a security monitoring capability**
- You have to **buy the tools, grow the people and mature the processes**
- Security monitoring is an **eternal commitment**

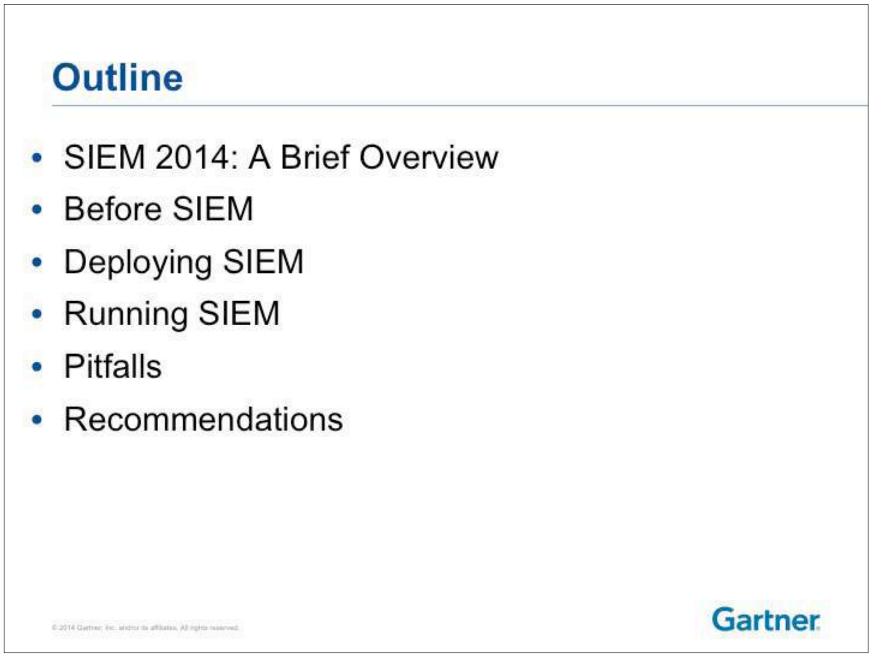


Key Issues

1. How to plan for a SIEM deployment?
2. How to deploy and expand your SIEM architecture?
3. What key processes and practices are needed for a successful SIEM implementation?

Gartner

How to plan for a SIEM deployment?How to deploy and expand your SIEM architecture?What key processes and practices are needed for a successful SIEM implementation?



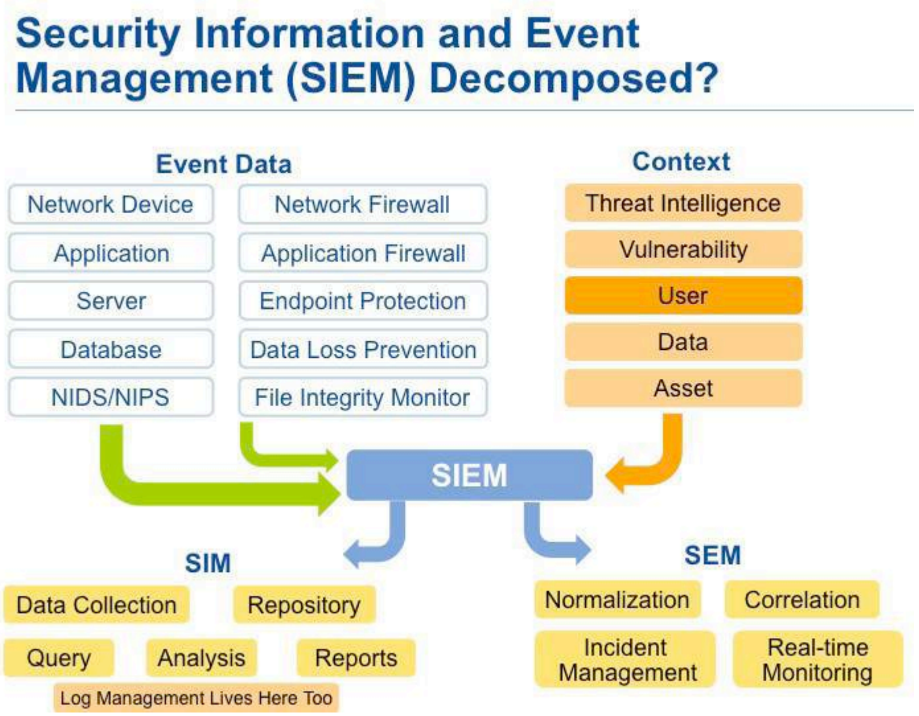
Outline

- SIEM 2014: A Brief Overview
- Before SIEM
- Deploying SIEM
- Running SIEM
- Pitfalls
- Recommendations

Gartner

Security information and event management (SIEM) is a key technology that provides security visibility, but it suffers from challenges with operational deployments. This presentation will reveal a guidance framework offers a structured approach for architecting and running an SIEM deployment at a large enterprise or evolving a stalled deployment.

SIEM 2014



Security Information and Event Management (SIEM) Decomposed?

Event Data

Network Device

Network Firewall

Application

Application Firewall

Server

Endpoint Protection

Database

Data Loss Prevention

NIDS/NIPS

File Integrity Monitor

Context

Threat Intelligence

Vulnerability

User

Data

Asset

SIEM

SIM

Data Collection

Repository

Query

Analysis

Reports

Log Management Lives Here Too

SEM

Normalization

Correlation

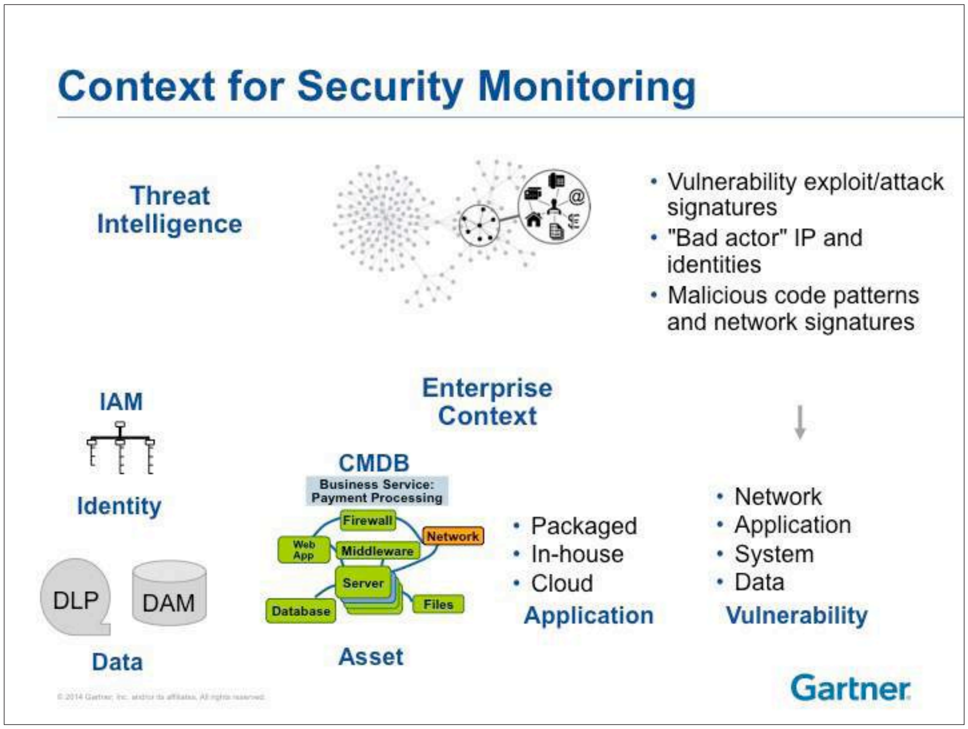
Incident Management

Real-time Monitoring

What it solves: SIEM technology delivers security event management (SEM), which supports threat management and security incident response through collection and analysis of security events from a wide variety of data sources in real time. It also delivers security information management (SIM), which provides log management and analysis functions in support of security policy compliance monitoring and incident investigation through analysis of and reporting on historical data from these sources. The core capabilities of SIEM technology are the broad scope of event collection and the ability to correlate events across disparate information sources. The technology is typically deployed to monitor:

- External threats
- Server and database resource access (if DAM tools are not deployed)
- User activity across multiple systems and applications

How it works: SIEM technology aggregates and analyzes the event data produced by devices, systems and applications. The primary data source is log data, but SIEM technology can also process other forms of data. The data is normalized so that events from disparate sources can be correlated and analyzed according to rule sets designed for specific purposes, such as network security event monitoring or user activity monitoring.



Context for Security Monitoring

Threat Intelligence

- Vulnerability exploit/attack signatures
- "Bad actor" IP and identities
- Malicious code patterns and network signatures

Enterprise Context

IAM

Identity

DLP DAM

Data

CMDB

Business Service: Payment Processing

Asset

- Packaged
- In-house
- Cloud

Application

- Network
- Application
- System
- Data

Vulnerability

Gartner

Emerging use cases, required capabilities and data sources:

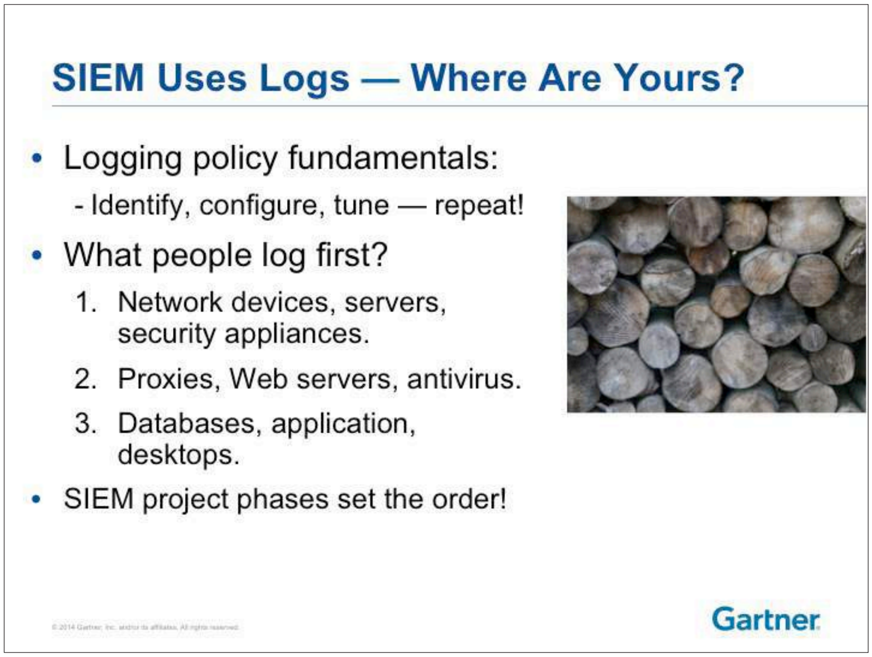
- User activity monitoring is a common requirement for many emerging use cases (for example, breach detection, fraud detection). Capabilities needed to support the requirement include integration with identity and access management infrastructure and the user context in correlation, analytics and reporting.

- Application activity monitoring is important, because application weaknesses are frequently exploited in targeted attacks, and abnormal application activity may be the only signal of a successful breach or of fraudulent activity. The ability to parse activity streams from packaged applications enables application layer monitoring for those components, and the ability to define and parse activity streams for custom applications enables application layer monitoring for in-house-developed applications.

- Data context is needed to discover incidents that involve sensitive data. Integration with DLP technology and the inclusion of data context in correlation, analytics and reporting are required capabilities.

- Early attack detection requires recognition of a change from the normal pattern of user activity, application activity or data access. Traditional correlation rules need to be augmented with approaches that establish a baseline of normal activity and alert on deviations.

Before SIEM



SIEM Uses Logs — Where Are Yours?

- Logging policy fundamentals:
  - Identify, configure, tune — repeat!
- What people log first?
  1. Network devices, servers, security appliances.
  2. Proxies, Web servers, antivirus.
  3. Databases, application, desktops.
- SIEM project phases set the order!

Gartner

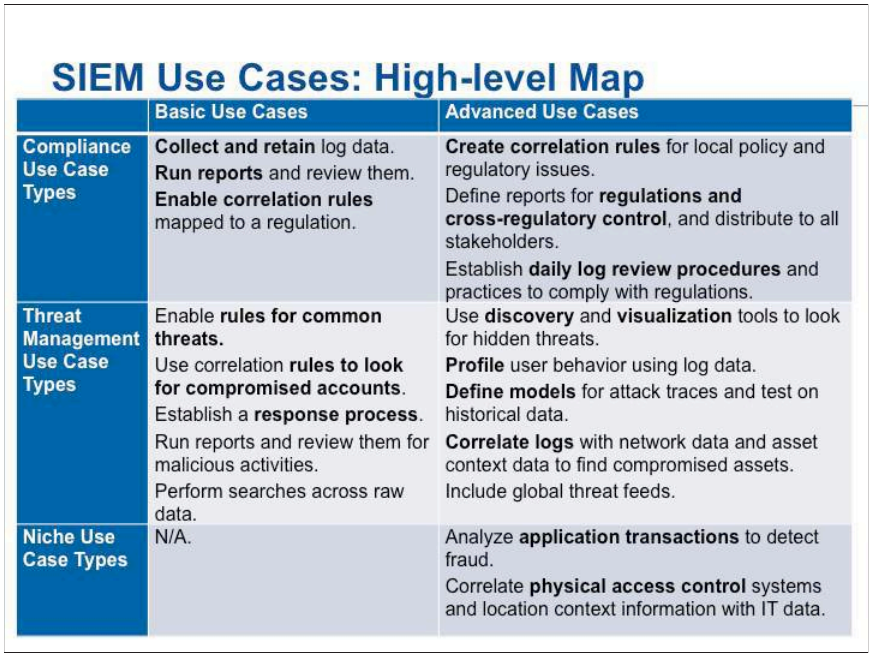
Logging Policy

In any approach, having a log policy and enabling logging on production log sources that feed into an SIEM — whether just for collection or for real-time monitoring — is an obvious prerequisite. Log policy will likely be determined by the use cases as well, even though there will be some baseline log settings set to “on” by default (such as logins/logouts on Unix systems, failed connections through firewalls and IDS/IPS alerts).

In some cases, turning extensive logging on will increase the load on the production servers to the point that the application may slow down. Such cases may require new hardware, which will increase the time to get logging enabled. Relational databases are one common example of a system where logging may affect performance.

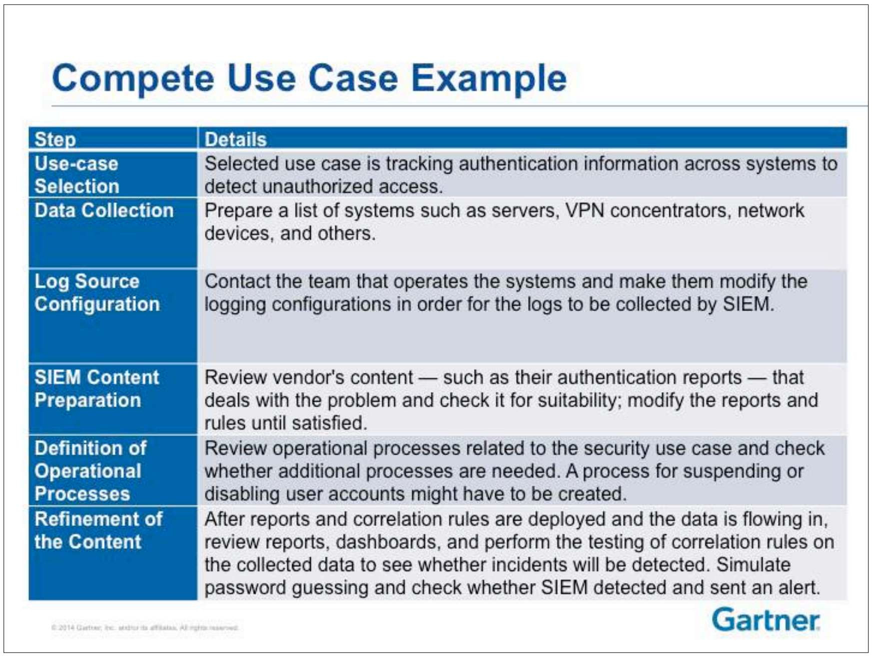
Implementing the logging policy and configuring systems for logging requires the cooperation of system owners and operators. In cases of common platforms and devices, such as Windows and Cisco routers, the configuration changes needed will be straightforward and well-covered in documentation. For custom applications and enterprise ERP applications, the effort will be much more involved. For example, specific ERP system logging configuration may well contradict existing operational processes and need to be negotiated with the team that operates the system.

There is also a common sequence for log source integrations. It should not be considered the “best practice” because log sources should be integrated based on the needs and enterprise use cases for SIEM.



SIEM Use Cases: High-level Map

	Basic Use Cases	Advanced Use Cases
Compliance Use Case Types	**Collect and retain** log data. **Run reports** and review them. **Enable correlation rules** mapped to a regulation.	**Create correlation rules** for local policy and regulatory issues. Define reports for **regulations and cross-regulatory control**, and distribute to all stakeholders. Establish **daily log review procedures** and practices to comply with regulations.
Threat Management Use Case Types	Enable **rules for common threats.** Use correlation **rules to look for compromised accounts**. Establish a **response process**. Run reports and review them for malicious activities. Perform searches across raw data.	Use **discovery** and **visualization** tools to look for hidden threats. **Profile** user behavior using log data. **Define models** for attack traces and test on historical data. **Correlate logs** with network data and asset context data to find compromised assets. Include global threat feeds.
Niche Use Case Types	N/A.	Analyze **application transactions** to detect fraud. Correlate **physical access control** systems and location context information with IT data.



Compete Use Case Example

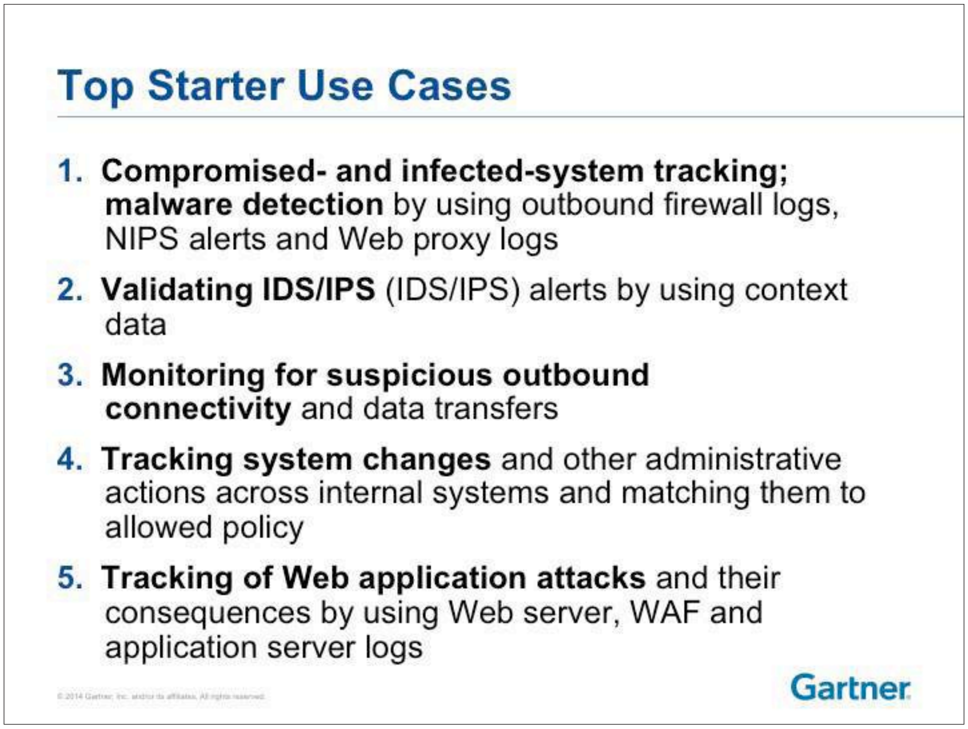
Step	Details
Use-case Selection	Selected use case is tracking authentication information across systems to detect unauthorized access.
Data Collection	Prepare a list of systems such as servers, VPN concentrators, network devices, and others.
Log Source Configuration	Contact the team that operates the systems and make them modify the logging configurations in order for the logs to be collected by SIEM.
SIEM Content Preparation	Review vendor's content — such as their authentication reports — that deals with the problem and check it for suitability; modify the reports and rules until satisfied.
Definition of Operational Processes	Review operational processes related to the security use case and check whether additional processes are needed. A process for suspending or disabling user accounts might have to be created.
Refinement of the Content	After reports and correlation rules are deployed and the data is flowing in, review reports, dashboards, and perform the testing of correlation rules on the collected data to see whether incidents will be detected. Simulate password guessing and check whether SIEM detected and sent an alert.

Gartner

Based on an example organization, here is how an SIEM deployment may proceed:

The initial use case is selected based on compliance mandates, risk assessment, threat catalog or other factors. Some common use cases are presented in this document.

A scope of needed data collection is finalized.
Log sources that are in scope are configured to send the data into an SIEM system (some log sources are configured so the SIEM system can retrieve data from them).
Prepare SIEM content (e.g., reports, rules and dashboards) to be used.
Define operational processes specific to this use case (if any).
Refine the content until the capability is operational.
Start work on the next use case.



Top Starter Use Cases

1. **Compromised- and infected-system tracking; malware detection** by using outbound firewall logs, NIPS alerts and Web proxy logs
2. **Validating IDS/IPS** (IDS/IPS) alerts by using context data
3. **Monitoring for suspicious outbound connectivity** and data transfers
4. **Tracking system changes** and other administrative actions across internal systems and matching them to allowed policy
5. **Tracking of Web application attacks** and their consequences by using Web server, WAF and application server logs

A lot of aspiring SIEM users are looking for "top use cases" to implement. Of course, the honest answer to "What are the best SIEM use cases?" must always be "it depends on your risks and priorities" (and your threat assessment), but in fact one may be able to identify the popular use cases, implemented successfully by many. Before I get to them, I want to once again say: you need to do what YOU need to do, not necessarily what your peers are doing.

With that that long preface, here are some of the common SIEM use cases that would make my "top list":

Authentication tracking and account compromise detection; admin and user tracking [this is the very use case that I detail in that post]

Compromised- and infected-system tracking; malware detection by using outbound firewall logs, NIPS alerts and Web proxy logs, as well as internal connectivity logs, network flows, etc

Validating intrusion detection system/intrusion prevention system (IDS/IPS) alerts by using vulnerability data and other context data about the assets collected in theSIEM [while some say "this is so 2002," this use case is still here in its modern form of using SIEM for "context-enabling" various alerts]

Monitoring for suspicious outbound connectivity and data transfers by using firewall logs, Web proxy logs and network flows; detecting exfiltration and other suspicious external connectivity

Tracking system changes and other administrative actions across internal systems and matching them to allowed policy; detecting violations of various internal policies, etc [and, yes, even the classic "root access from an unknown IP in a foreign country at 3AM, leading to system changes" sits here as well]

Tracking of Web application attacks and their consequences by using Web server, WAF and application server logs; detecting attempts to compromise and abuse Web applications by combining logs from different components.

Note that I am leaving the use cases around log search ("type an IP, see logs from all systems related to it") and basic incident investigations aside, because, frankly, they don't really require a SIEM – a nice indexed pile of logs would do.

What makes them the top starter use cases? Reasons include:

The necessary logs are easy to collect; they are supported by most SIEM tools [normalized and categorized for easy correlation]

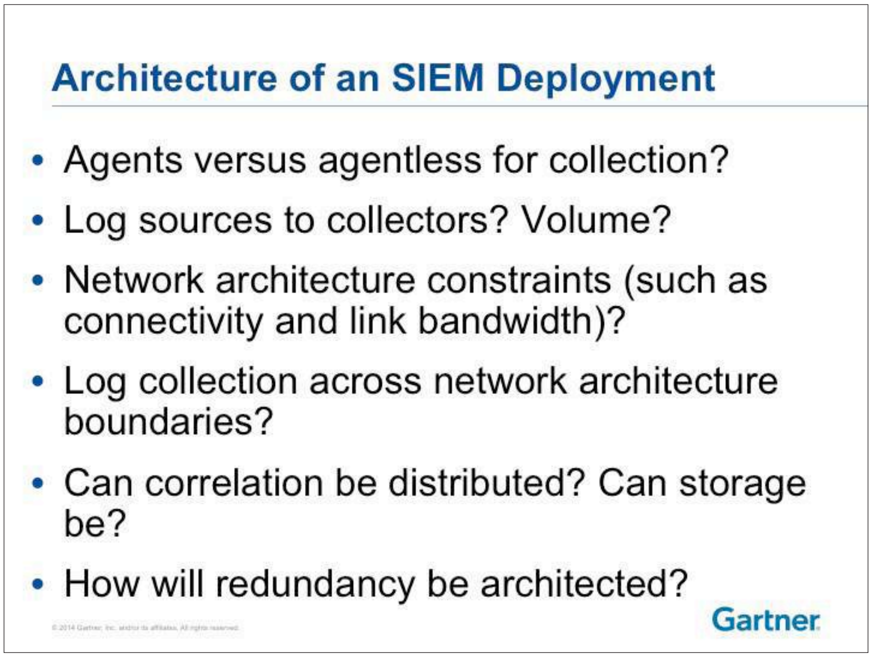
Canned rules are often included in top products to enable these with minimal site customization
Easy analysis of alerts requires only basic SIEM operational processes

Using SIEM for these "clear and present" dangers has value for most organizations

These allow the SIEM operators to learn and gain experience and then go do more fun things with their SIEM

The same template can be used to document all these use cases — but I am leaving it as an exercise to the reader [or maybe for later GTP SIEM papers]

Deploying SIEM



Architecture of an SIEM Deployment

- Agents versus agentless for collection?
- Log sources to collectors? Volume?
- Network architecture constraints (such as connectivity and link bandwidth)?
- Log collection across network architecture boundaries?
- Can correlation be distributed? Can storage be?
- How will redundancy be architected?

Gartner

Additional Architecture Questions to Be Answered During Deployment

Organizations should be asking themselves additional questions while deploying their SIEM architectures:

Where should we use agents versus agentless collection of log and context data (if there is a choice)?

What collector form factor (appliance, software, virtual image) should we use? How many collectors? Which collector types?

How do we decide which log sources go into which collector if there are many collectors per site?

How do we deal with super-high volume and super-low volume log sources?

How do we architect log collection around network architecture boundaries, such as zones and access control lists (ACLs)? Specifically, how do we run demilitarized zone (DMZ) log collection?

Is there a separate audit zone in network security architecture?

Can correlation be distributed? Tiered? How can storage be distributed across sites?

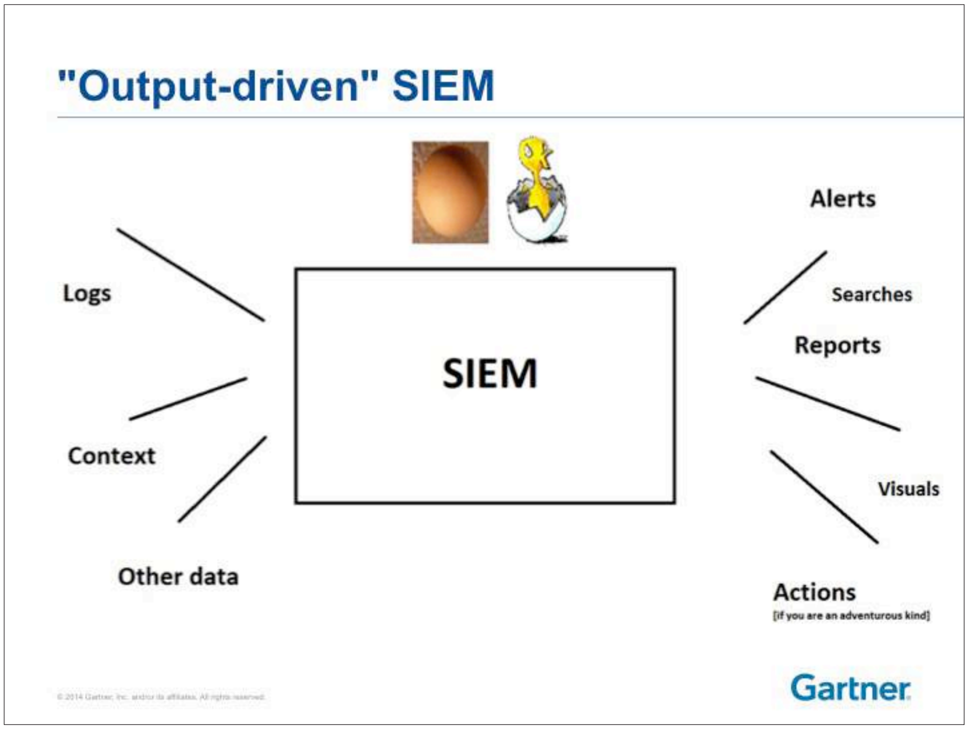
What is being stored: structured data, unstructured data or both? Can many data stores of structured or unstructured data be queried from one place?

What do we do if any particular component is overwhelmed?

How will redundancy be architected?

What network architecture constraints (such as connectivity and link bandwidth) are in place and how do we work around them for log data transport?

How do we deal with other external constraints on architecture: firewall rules, security policy, available servers and user population?



"Output-driven" SIEM

Logs

Context

Other data

SIEM

Alerts

Searches

Reports

Visuals

Actions

[if you are an adventurous kind]

Gartner

Output-Driven SIEM Planning

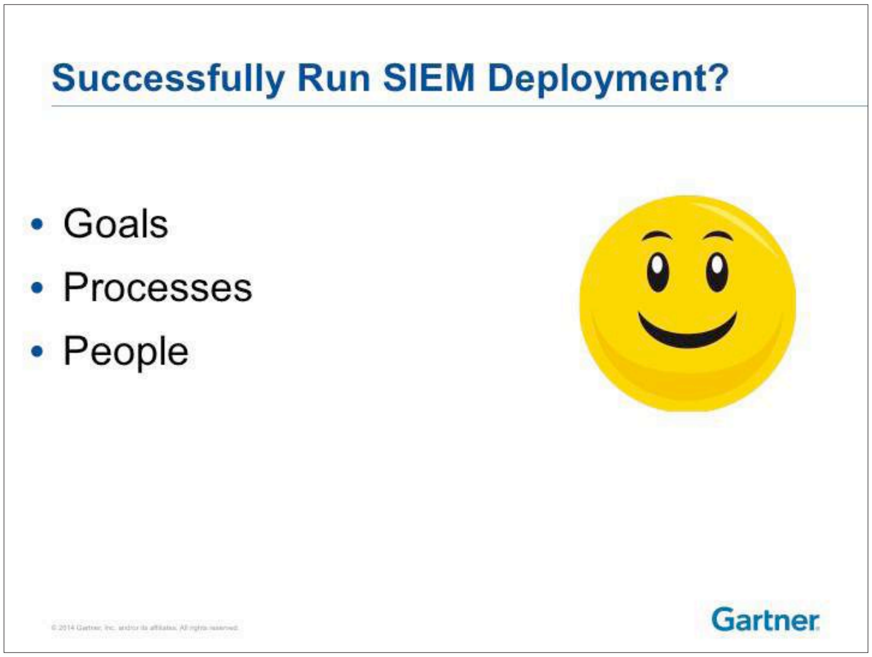
"Output-driven SIEM" simply means deploying a security information and event management tool in such a way that nothing comes into the SIEM unless and until there is a clear knowledge of how it will be utilized and/or presented. Thus, only existing/planned reports, visuals, alerts, dashboards, profiling algorithms, context fusion and so on can make an SIEM implementer "open the floodgates" and admit a particular log type into the tool. If a process exists outside of an SIEM tool that will make use of the SIEM data, then that qualifies as well.

With that model of SIEM, the "what if we need it someday?" argument does not work — such log entries can be easily and cheaply collected by a log management tool. The use-case-driven collection does not preclude, but facilitates analysis because the SIEM tool stays at its optimum performance level without incurring excessive hardware costs.

In this model, goals drive tool requirements, requirements drive use cases and use cases drive functionality and collection scope. This model as well-known and effective as it is, is sadly uncommon among the organizations deploying SIEM tools today. Customers often ask the vendor field engineers and consultants "Now that we have all this data [and now that our SIEM is very slow], how do we use it?" is much more common — and much less productive because many SIEM projects never move beyond that stage, even after many years of operation.

This is dramatically different from an approach one should take with broad-scope log management, which is aimed at general system troubleshooting or incident response support. This is an area where differences between SIEM, which focuses on security monitoring, and broad scope log management, which focuses on collecting all the logs for various reasons, manifests themselves. Log management technology benefits from an "input-driven" approach, and getting every possible bit of data in would be admirable. However, doing the same with an SIEM is a great way to turn a deployment into a quivering, jumbled mess of barely performing components and a plethora of useless data.

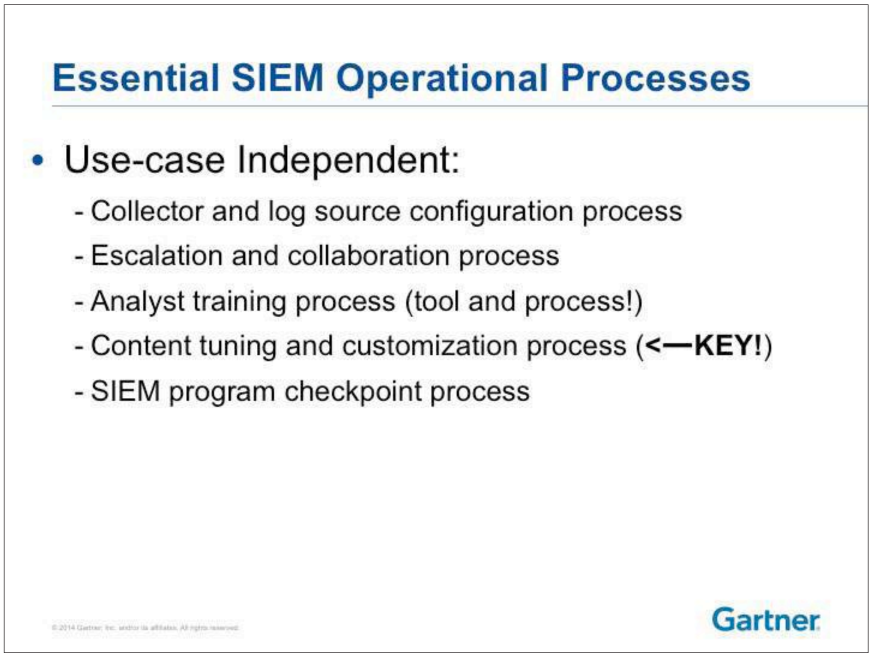
Running SIEM



Successfully Run SIEM Deployment?

- Goals
- Processes
- People

Gartner



Essential SIEM Operational Processes

- Use-case Independent:
  - Collector and log source configuration process
  - Escalation and collaboration process
  - Analyst training process (tool and process!)
  - Content tuning and customization process (**<—KEY!**)
  - SIEM program checkpoint process

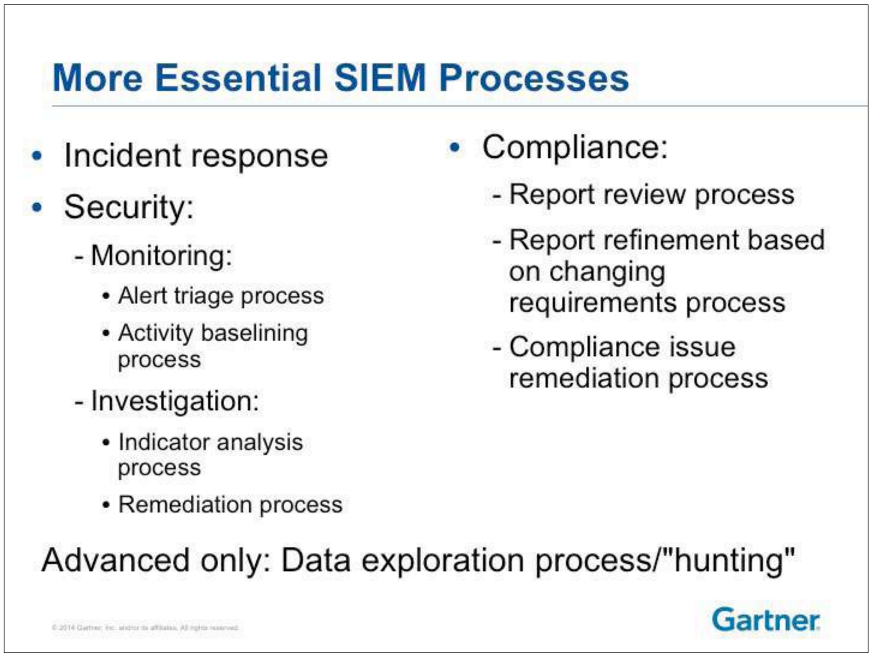
Gartner

Essential SIEM processes can be categorized based on a use case type:

Use-case-independent processes are mandatory for all SIEM deployments.

Compliance use case processes are necessary for those using their SIEM tool for regulatory compliance.

Security use case processes are compulsory for SIEM deployments that are utilized for information security.

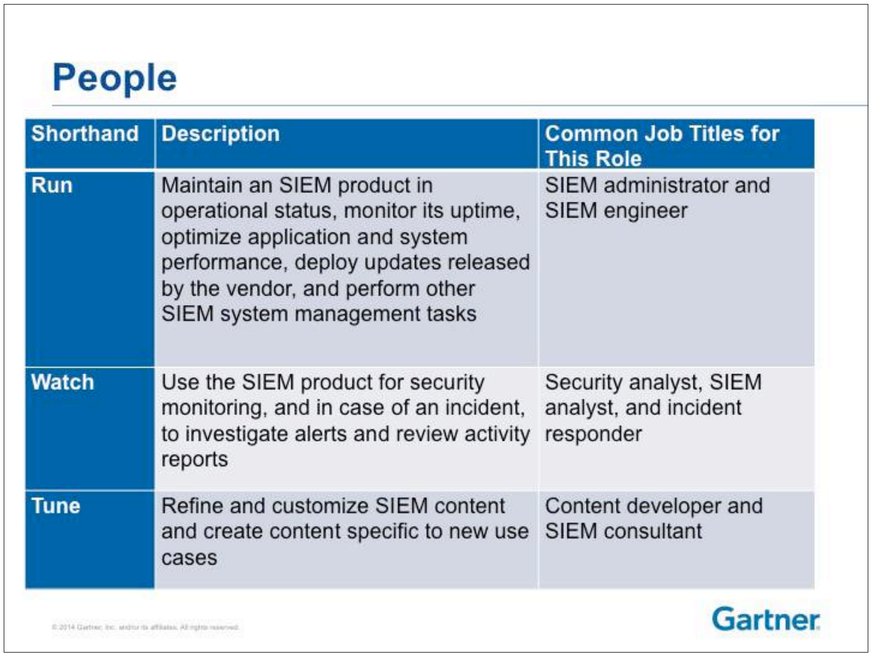


More Essential SIEM Processes

- Incident response
- Security:
  - Monitoring:
    - Alert triage process
    - Activity baselining process
  - Investigation:
    - Indicator analysis process
    - Remediation process
- Compliance:
  - Report review process
  - Report refinement based on changing requirements process
  - Compliance issue remediation process

Advanced only: Data exploration process/"hunting"

Gartner

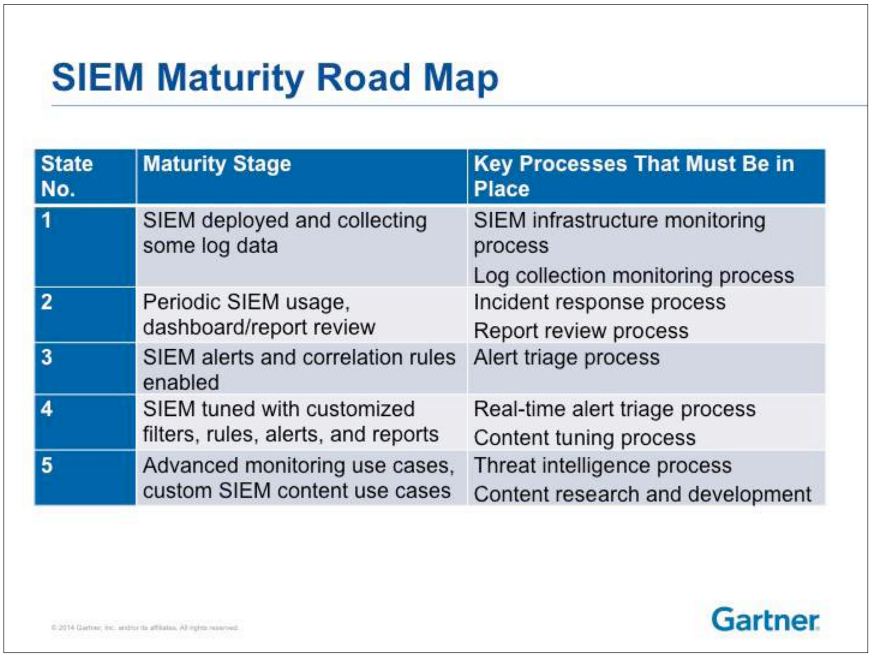


People

Shorthand	Description	Common Job Titles for This Role
Run	Maintain an SIEM product in operational status, monitor its uptime, optimize application and system performance, deploy updates released by the vendor, and perform other SIEM system management tasks	SIEM administrator and SIEM engineer
Watch	Use the SIEM product for security monitoring, and in case of an incident, to investigate alerts and review activity reports	Security analyst, SIEM analyst, and incident responder
Tune	Refine and customize SIEM content and create content specific to new use cases	Content developer and SIEM consultant

Gartner

Evolving SIEM

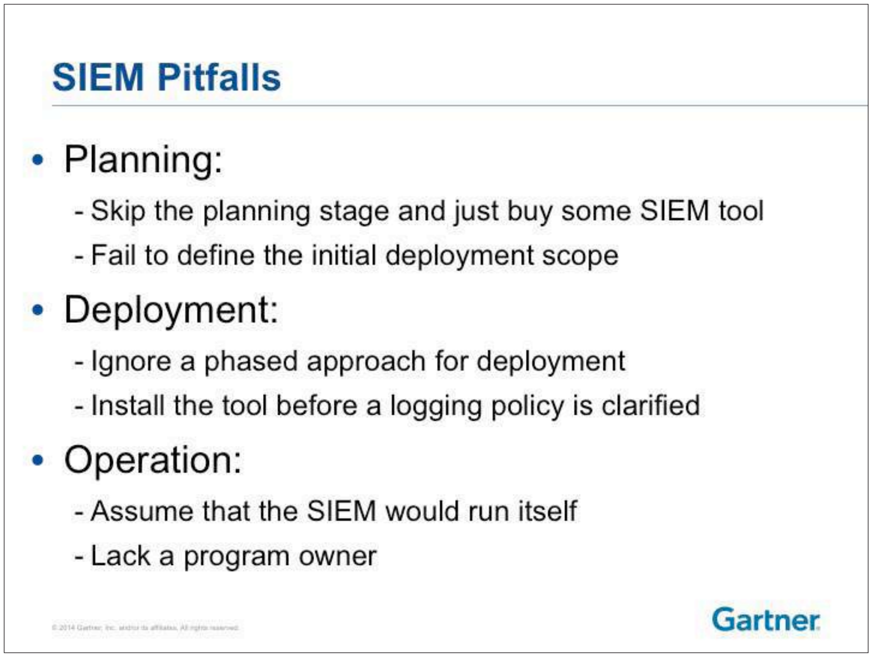


SIEM Maturity Road Map

State No.	Maturity Stage	Key Processes That Must Be in Place
1	SIEM deployed and collecting some log data	SIEM infrastructure monitoring process Log collection monitoring process
2	Periodic SIEM usage, dashboard/report review	Incident response process Report review process
3	SIEM alerts and correlation rules enabled	Alert triage process
4	SIEM tuned with customized filters, rules, alerts, and reports	Real-time alert triage process Content tuning process
5	Advanced monitoring use cases, custom SIEM content use cases	Threat intelligence process Content research and development

Gartner

SIEM Pitfalls

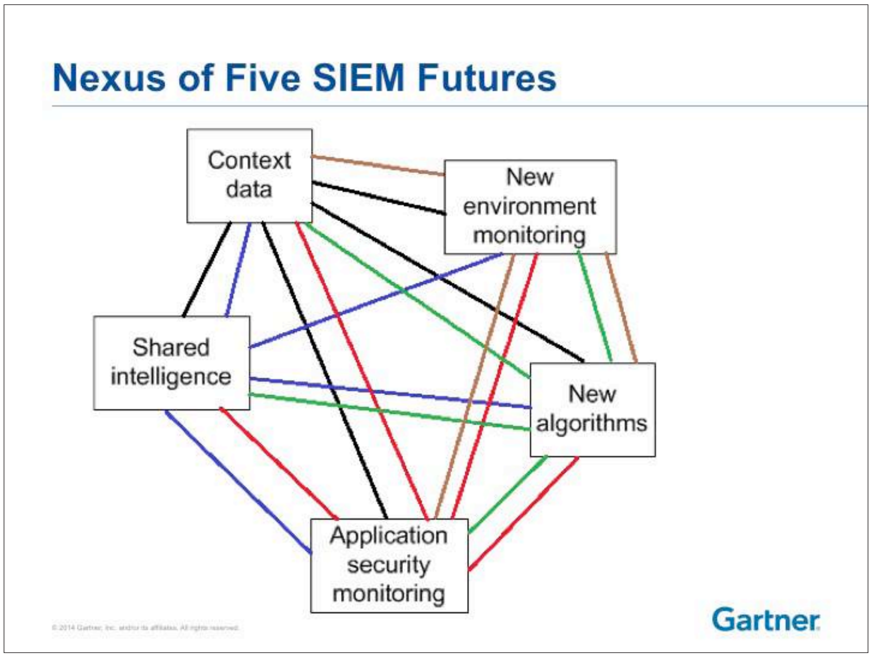


SIEM Pitfalls

- Planning:
  - Skip the planning stage and just buy some SIEM tool
  - Fail to define the initial deployment scope
- Deployment:
  - Ignore a phased approach for deployment
  - Install the tool before a logging policy is clarified
- Operation:
  - Assume that the SIEM would run itself
  - Lack a program owner

Planning, implementing and operating an SIEM tool at a large enterprise or a large government agency is an involved project that requires skilled and dedicated personnel, well-thought-out plans, and political and communication abilities. The process is understandably fraught with many risks and pitfalls. In fact, many large deployments have succumbed to these pitfalls, and their SIEM tools failed to deliver value to the organization.

SIEM Futures



Nexus of Five SIEM Futures

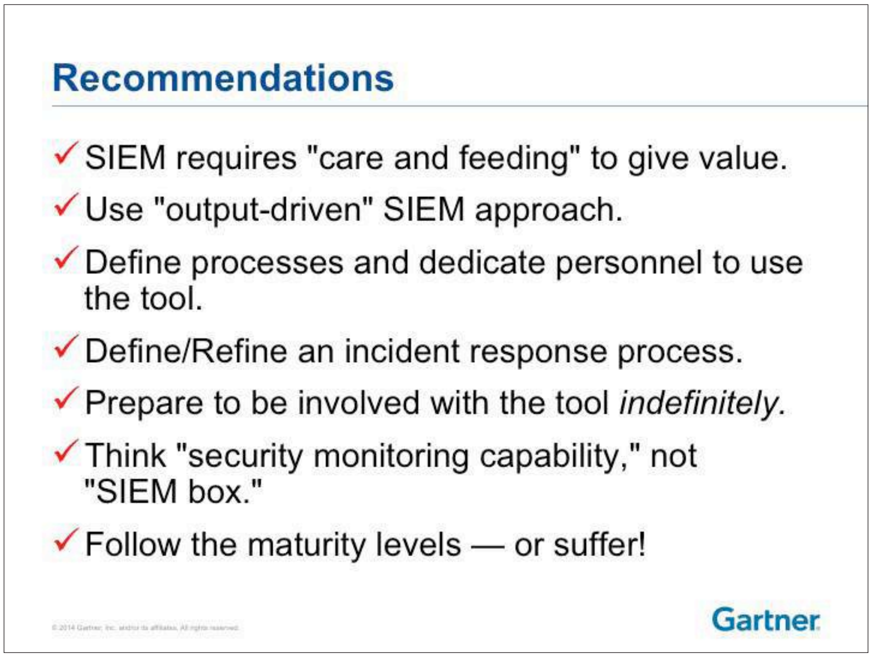
Context data

New environment monitoring

Shared intelligence

New algorithms

Application security monitoring



Recommendations

- ✓ SIEM requires "care and feeding" to give value.
- ✓ Use "output-driven" SIEM approach.
- ✓ Define processes and dedicate personnel to use the tool.
- ✓ Define/Refine an incident response process.
- ✓ Prepare to be involved with the tool *indefinitely*.
- ✓ Think "security monitoring capability," not "SIEM box."
- ✓ Follow the maturity levels — or suffer!

Gartner

The “plan strategically, deploy tactically” mantra sometimes results in SIEM architectures that are hard to expand and grow. Still, for many organizations, it is better to have an SIEM solution that has trouble growing than an SIEMone that never gets fully deployed due to loading the initial phase with too many goals.

SIEM architecture determines performance and flexibility, but the ultimate success of an SIEM program is often determined more by operational processes than by its architecture or specific tool choice.

SIEM can perform few functions without specific content developed (or tuned) based on the organization’s requirements. Content architecture is just as essential as network architecture for an SIEM solution.

Defining scope and objectives, broad use cases (such as compliance or security monitoring) and ultimately specific use cases (such as Payment Card Industry Data Security Standard [PCI DSS] server log review or monitoring Web servers for attacks) presents truly one of the most critical tasks in the entire SIEM process.

A good approach to use is an “output-driven SIEM,” which simply means deploying an SIEM tool in such a way that nothing comes into an SIEM unless and until there is a clear knowledge of how it would be utilized and/or presented.

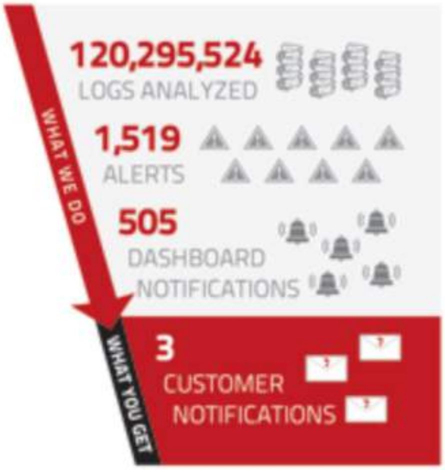
SIEM Simplified

Your need: complete coverage, zero hassle

Barriers to the effective implementation of a SIEM and log management solution include a lack of in-depth knowledge, and insufficient time or resources to effectively extract the actionable information concerning the IT infrastructure. Monitoring all the log sources in your IT environment is a time-consuming task, even with a SIEM or log management solution. Sifting through hundreds of incidents a day pulled from millions of logs and dozens of reports requires discipline, patience and expertise. How can you this do this effectively at reasonable cost?

Your Solution: SIEM Simplified(SM)

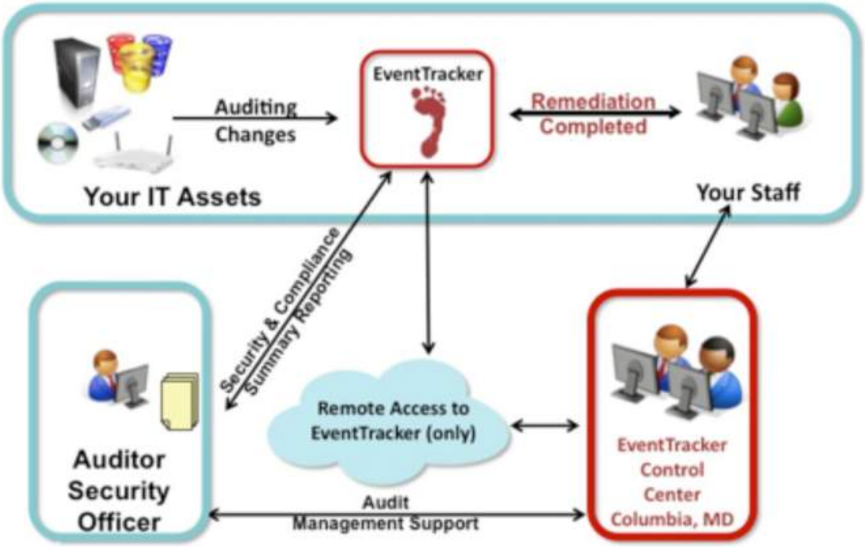
SIEM Simplified is our professional services engagement to enhance the value of the EventTracker Enterprise and EventTracker Security Center products. Our experienced staff assumes responsibility for all SIEM related tasks including daily incident reviews, daily/weekly log reviews, configuration assessments, incident investigation support and audit support. We augment your IT team, allowing you to remain focused on the unique requirements of your enterprise while actively leveraging our expertise. Our team includes experts in various technologies including Windows, Cisco, VMware, Checkpoint and many security solutions such as Snort, McAfee, Imperva etc.



How it works

Step 1: EventTracker is installed, either on your premises or in a tier-1 datacenter and configured to monitor your IT assets. The installation can be dedicated and customized to your specific needs.

Step 2: Once the installation is complete, staff at the EventTracker Control Center (ECC), based in Columbia, Maryland are granted limited, audited access to only the instance of EventTracker. No other access to any other IT assets is required or expected.

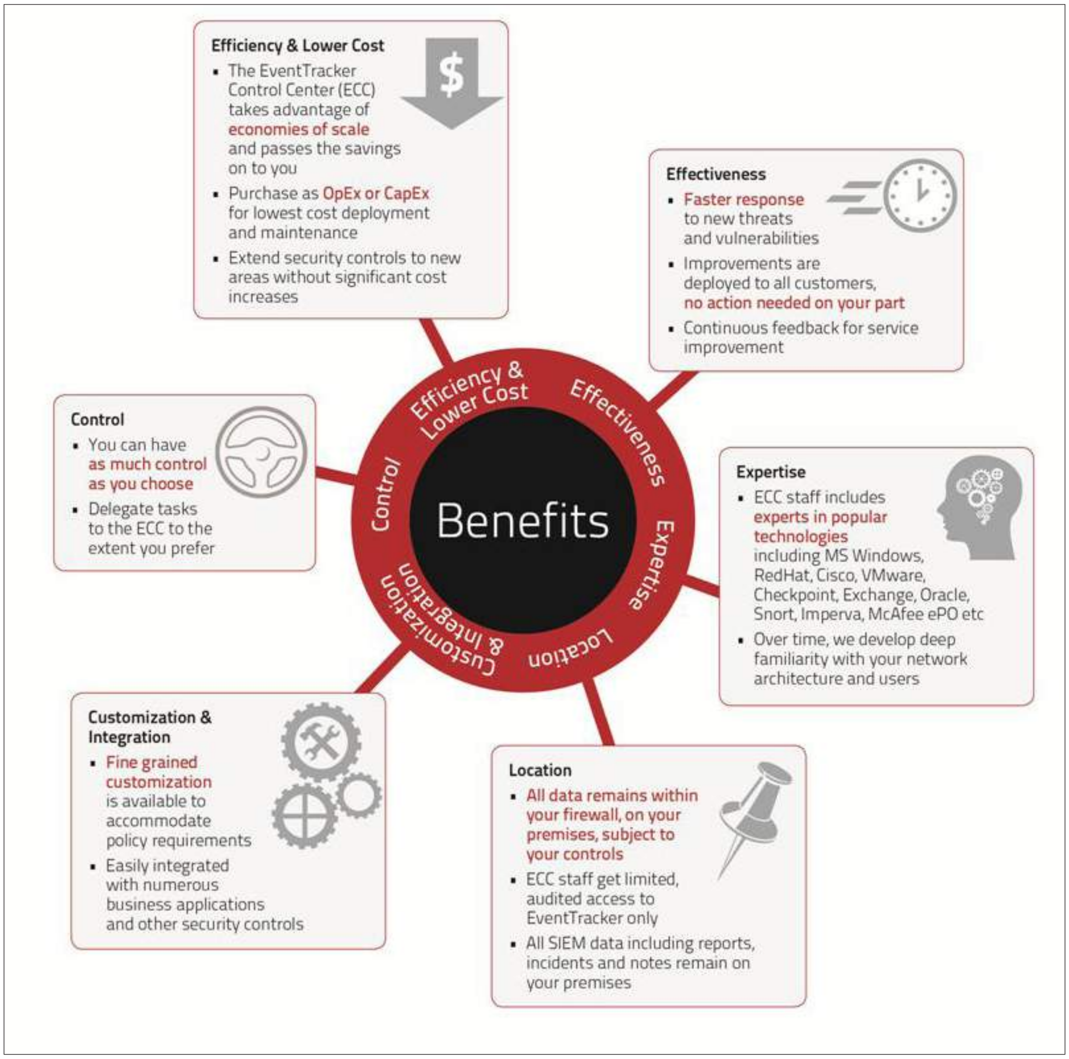


Step 3: We work with you to define an alert response procedure which covers, when, why, who and how ECC staff should escalate incidents to your attention.

Step 4: ECC staff begin monitoring your IT assets, providing daily log reviews, escalating incidents per procedure and maintaining the EventTracker installation in top working order. They are also available to answer any ad-hoc questions or provide support for incident review, audit assistance etc.

Step 5: We conduct quarterly assessments of the service with key members of your team to continuously improve the process and stay abreast of any changes to your environment.

Benefits



Efficiency & Lower Cost

- The EventTracker Control Center (ECC) takes advantage of economies of scale and passes the savings on to you
- Purchase as OpEx or CapEx for lowest cost deployment and maintenance
- Extend security controls to new areas without significant cost increases

Effectiveness

- Faster response to new threats and vulnerabilities
- Improvements are deployed to all customers, no action needed on your part
- Continuous feedback for service improvement

Control

- You can have as much control as you choose
- Delegate tasks to the ECC to the extent you prefer

Expertise

- ECC staff includes experts in popular technologies including MS Windows, RedHat, Cisco, VMware, Checkpoint, Exchange, Oracle, Snort, Imperva, McAfee ePO etc
- Over time, we develop deep familiarity with your network architecture and users

Customization & Integration

- Fine grained customization is available to accommodate policy requirements
- Easily integrated with numerous business applications and other security controls

Location

- All data remains within your firewall, on your premises, subject to your controls
- ECC staff get limited, audited access to EventTracker only
- All SIEM data including reports, incidents and notes remain on your premises

Features

Component of these services are customized to fit your requirements and may include:

Daily Incident Review

Our expert staff review the incidents prioritized by the EventTracker Knowledge Packs for patterns that merit escalation to your IT staff. A defined Incident Response Procedure is used for notification and escalation. Automated 24×7 processes are also used to notify the EventTracker Control Center staff.

Daily/Weekly Log Review

Our expert staff work with you and your auditor to determine the list of reports that need to be run and reviewed daily and weekly. This is determined by the applicable regulatory and/or internal policy. ECC staff review the daily and weekly generated reports and annotate them to indicate that the review was performed. Any anomalies are notified to the relevant person on your team for remediation. This closed loop guarantees compliance and tight security.

Weekly Configuration Assessment Review

A review of the configuration of systems and applications against best-practice templates specified by external standards such as Microsoft, NIST, DISA or an auditor. Findings from this process result in a list of gaps (mis-configurations) and result in a remediation plan. This process also includes a comparison of system configuration with compliance objectives.

Incident Investigation

We provide support to an enterprise currently engaged in dealing with a security incident. We will assist in the review of logs and other security information archived by EventTracker to determine what activity has actually occurred. We conduct a forensic analysis of patterns to determine weakness and possible path of exploit. This results in recommendations for remediation to deny such attacks in the future. This service is available on a contracting (i.e., ongoing) basis or consulting (single incident) basis.

Audit Assistance

We provide support enterprises engaged in dealing with IT Audits. We will assist reviewing logs and other security information archived by EventTracker and respond to questions from the Auditor. We can provide the Plan of Action and Milestones (POAM) response to any deficiencies and follow through as required. This service is available on a contracting (i.e., ongoing) basis or a consulting (single episode) basis.

Source: EventTracker

About EventTracker

EventTracker delivers business critical solutions that transform high-volume cryptic log data into actionable, prioritized intelligence that will fundamentally change your perception of the utility, value and organizational potential inherent in log files. Our industry award winning solutions offer Security Information and Event Management (SIEM), real-time Log Management, and powerful Change and Configuration Management to detect and deter costly security breaches, improve enterprise security postures, and comply with multiple regulatory mandates in addition to optimizing IWeT operations.

Our clients include commercial enterprises, educational institutions and government organizations with deployments in over 850 global customer locations.

SIEM Simplified is our professional services offering for customers to enhance the value of EventTracker Enterprise and Security Center. Our experienced staff provides additional resources to IT security teams for all SIEM-related tasks including daily incident reviews, log reviews, configuration assessments and audit support. The team reviews more than 1 billion logs daily.

EventTracker
www.eventtracker.com

Our MSP partners offer much needed security products to their clients in regulated industries. A feature-rich SIEM solution, simple licensing and payment models, and flexibility in offerings enables our customers to remain competitive, generate greater revenue and increase customer loyalty.

Visit www.eventtracker.com for more information. Follow us on Twitter @logtalk.

For further information, please contact:

Authorised Distributor/Reseller

networks unlimited
making networks better

Brought to you in the UK by: Networks Unlimited

T: +44 (0)1798 873 001 • E: info@networks-unlimited.co.uk

How to succeed at SIEM is published by EventTracker. Editorial content supplied by EventTracker is independent of Gartner analysis. All Gartner research is used with Gartner's permission, and was originally published as part of Gartner's syndicated research service available to all entitled Gartner clients. © 2014 Gartner, Inc. and/or its affiliates. All rights reserved. The use of Gartner research in this publication does not indicate Gartner's endorsement of EventTracker's products and/or strategies. Reproduction or distribution of this publication in any form without Gartner's prior written permission is forbidden. The information contained herein has been obtained from sources believed to be reliable. Gartner disclaims all warranties as to the accuracy, completeness or adequacy of such information. The opinions expressed herein are subject to change without notice. Although Gartner research may include a discussion of related legal issues, Gartner does not provide legal advice or services and its research should not be construed or used as such. Gartner is a public company, and its shareholders may include firms and funds that have financial interests in entities covered in Gartner research. Gartner's Board of Directors may include senior managers of these firms or funds. Gartner research is produced independently by its research organization without input or influence from these firms, funds or their managers. For further information on the independence and integrity of Gartner research, see "Guiding Principles on Independence and Objectivity" on its website, http://www.gartner.com/technology/about/ombudsman/omb_guide2.jsp.