Backdoors & Breaches

Procedures Cards

BLACK HILLS
Information Security

BLACK HILLS
Information Security

Crisis Management

Your Legal and Management Teams have procedures for effectively and ethically notifying impacted victims of compromises.

NOTES

This counteracts the "Data Uploaded to Pastebin" Inject Card.

TOOLS

This almost never happens. But, a good notification strategy will really help deal with the political fallout.

Security Information and Event Management (SIEM) Log Analysis

Yeah... good luck with this one. Are you logging the right things? Do you regularly emulate attack scenarios to see if you can detect them?

TOOLS

SOF-ELK
JPCert Tools Analysis

https://github.com/philhagen/sof-elk
https://jpcertcc.github.io/ToolAnalysisResultSheet

Endpoint Analysis

This is where the defenders use their SANS IR Cheat Sheets to detect attacks on workstations. Time to bring in the Help Desk... and pray.

TOOLS

DeepBlueCLI
SANS IR Cheat Sheets

https://github.com/sans-blue-team/DeepBlueCLI

User and Entity Behavior Analytics (UEBA)

It's like logging, but it actually works. UEBA looks for multiple concurrent logins, impossible logins based on geography, unusual file access, passwords sprays, and more!

TOOLS

LogonTracer

https://github.com/JPCERTCC/LogonTracer

Server Analysis

The ability to baseline a system and verify that it is operating in a normal state. By the way, this is more than simply running Task Manager and looking for evil_backdoor.exe.

TOOLS

DeepBlueCLI
SANS Analysis Cheat Sheets

https://github.com/sans-blue-team/DeepBlueCLI

Isolation

Your Network Team is on their game. They can easily isolate infected systems to prevent further harm.

TOOLS

Switch and Router Commands

Firewall Log Review

Can your organization analyze and understand firewall logs? Do you regularly emulate attack scenarios and verify that your procedures work?

TOOLS

SOF-ELK

https://github.com/philhagen/sof-elk

Internal Segmentation

Turn on your host-based firewalls. Segment different organizational units. Treat the internal network as hostile, because it is.

TOOLS

netsh advfirewall
Windows Defender Firewall
iptables

NetFlow, Zeek/Bro, Real Intelligence Threat Analytics (RITA) Analysis

Does your organization capture and review network traffic? Good! Do you know how to parse and review it? Is that process documented? Or, do you just run Zeek/Security Onion/ELK because the cool kids are doing it?

TOOLS

Real Intelligence Threat Analytics (RITA)
Security Onion
AI-Hunter

https://www.activecountermeasures.com/free-tools/rita
https://securityonion.net
https://www.activecountermeasures.com

Endpoint Security Protection Analysis

We know, you have AV. Great! Do you actually get alerts and logs? Do you immediately review them? Or, do you simply turn it on and walk away while the network explodes like you're in a bad action movie?

TOOLS

Check with your vendor, they miss you and always want to chat.

Server Analysis

The ability to baseline a system and verify that it is operating in a normal state. By the way, this is more than simply running Task Manager and looking for evil_backdoor.exe.

TOOLS

DeepBlueCLI
SANS Analysis Cheat Sheets

https://github.com/sans-blue-team/DeepBlueCLI

Security Information and Event Management (SIEM) Log Analysis

Yeah... good luck with this one. Are you logging the right things? Do you regularly emulate attack scenarios to see if you can detect them?

TOOLS

SOF-ELK
JPCert Tools Analysis

JPCERT CC®

https://github.com/philhagen/sof-elk
https://jpcertcc.github.io/ToolAnalysisResultSheet

Firewall Log Review

Can your organization analyze and understand firewall logs? Do you regularly emulate attack scenarios and verify that your procedures work?

TOOLS

SOF-ELK

https://github.com/philhagen/sof-elk

Internal Segmentation

Turn on your host-based firewalls. Segment different organizational units. Treat the internal network as hostile, because it is.

TOOLS

netsh advfirewall
Windows Defender Firewall
iptables

Crisis Management

Your Legal and Management Teams have procedures for effectively and ethically notifying impacted victims of compromises.

NOTES

This counteracts the "Data Uploaded to Pastebin" Inject Card.

TOOLS

This almost never happens. But, a good notification strategy will really help deal with the political fallout.

Isolation

Your Network Team is on their game. They can easily isolate infected systems to prevent further harm.

TOOLS

Switch and Router Commands

Endpoint Analysis

This is where the defenders use their SANS IR Cheat Sheets to detect attacks on workstations. Time to bring in the Help Desk... and pray.

TOOLS

DeepBlueCLI
SANS IR Cheat Sheets

https://github.com/sans-blue-team/DeepBlueCLI

User and Entity Behavior Analytics (UEBA)

It's like logging, but it actually works. UEBA looks for multiple concurrent logins, impossible logins based on geography, unusual file access, passwords sprays, and more!

TOOLS

LogonTracer

abNORMAL

https://github.com/JPCERTCC/LogonTracer

NetFlow, Zeek/Bro, Real Intelligence Threat Analytics (RITA) Analysis

Does your organization capture and review network traffic? Good! Do you know how to parse and review it? Is that process documented? Or, do you just run Zeek/Security Onion/ELK because the cool kids are doing it?

TOOLS

Real Intelligence Threat Analytics (RITA)
Security Onion
AI-Hunter

Security Onion
AI HUNTER

https://www.activecountermeasures.com/free-tools/rita
https://securityonion.net
https://www.activecountermeasures.com

Endpoint Security Protection Analysis

We know, you have AV. Great! Do you actually get alerts and logs? Do you immediately review them? Or, do you simply turn it on and walk away while the network explodes like you're in a bad action movie?

TOOLS

Check with your vendor, they miss you and always want to chat.

Backdoors & Breaches

Scenario 2

BLACK HILLS Information Security

NetFlow, Zeek/Bro, Real Intelligence Threat Analytics (RITA) Analysis

Does your organization capture and review network traffic? Good! Do you know how to parse and review it? Is that process documented? Or, do you just run Zeek/Security Onion/ELK because the cool kids are doing it?

TOOLS

Real Intelligence Threat Analytics (RITA)
Security Onion
AI-Hunter

Security Onion

AI HUNTER

https://www.activecountermeasures.com/free-tools/rita
https://securityonion.net
https://www.activecountermeasures.com

Endpoint Security Protection Analysis

We know, you have AV. Great! Do you actually get alerts and logs? Do you immediately review them? Or, do you simply turn it on and walk away while the network explodes like you're in a bad action movie?

TOOLS

Check with your vendor, they miss you and always want to chat.

Firewall Log Review

Can your organization analyze and understand firewall logs? Do you regularly emulate attack scenarios and verify that your procedures work?

TOOLS

SOF-ELK

https://github.com/philhagen/sof-elk

Internal Segmentation

Turn on your host-based firewalls. Segment different organizational units. Treat the internal network as hostile, because it is.

TOOLS

netsh advfirewall
Windows Defender Firewall
iptables

Crisis Management

Your Legal and Management Teams have procedures for effectively and ethically notifying impacted victims of compromises.

NOTES

This counteracts the "Data Uploaded to Pastebin" Inject Card.

TOOLS

This almost never happens. But, a good notification strategy will really help deal with the political fallout.

Isolation

Your Network Team is on their game. They can easily isolate infected systems to prevent further harm.

TOOLS

Switch and Router Commands

Endpoint Analysis

This is where the defenders use their SANS IR Cheat Sheets to detect attacks on workstations. Time to bring in the Help Desk... and pray.

TOOLS

DeepBlueCLI
SANS IR Cheat Sheets

https://github.com/sans-blue-team/DeepBlueCLI

User and Entity Behavior Analytics (UEBA)

It's like logging, but it actually works. UEBA looks for multiple concurrent logins, impossible logins based on geography, unusual file access, passwords sprays, and more!

TOOLS

LogonTracer

abNORMAL

https://github.com/JPCERTCC/LogonTracer

Server Analysis

The ability to baseline a system and verify that it is operating in a normal state. By the way, this is more than simply running Task Manager and looking for evil_backdoor.exe.

TOOLS

DeepBlueCLI
SANS Analysis Cheat Sheets

https://github.com/sans-blue-team/DeepBlueCLI

Security Information and Event Management (SIEM) Log Analysis

Yeah... good luck with this one. Are you logging the right things? Do you regularly emulate attack scenarios to see if you can detect them?

TOOLS

SOF-ELK
JPCert Tools Analysis

JPCERT CC®

https://github.com/philhagen/sof-elk
https://jpcertcc.github.io/ToolAnalysisResultSheet

Backdoors & Breaches

BLACK HILLS Information Security

NetFlow, Zeek/Bro, Real Intelligence Threat Analytics (RITA) Analysis

Does your organization capture and review network traffic? Good! Do you know how to parse and review it? Is that process documented? Or, do you just run Zeek/Security Onion/ELK because the cool kids are doing it?

TOOLS

Real Intelligence Threat Analytics (RITA)
Security Onion
AI-Hunter

Security Onion

AI HUNTER

https://www.activecountermeasures.com/free-tools/rita
https://securityonion.net
https://www.activecountermeasures.com

Security Information and Event Management (SIEM) Log Analysis

Yeah... good luck with this one. Are you logging the right things? Do you regularly emulate attack scenarios to see if you can detect them?

TOOLS

SOF-ELK
JPCert Tools Analysis

JPCERT CC®

https://github.com/philhagen/sof-elk
https://jpcertcc.github.io/ToolAnalysisResultSheet

Isolation

Your Network Team is on their game. They can easily isolate infected systems to prevent further harm.

TOOLS

Switch and Router Commands

Endpoint Security Protection Analysis

We know, you have AV. Great! Do you actually get alerts and logs? Do you immediately review them? Or, do you simply turn it on and walk away while the network explodes like you're in a bad action movie?

TOOLS

Check with your vendor, they miss you and always want to chat.

Firewall Log Review

Can your organization analyze and understand firewall logs? Do you regularly emulate attack scenarios and verify that your procedures work?

TOOLS

SOF-ELK

https://github.com/philhagen/sof-elk

Crisis Management

Your Legal and Management Teams have procedures for effectively and ethically notifying impacted victims of compromises.

NOTES

This counteracts the "Data Uploaded to Pastebin" Inject Card.

TOOLS

This almost never happens. But, a good notification strategy will really help deal with the political fallout.

Endpoint Analysis

This is where the defenders use their SANS IR Cheat Sheets to detect attacks on workstations. Time to bring in the Help Desk... and pray.

TOOLS

DeepBlueCLI
SANS IR Cheat Sheets

https://github.com/sans-blue-team/DeepBlueCLI

User and Entity Behavior Analytics (UEBA)

It's like logging, but it actually works. UEBA looks for multiple concurrent logins, impossible logins based on geography, unusual file access, passwords sprays, and more!

TOOLS

LogonTracer

abNORMAL

https://github.com/JPCERTCC/LogonTracer

Server Analysis

The ability to baseline a system and verify that it is operating in a normal state. By the way, this is more than simply running Task Manager and looking for evil_backdoor.exe.

TOOLS

DeepBlueCLI
SANS Analysis Cheat Sheets

https://github.com/sans-blue-team/DeepBlueCLI

Internal Segmentation

Turn on your host-based firewalls. Segment different organizational units. Treat the internal network as hostile, because it is.

TOOLS

netsh advfirewall
Windows Defender Firewall
iptables

Backdoors & Breaches

Scenario 4

BLACK HILLS Information Security