Blumira + ThreatGEN

Cybersecurity Visibility For IT/OT Threats

Because ICS security doesn’t exist in a vacuum

01

Oil & Gas Customer Case Study

The Challenge: Lack of Security Visibility

A ThreatGEN Midstream oil and gas company customer was concerned they were sailing blind:

- No visibility in threats on either the IT or OT side of the organization
- Asset management was lacking
- Missing ability to record and playback incidents

The Solution

It's critical to monitor cybersecurity across converging OT/IT systems

- Hybrid technologies that combine IT/OT
- Provide broad, org-wide security monitoring and alerting solution
- Asset management, IDS/IPS for network and host
- A cloud SIEM platform for automated detection & response

Forescout for IT/OT Monitoring

- **To inventory & monitor IT assets**, ThreatGEN deployed **Forescout's eyeSight platform**.

- To effectively inventory, **classify and monitor OT/ICS assets**, as well as detect threats on the industrial network, ThreatGEN deployed **Forescout's eyeInspect platform**.

eyeSight
Comprehensive Device Visibility

AGENTLESS
Gain a unified, real-time inventory of network-connected devices.

ACCURATE
Profile all devices to gain context for building proactive security and compliance.

EFFECTIVE
Identify rogue, vulnerable or noncompliant devices and build policies to limit risk.

DEPENDABLE
Gain real-time assurance that security tools and compliance controls are working.

EFFICIENT
Automatically measure and report compliance posture and cyber risk exposure while minimizing human error and increasing efficiency.

Continuously discover, classify and assess all connected things across your enterprise

Forescout eyeSight delivers unparalleled insight into your entire Enterprise of Things (EoT) without disrupting critical business processes.

- Discover every IP-connected device
- Auto-classify devices and gain comprehensiv
- Assess policy compliance and device security

DISCOVER
See devices the instant they connect to the network
Continuously monitor as transient devices come and go
Get real-time asset inventory without business disruption

CLASSIFY
Identify diverse types of IT, IoT and OT devices
Harness the power of the Forescout Device Cloud
Improve auto-classification efficacy, coverage and velocity

forescout.com/platform/eyeSight salesdev@forescout.com

Forescout eyeInspect)) DATASHEET

FORESCOUT
Active Defense for the Enterprise of Things™

eyeInspect
Formerly SilentDefense™

AGENTLESS
Gain a unified, real-time and complete OT asset inventory of connected IP and serial devices.

ACCURATE
Baseline assets and defend your network with thousands of OT-specific threat indicators and powerful machine-learning-based anomaly detection.

EFFECTIVE
Proactively assess risks, discover threats, measure their business impact and prioritize remediation tasks.

DEPENDABLE
Gain real-time assurance that security tools and compliance controls are working.

EFFICIENT
Automate time-intensive compliance and risk assessment tasks while minimizing human error and increasing efficiency.

Reduce risk, automate compliance and optimize threat analysis for ICS and OT environments

Forescout eyeInspect provides in-depth device visibility for OT networks and enables effective, real-time management of a full range of operational and cyber risks.

- Establish a baseline of admissible network behavior using thousands of ICS/OT-specific threat indicators and queries
- Aggregate thousands of alerts and millions of logs according to their risk level and cause
- Auto-classify and assess devices for policy and regulatory compliance

VISUALIZE
See devices the instant they connect to the network
Continuously monitor as devices come and go
Get real-time asset inventory without business disruption

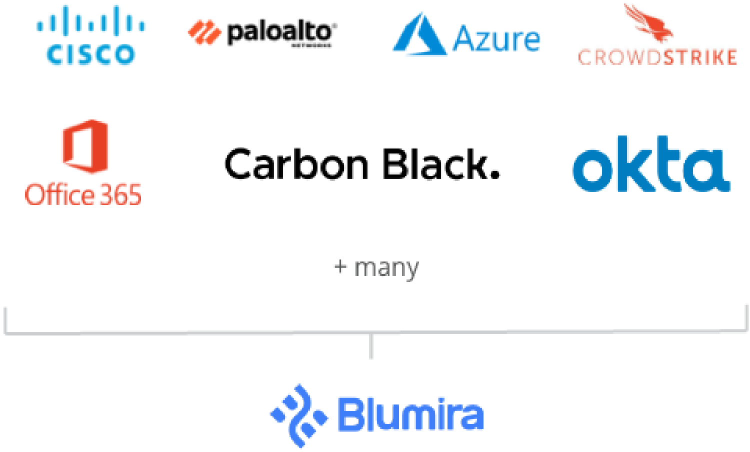
DETECT
Identify diverse types of IP-enabled and serial OT devices
Baseline devices and device groups
Optimize auto-classification efficacy and continuous monitoring

RESPOND
Automate compliance assessments
Assess risk with intuitive risk scores
Gain situational awareness of cyber and operational risk

1

forescout.com/platform/eyeInspect salesdev@forescout.com toll free 1-866-377-8771

Blumira's Cloud SIEM for Detection & Response



- **Blumira's cloud SIEM provides:**
  - Log aggregation
  - Threat detection & correlation
  - Prioritized alerts
  - Security reporting
  - Threat response

- **Secure setup:**
  - Sensitive data stays on-premises
  - Detailed incident information is accessible via onsite solutions
  - Alerts & metadata are sent via SIEM, available to all

- **Wide integration coverage:**
  - Blumira is not restricted to Forescout data collection
  - Integrates with many other on-prem/cloud services

Blumira

Conclusion: Holistic Cybersecurity

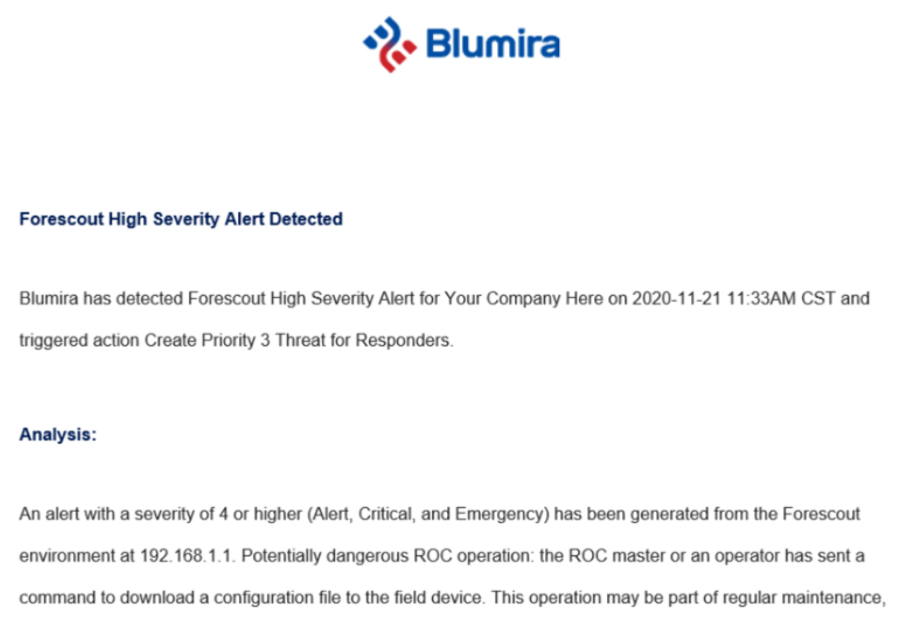
ThreatGen Integrated Solution:
Forescout eyeInsight
Blumira + ThreatGEN full stack monitoring

▶ **50 million**

Events Ingested Daily

▶ **ThreatGEN's oil & gas midstream client now has:**

- Holistic cybersecurity monitoring solution
- Alerts on variety of risks & threats
  - Within minutes, some trigger automated response
- Security playbooks for threat response
- Better cybersecurity practice awareness



Blumira

Forescout High Severity Alert Detected

Blumira has detected Forescout High Severity Alert for Your Company Here on 2020-11-21 11:33AM CST and triggered action Create Priority 3 Threat for Responders.

Analysis:

An alert with a severity of 4 or higher (Alert, Critical, and Emergency) has been generated from the Forescout environment at 192.168.1.1. Potentially dangerous ROC operation: the ROC master or an operator has sent a command to download a configuration file to the field device. This operation may be part of regular maintenance,

▶ **Business results:**

- Manageable detection & response
- Automated filtering, sorting and correlation by Blumira's platform
- Prevents alert fatigue and overwhelming analysts

Blumira

02

How Blumira Works

Blumira

Threats Detected by Blumira

Ransomware

Reconnaissance Scanning

Privilege Escalation

New Admin Accounts

Data Exfiltration

Malicious Executables

Malware Applications

Access Attempts

Password Spraying

Brute-Force Attacks

Geo-Impossible Login

Multiple Failed Logins

Account Lockouts

Hacker Tool: Credential Theft

Misconfiguration

RDP / SMB Exposure

Privileged Access

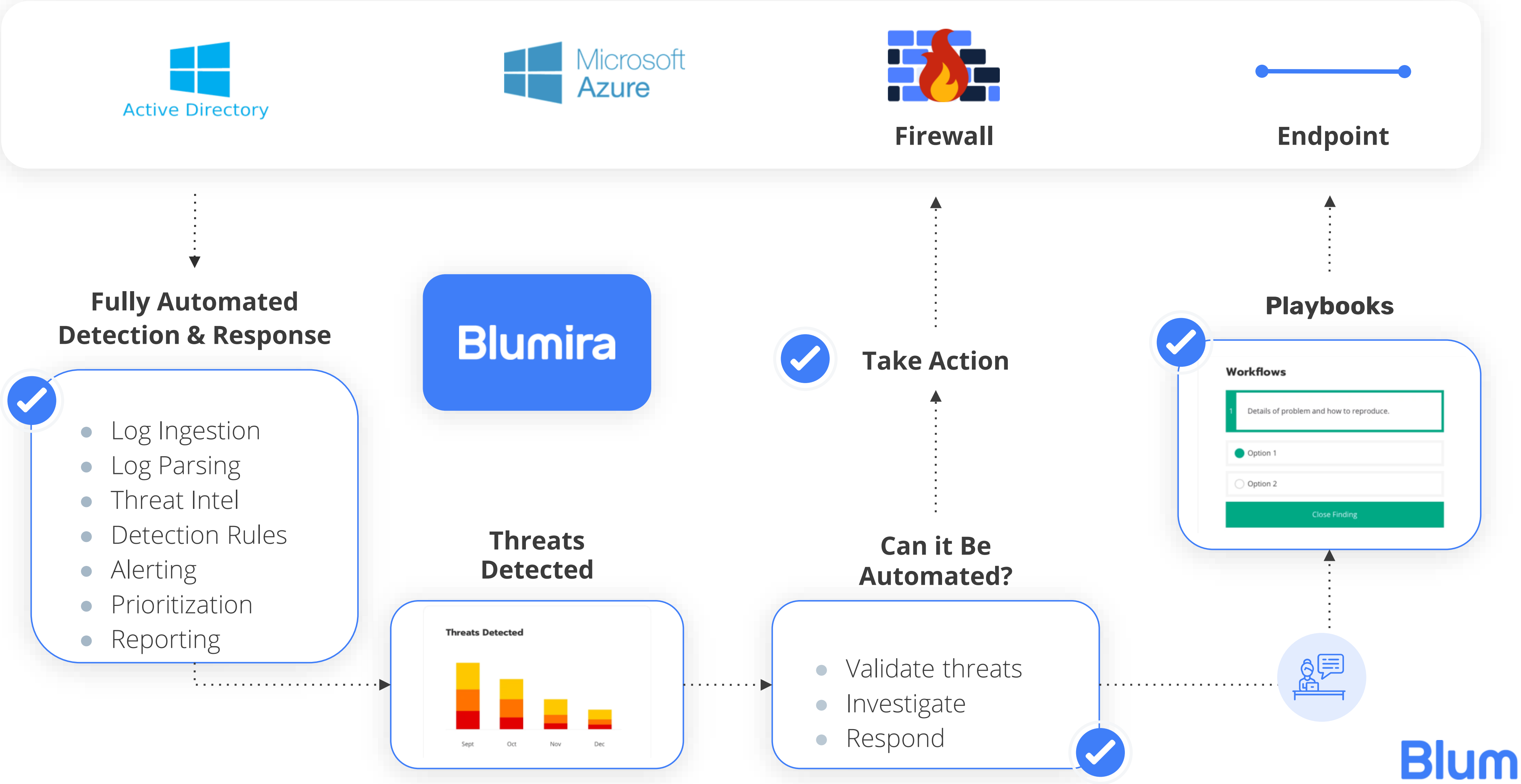
Exploits

Bluekeep

Cobalt Strike

***Note**: Blumira detects much more! These are only a few key examples.*

End-to-End Threat Detection



Active Directory

Microsoft Azure

Firewall

Endpoint

Fully Automated Detection & Response

- Log Ingestion
- Log Parsing
- Threat Intel
- Detection Rules
- Alerting
- Prioritization
- Reporting

Blumira

Threats Detected

Can it Be Automated?

- Validate threats
- Investigate
- Respond

Take Action

Playbooks

Blumira

Blumira Integrates With Any Service

Cloud Infrastructure	Microsoft Azure Azure Active Directory okta DUO SECURITY
Endpoint	Carbon Black. CROWDSTRIKE SOPHOS Malwarebytes TREND MICRO™ eset® BlackBerry. CYLANCE.
Productivity	Office 365 G Suite proofpoint. FORCEPOINT cisco. Cisco Umbrella
Host	Windows Server Windows Active Directory Linux
Firewall	paloalto NETWORKS cisco Meraki Check Point® SOFTWARE TECHNOLOGIES LTD. SOPHOS

Blumira

Thank you!

ThreatGEN

Try Out Blumira:
blumira.com/trial

Blumira