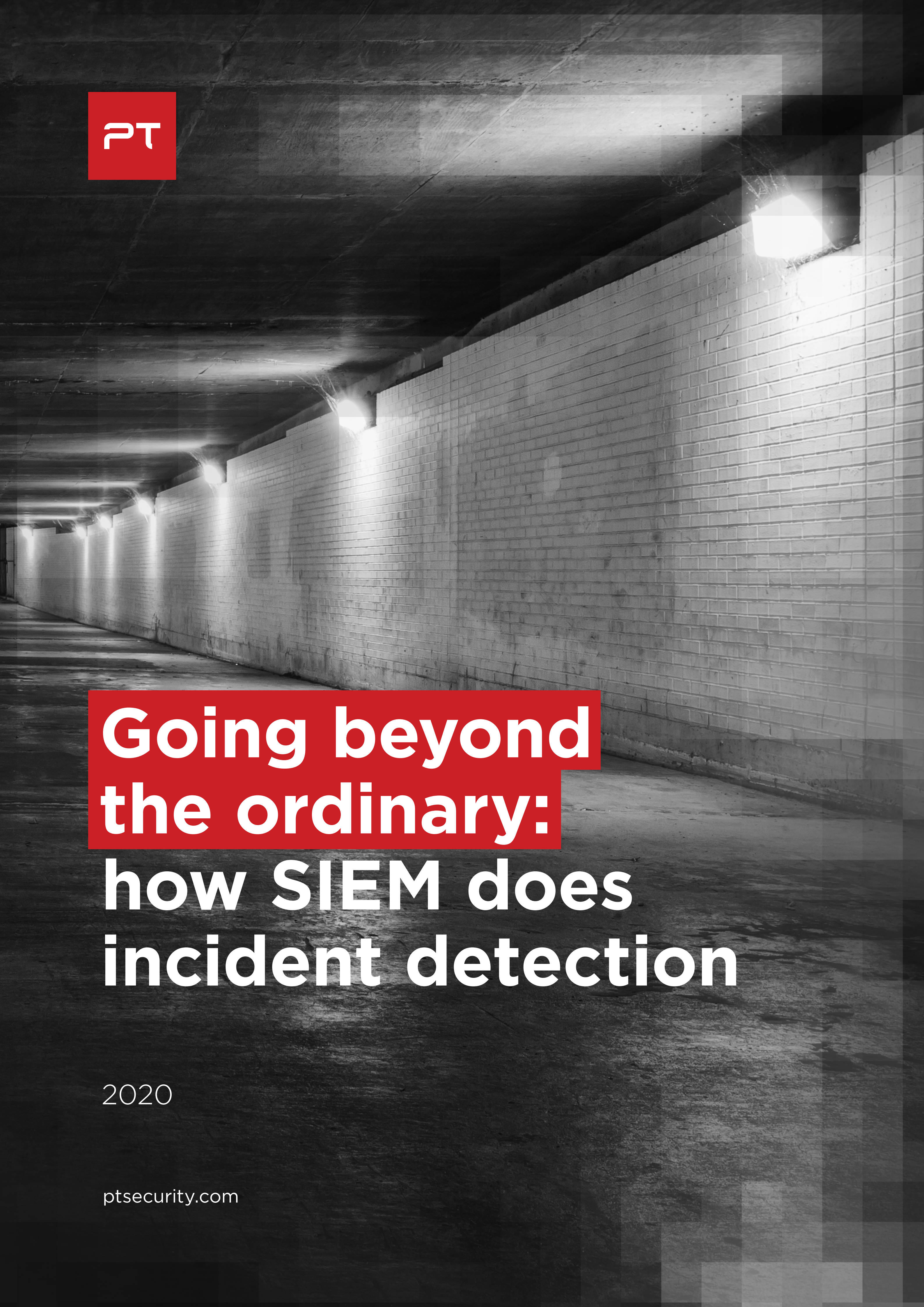


Going beyond the ordinary: how SIEM does incident detection

2020

ptsecurity.com

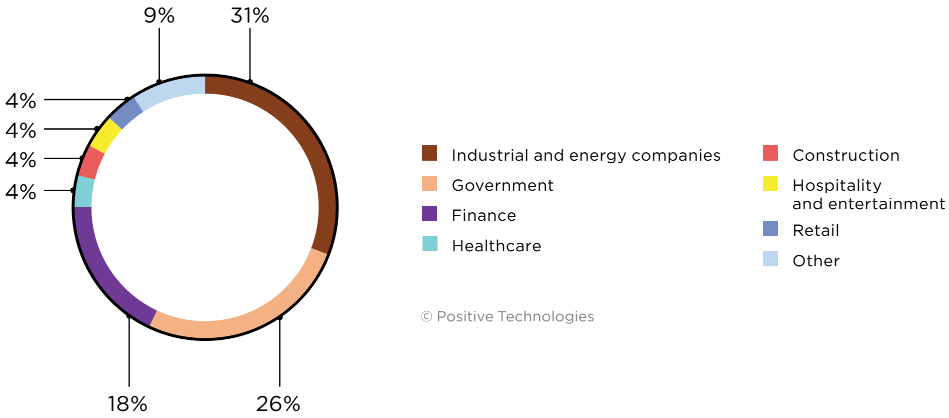
Contents

About the research

Company infrastructures are rich with events potentially indicating security incidents, such as user violations of security policies or a breach of the local network. Security information and event management (SIEM) solutions perform centralized collection and analysis of event information. SIEM solutions do more than just collect event information from diverse sources including network devices, applications, OS logs, and security software. They also automate the incident detection process and provide timely notifications to security teams. A pilot project can demonstrate the value of the SIEM approach in maximally life-like conditions. By working with such projects, experts provide a great deal of useful feedback that helps to continue shaping the product.

In this document, we will describe the results of 23 pilot projects involving MaxPatrol SIEM in the second half of 2019 and early 2020.[1] We will use this dataset to show how information from diverse sources can be combined with SIEM to detect corporate security incidents in an effective way. We will also touch on how to use a SIEM solution to get some "unusual" jobs done.

124 days
average pilot project duration



© Positive Technologies

Figure 1. Participant portrait

[1] *The dataset consists of pilot deployments of MaxPatrol SIEM for which the designated project infrastructure and resulting data were sufficient for detecting actual incidents. Statistics do not include companies that declined to consent to use of anonymized results from the pilot project for research purposes.*

How to get started detecting incidents with SIEM

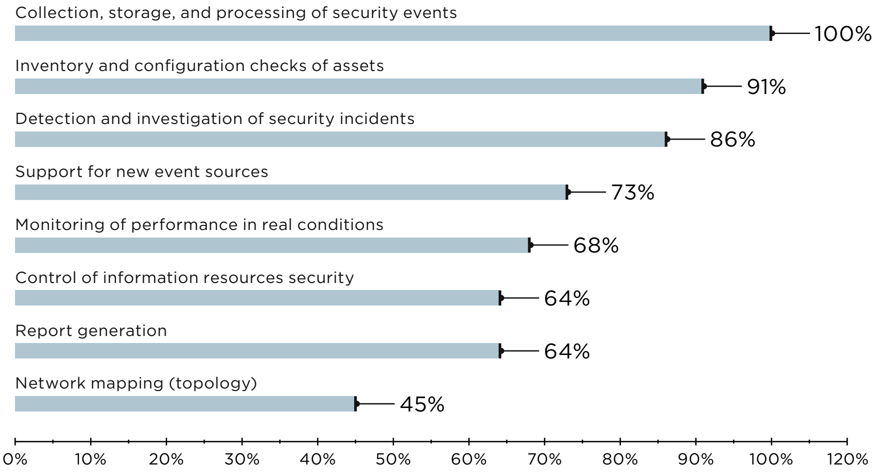
Careful preparation is necessary before starting to detect incidents with a SIEM solution. For clients, we advise the following steps:

1. Outline the tasks you want to perform with SIEM. Consider your infrastructure, security policies, industry guidelines, and regulatory requirements.
2. Determine which sources need to be connected to SIEM for those tasks.
3. When preparing for a pilot deployment, clearly delineate the pilot zone. Whichever part of infrastructure you choose for the pilot, make sure that it is sufficient for evaluating the SIEM solution and accomplishing your objectives.

Now we will look more closely at the tasks that we have helped to perform with SIEM in pilot projects and consider which sources should be connected for detecting various incident types. We will also give examples of actual incidents and attacks detected during our pilot projects.

Doing both the usual and the unusual with SIEM

Traditionally, a SIEM system is responsible for accumulation and timely processing of data about security events. The most important tasks of any pilot project, therefore, are to collect, store, and process security events. But SIEM solutions are capable of doing more. They can also help to detect and investigate security incidents, perform asset inventories, and monitor the state of protection. The tasks for the pilot project should harmonize with the overall objectives for use of SIEM at the company.



© Positive Technologies

Figure 2. List of popular tasks for MaxPatrol SIEM pilot deployments (percentage of projects)

We always recommend articulating tasks that are truly important to the client company, as well as attuned to its infrastructure and regulatory requirements. Companies should not stop at simply seeing whether SIEM is on and working. This approach enables assessing SIEM functionality, verifying configuration, determining which event sources are necessary for performance of the stated tasks, and making sure there are no blind spots.

Real-life example: unauthorized assets

At one company, the SIEM solution was configured to detect any unauthorized assets on the network. This caused the discovery that IT staff members were adding assets without informing the security team. Thanks to built-in inventory capabilities, it became possible to detect development-related events in real time and standardize the DevOps process.

Task	**Solution**
Monitor privilege escalation on Linux servers	Created correlation rule to monitor all privilege escalations. If an account that is not in the list of allowed accounts requests privilege escalation, an incident is generated.
Monitor unauthorized connections by laptops to the client's network equipment	Implemented monitoring of MAC addresses on network device ports. If a MAC address is added or removed, an incident is generated.
Monitor unauthorized use of remote access software	Created a list of workstations on which connections by DameWare (used at the client for technical support) are forbidden. If a remote connection is made to any of the workstations in the list, an incident is generated.

© Positive Technologies

Figure 3. Examples of other tasks performed in SIEM pilot deployments

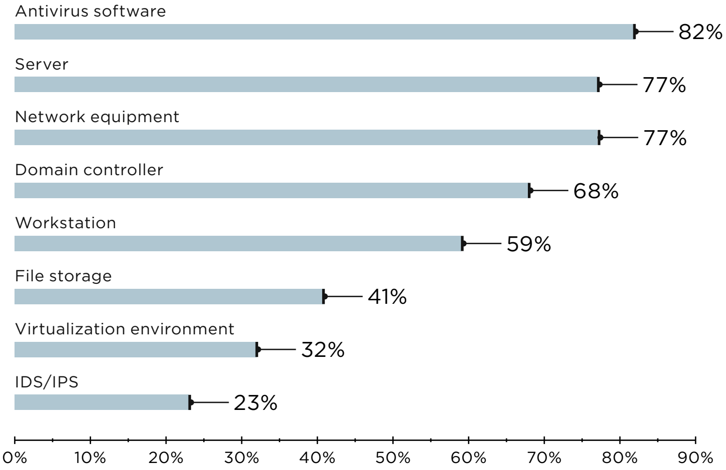
Event sources

The search for incidents starts with connecting sources that generate a wide range of events. For the fullest possible picture of what is happening on infrastructure, we recommend connecting all sources of IT and security events to the SIEM solution.

IT sources refer to applications and software that generate IT events. IT sources do not evaluate events as being "good" or "bad." Examples: server and workstation logs (access control, uptime, policy compliance), network equipment (configuration changes, device access).

Security event sources are specially made software and hardware products that generate security events. These sources are enriched with external knowledge for interpreting any given event as "good" or "bad" for security. Examples: IDS/IPS (for collecting data on network attacks), antivirus software (for detection of malware).

A pilot project can be hosted either on a testbed (imitating part of the client's actual infrastructure) or in a designated pilot zone that includes multiple sources.



© Positive Technologies

Figure 4. Popular event sources connected to MaxPatrol SIEM pilot deployments (percentage of projects)

For universal coverage of event sources, SIEM should be able to interact with a wide range of network protocols and technologies, including syslog, WMI, RPC, Telnet, SSH, and ODBC. The syslog protocol is used for getting messages from system logs and Windows security logs (WinEventLog, WindowsAudit) on servers and workstations. Thanks to this, the SIEM solution obtains information about events defined by Windows audit policies (such as login, access to objects, and changes in privileges). WMI allows collecting information from Windows devices about creation, modification, or deletion of files with a certain extension; connection of physical devices; launch of OS services; and more. It is also a good idea to use Sysmon, an extended audit tool, since the Windows audit log does not retain all information. Sysmon tracks any changes to registry keys, retrieval of hashes of user passwords, malicious network activity, and malware sources (including the hash value of the file that started a process).

> *Not all incidents can be detected just with data from servers and workstations. For detecting attacks in network traffic (such as malware tunneling or DCSync attacks) we recommended using supplemental solutions such as Network Traffic Analysis (NTA) or Network Detection Response (NDR).*

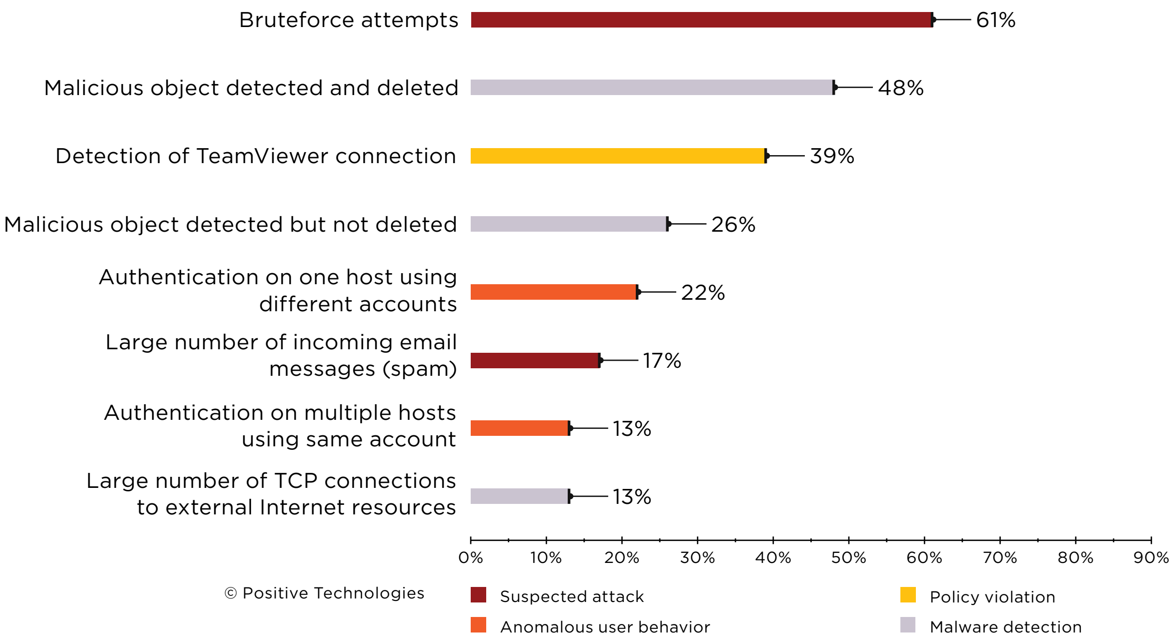
Here is a list of key security events detectable by SIEM and corresponding event sources:

Security event	***Event source***
Malicious content delivered by legitimate means, usually by email (spam and phishing)	▪ Proxy servers with content checks ▪ Web traffic protection ▪ Email protection ▪ Endpoint protection with built-in web resource and email checks
Reconnaissance of company infrastructure: discovery of available services and vulnerable hosts	▪ Firewalls ▪ IDS/IPS
Disruption to availability of services and systems (such as a DDoS attack)	▪ Firewalls ▪ IDS/IPS ▪ DoS detection and blocking systems
Exploitation of vulnerabilities in system components	▪ IDS/IPS
Use of hacker utilities to obtain system access or perform other forbidden actions	▪ IDS/IPS ▪ Security scanners and audit tools ▪ Antivirus software

Security event	***Event source***
Malicious code execution	▪ Antivirus software ▪ IDS/IPS
Violation of security policies or regulatory non-compliance (such as with PCI DSS)	▪ Vulnerability scanners
Loss of sensitive data over any communication channel	▪ Data loss prevention (DLP) systems
Detection of anomalies and significant deviations in an object or its behavior from the norm	▪ Next-generation firewall (NGFW) ▪ Data loss prevention (DLP) systems ▪ User and entity behavior analytics systems

Detection of bona fide security incidents

During SIEM pilot projects, we frequently model the conditions that would lead to detection of a cyberincident. However, even without modeling, MaxPatrol SIEM detected real security incidents in 100 percent of the projects in the dataset of this report. The pilot projects uncovered security events consistent with cyberattacks, malware infection, security policy violations, and anomalous user behavior.



© Positive Technologies

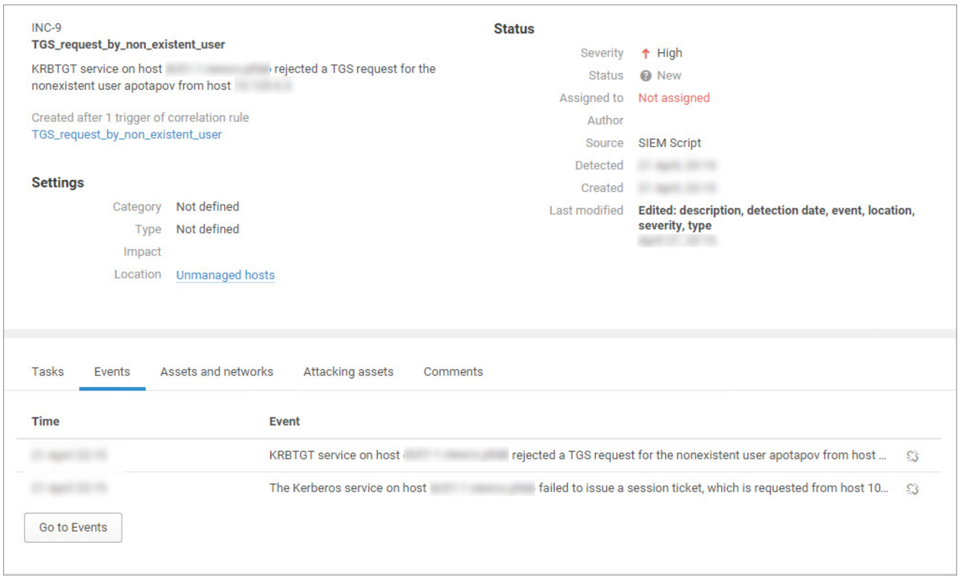
Figure 5. Most frequently detected security incidents in MaxPatrol SIEM pilot deployments (percentage of projects)

Suspected attack

Positive Technologies frequently identifies traces of prior cyberattacks during penetration testing of client infrastructure. In these cases, one of two things is true: the attack went unnoticed entirely, or incident investigation did not result in detection of all compromised hosts and full remediation of the consequences. The inability to "see" all the events on company infrastructure can be caused both by lack of proper tools for attack detection and insufficient data from event sources.

Our pilot projects led to identification of events indicating potential attacks. Many of these events are caused by attacker attempts to study the compromised system and internal network. Once on the internal network, attackers need to figure out where they are on the victim's infrastructure, decide what to do next, and get user credentials for connecting to servers and workstations. Timely detection of such events aids in stopping cyberattacks at the early stages and minimizing the damage.

For example, in one pilot project we detected a request for a Kerberos session ticket for a non-existent user. Such events can indicate service misconfiguration (such as if the account for running the service was deleted but the service itself continued to function) or an attempt to enumerate users.



INC-9
TGS_request_by_non_existent_user
KRBTGT service on host [redacted] rejected a TGS request for the nonexistent user apotapov from host [redacted]

Created after 1 trigger of correlation rule
TGS_request_by_non_existent_user

Settings

Category	Not defined
Type	Not defined
Impact	
Location	Unmanaged hosts

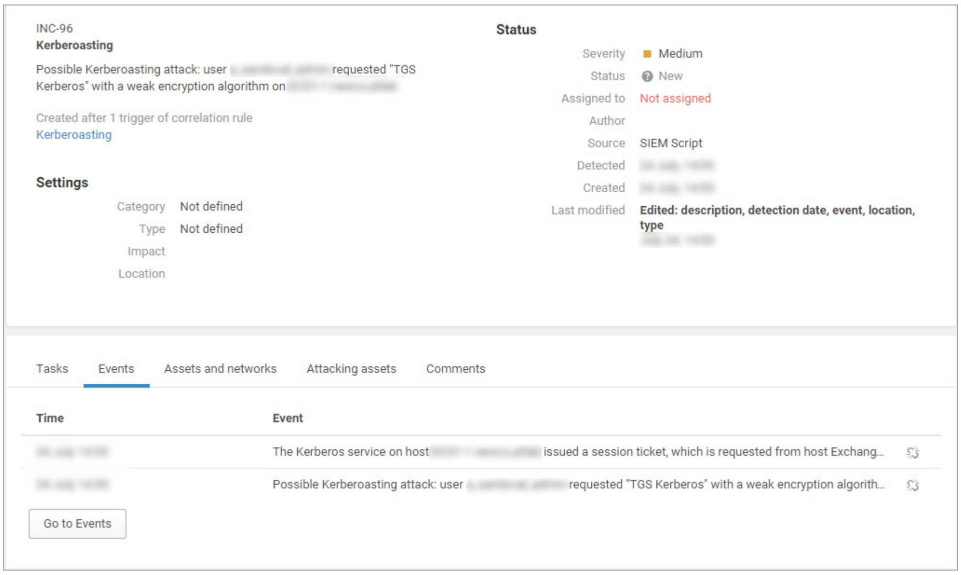
Status

Severity	↑ High
Status	New
Assigned to	Not assigned
Author	
Source	SIEM Script
Detected	[redacted]
Created	[redacted]
Last modified	**Edited: description, detection date, event, location, severity, type** [redacted]

Time	Event
[redacted]	KRBTGT service on host [redacted] rejected a TGS request for the nonexistent user apotapov from host ...
[redacted]	The Kerberos service on host [redacted] failed to issue a session ticket, which is requested from host 10...

Figure 6. A Kerberos Session Ticket for Non-Existent User incident

When targeting the domain controller on domains that use Kerberos authentication, attackers may use Kerberoasting. Any user logged in on the domain can request a Kerberos Ticket Granting Service (TGS) ticket. The TGS ticket is encrypted with the NT hash of the password of the user who launched the service. An attacker who has the TGS ticket can decrypt it by bruteforcing the password of the associated service account, since the password is often found in a dictionary or otherwise easy to guess. Such attacks were found in a number of pilot projects.



INC-96
Kerberoasting

Possible Kerberoasting attack: user [redacted] requested "TGS Kerberos" with a weak encryption algorithm on [redacted]

Created after 1 trigger of correlation rule
Kerberoasting

Settings

Category	Not defined
Type	Not defined
Impact	
Location	

Status

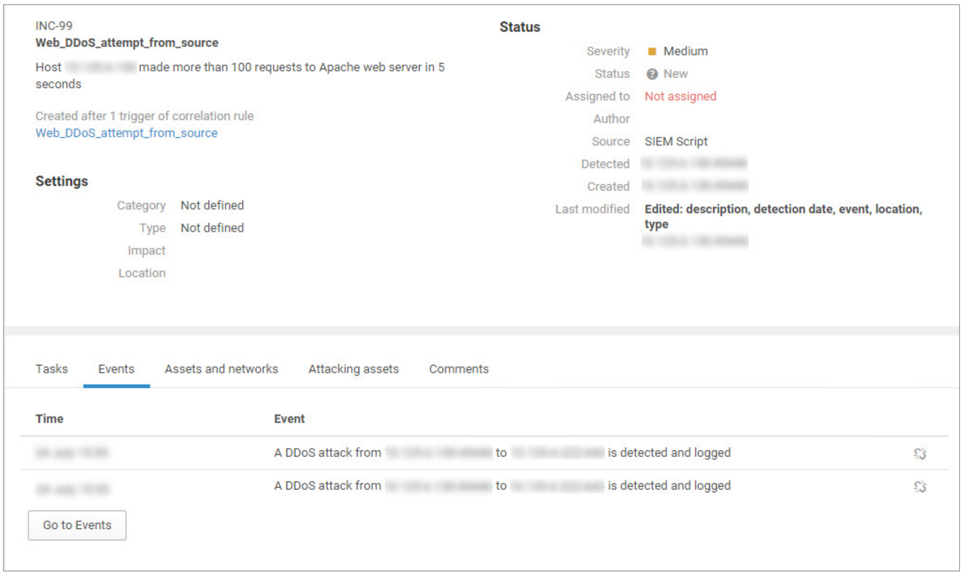
Severity	■ Medium
Status	New
Assigned to	Not assigned
Author	
Source	SIEM Script
Detected	[redacted]
Created	[redacted]
Last modified	**Edited: description, detection date, event, location, type** [redacted]

Time	Event
[redacted]	The Kerberos service on host [redacted] issued a session ticket, which is requested from host Exchang...
[redacted]	Possible Kerberoasting attack: user [redacted] requested "TGS Kerberos" with a weak encryption algorith...

Figure 7. A Kerberoasting Attack incident

Enumeration of users with Kerberos and Kerberoasting corresponds to Discovery and Credential Access under the MITRE ATT&CK classification. A SIEM solution with rules for detecting common tactics, techniques, and procedures (TTPs) can detect attackers while they are still trying to discover domain accounts, applications, and services.

SIEM can also assist in detecting other types of attacks. One pilot project came just in the nick of time to stop a DDoS attack. After analysis of the external addresses used by the attackers, these addresses were blocked on the corporate firewall.



INC-99
Web_DDoS_attempt_from_source

Host [redacted] made more than 100 requests to Apache web server in 5 seconds

Created after 1 trigger of correlation rule
Web_DDoS_attempt_from_source

Settings

Category	Not defined
Type	Not defined
Impact	
Location	

Status

Severity	■ Medium
Status	New
Assigned to	Not assigned
Author	
Source	SIEM Script
Detected	[redacted]
Created	[redacted]
Last modified	**Edited: description, detection date, event, location, type** [redacted]

Time	Event
[redacted]	A DDoS attack from [redacted] to [redacted] is detected and logged
[redacted]	A DDoS attack from [redacted] to [redacted] is detected and logged

Figure 8. Detection of DDoS with MaxPatrol SIEM

A number of pilot projects included retrospective analysis of security events that turned up attacks and compromises that previously had been overlooked or unrightly neglected. We were able to detect and stop a targeted attack on one company that had lasted at least eight years. Based on analysis of SIEM event logs, we found traces of attacker actions on 195 infrastructure hosts.

As the investigation showed, the intruders had been active for that entire time, using malware for:

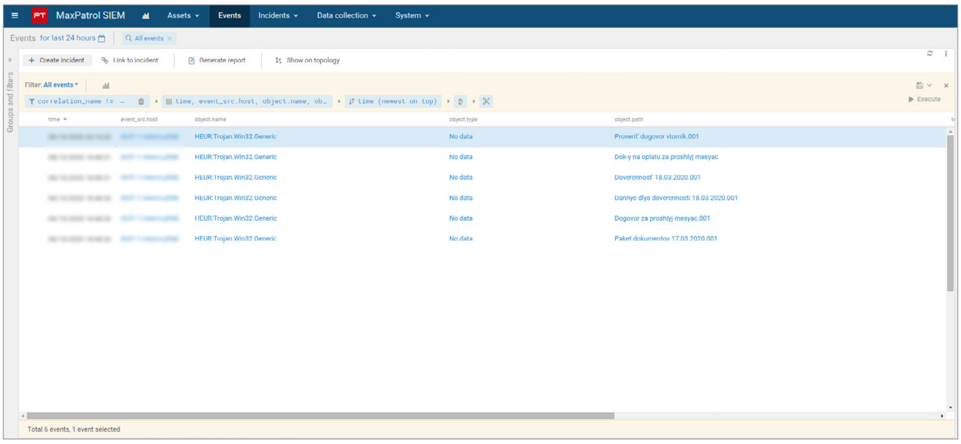
- Communicating with the C2 server
- Remotely executing commands
- Probing the compromised infrastructure
- Extracting credentials from hosts
- Compressing data
- Sending and receiving files from the C2 server

Soon after, the attackers' C2 servers were blocked and the attacker presence was eliminated. Positive Technologies investigators attributed the attack to the TaskMasters group.

Malware detection

One fifth of incidents detected in pilot projects involved malware. Most of these incidents (about 85%) started with phishing emails. According to our report on APT threats to companies worldwide, 90 percent of groups start their attacks with such phishing.

In one pilot project we detected a large number of malicious messages, containing Trojan-Banker.RTM in particular, sent by company employees from 592 different IP addresses. Operators of this malware tend to be interested in corporate bank accounts and therefore target their mailings to accountants and financial staff. They imitate legitimate correspondence, with such subject lines as "Refund request," "Documents for last month," and "Employee passport details."



Filter: All events *

```
correlation_name != –   |||  time, event_src.host, object.name, ob…   time (newest on top)
```

time	event_src.host	object.name	object.type	object.path
[redacted]	[redacted]	HEUR:Trojan.Win32.Generic	No data	Proverit' dogovor vtornik.001
[redacted]	[redacted]	HEUR:Trojan.Win32.Generic	No data	Dok-y na oplatu za proshlyj mesyac
[redacted]	[redacted]	HEUR:Trojan.Win32.Generic	No data	Doverennost' 18.03.2020.001
[redacted]	[redacted]	HEUR:Trojan.Win32.Generic	No data	Dannye dlya doverennosti 18.03.2020.001
[redacted]	[redacted]	HEUR:Trojan.Win32.Generic	No data	Dogovor za proshlyj mesyac.001
[redacted]	[redacted]	HEUR:Trojan.Win32.Generic	No data	Paket dokumentov 17.03.2020.001

Total 6 events, 1 event selected

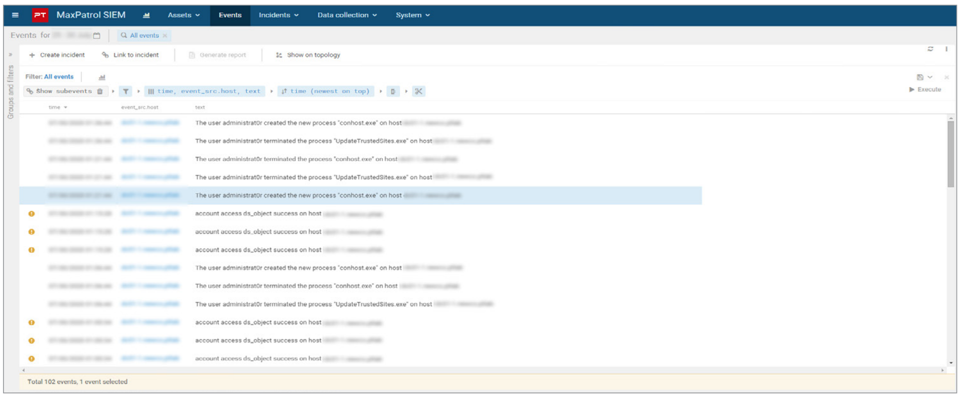
Figure 9. Detection of phishing with MaxPatrol SIEM

Real-life example: phishing

At one company, we detected activity by an attacker who had breached the network perimeter by means of a phishing message. The malware had started collecting information about the network. The SIEM solution flagged that an asset in the user group (accounting) was running administrative commands to collect domain information. In this case, SIEM detected a phishing-related compromise that had gone unnoticed by another layer of protection.

Anomalous user behavior

In our report on internal penetration testing, we noted that methods for attacking an internal network can involve exploitation of software vulnerabilities, OS architectures and authentication mechanisms, as well as legitimate actions enabled by system functionality. Legitimate actions, for the purpose of pursuing an attack, comprise almost half of our pentesters' actions. Such actions can be hard to tell apart from the everyday activity of users or admins, but may still indicate the hidden presence of attackers. This is why anomalous user behavior should act as a trigger for more detailed review of events. For example, events of particular interest should include attempts to export lists of local groups or users, as well as creation of a new account right after logging in. Several SIEM pilot projects detected use of a single account on multiple workstations, which may mean a compromise of account credentials. Employee activity during the nighttime may also warrant suspicion.



```
Show subevents › ▼ › time, event_src.host, text › time (newest on top)
```

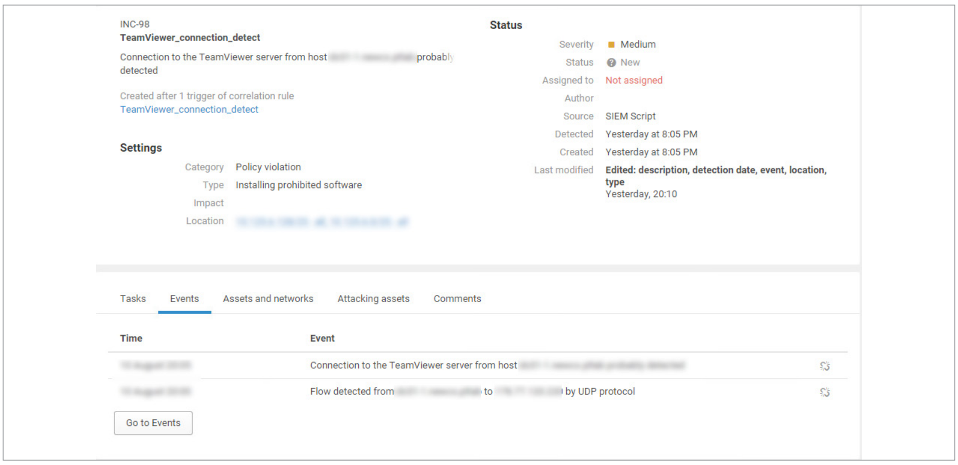
	time	event_src.host	text
	[redacted]	[redacted]	The user administrat0r created the new process "conhost.exe" on host [redacted]
	[redacted]	[redacted]	The user administrat0r terminated the process "UpdateTrustedSites.exe" on host [redacted]
	[redacted]	[redacted]	The user administrat0r terminated the process "conhost.exe" on host [redacted]
	[redacted]	[redacted]	The user administrat0r terminated the process "UpdateTrustedSites.exe" on host [redacted]
	[redacted]	[redacted]	The user administrat0r created the new process "conhost.exe" on host [redacted]
!	[redacted]	[redacted]	account access ds_object success on host [redacted]
!	[redacted]	[redacted]	account access ds_object success on host [redacted]
!	[redacted]	[redacted]	account access ds_object success on host [redacted]
	[redacted]	[redacted]	The user administrat0r created the new process "conhost.exe" on host [redacted]
	[redacted]	[redacted]	The user administrat0r terminated the process "conhost.exe" on host [redacted]
	[redacted]	[redacted]	The user administrat0r terminated the process "UpdateTrustedSites.exe" on host [redacted]
!	[redacted]	[redacted]	account access ds_object success on host [redacted]
!	[redacted]	[redacted]	account access ds_object success on host [redacted]
!	[redacted]	[redacted]	account access ds_object success on host [redacted]

Total 102 events, 1 event selected

Figure 10. Example of a Nighttime Activity incident

Policy violations

Violations of security policies form another category of incidents. These violations refer to non-compliance with regulatory requirements (such as PCI DSS) or corporate security policies. These documents are intended to ensure an acceptable level of company-wide protection. However, users do not always comply with them in practice. During the pilot projects, policy violations were detected at half of companies. In 39 percent of pilot projects, remote administration software was detected. These events may be legitimate: for example, technical support may need to connect to a server remotely to perform configuration. But the events may also indicate use by attackers of Remote Access Tools for accessing internal resources. Companies are advised to restrict which computers are allowed to run remote access software.



INC-98
TeamViewer_connection_detect
Connection to the TeamViewer server from host [redacted] probably detected

Created after 1 trigger of correlation rule
TeamViewer_connection_detect

Settings

Category: Policy violation
Type: Installing prohibited software
Impact:
Location: [redacted]

Status

Severity: ■ Medium
Status: New
Assigned to: Not assigned
Author:
Source: SIEM Script
Detected: Yesterday at 8:05 PM
Created: Yesterday at 8:05 PM
Last modified: **Edited: description, detection date, event, location, type**
Yesterday, 20:10

Time	Event
[redacted]	Connection to the TeamViewer server from host [redacted]
[redacted]	Flow detected from [redacted] to [redacted] by UDP protocol

Figure 11. A TeamViewer Use incident

Real-life example: policy compliance

SIEM can be used to verify security compliance. One company needed to eliminate use of certain software; with the help of the SIEM solution, it could now detect when that software was being used. In another case, SIEM was used at several clients to verify compliance with password change policies.

Conclusion

All companies experience security incidents, including malware and events potentially indicating a cyberattack or policy violation. Penetration tests carried out by Positive Technologies confirm that companies often find traces of earlier hacker attacks that were not detected by security teams at the time. Detecting attacks at the early stages requires knowing about everything going on inside corporate infrastructure. Collecting as much information as possible is key: more events and more connected sources mean higher odds of catching suspicious activity, taking action, and minimizing damage.

The sheer amount of data makes automated processing, such as with SIEM, the only feasible option. SIEM solutions use correlation to find connections within the data and identify potential incident scenarios. The experience of the PT Expert Security Center shows that SIEM correlation rules are the starting point for detection of most cyberattacks,[2] including multistage APTs, and for incident investigation. Connecting an additional NTA/NDR solution for deep traffic analysis broadens the reach of SIEM to include network traffic as well as hosts. No matter what kinds of protection are in place, incident investigation always requires skilled experts to fully reconstruct the kill chain and consider further steps.

[2] *MaxPatrol SIEM draws on built-in correlation rules to flag relevant TTPs without requiring additional configuration. MaxPatrol SIEM also contains detection rules for popular attacker TTPs (under the MITRE ATT&CK classification) for detecting attacks at the early stages.*

About Positive Technologies

ptsecurity.com
pt@ptsecurity.com
facebook.com/PositiveTechnologies
facebook.com/PHDays

For 18 years, Positive Technologies has been creating innovative solutions for information security. We develop products and services to detect, verify, and neutralize the real-world business risks associated with corporate IT infrastructure. Our technologies are backed by years of research experience and the expertise of world-class cybersecurity experts.

Over 2,000 companies in 30 countries trust us to keep them safe.

Follow us on social media (LinkedIn, Twitter) and the News section at ptsecurity.com.